PODER JUDICIÁRIO
TRIBUNAL REGIONAL FEDERAL DA 6ª REGIÃO
Subsecretaria de Infraestrutura

ESTUDO TÉCNICO PRELIMINAR - ETP (LEI 14.133/2021) 0724279

CONTRATAÇÃO DE SERVIÇOS E/OU AQUISIÇÃO DE BENS PERMANENTES E DE CONSUMO

Introdução

ETP foi elaborado conforme:

- a ordem dos elementos indicados no § 1º Art. 18 Lei 14.133/2021 (Nova Lei de Licitações e Contratos);

- o guia de suporte ao preenchimento de ETP 0366701, com orientações sobre conceitos, elaboração de textos e referências normativas.

Observação: conforme § 2º Art. 18 Lei 14.133/2021, ETP deverá conter ao menos os itens**I, IV, VI, VIII e XIII** e, quando não contemplar ser incluídas as devidas justificativas.

I - Descrição da necessidade da contratação, considerado o problema a ser resolvido sob a perspectiva do interesse público

A necessidade da contratação do TRF6 foi apontada em conjunto com o TRF1 no Estudo Técnico Preliminar do CJF (reprodução abaixo:

A Solução de backup da Justiça Federal da 1ª Região (JF1) atualmente instalada decorre do fornecimento objeto dos con 6.839/2010, por meio dos quais foi adquirida a solução Netbackup do fabricante Veritas. A última contratação observou modelo d quantidade de dados "bacapeados" (volumetria), com aquisição de 30 TB (trinta terabytes). Ocorre que no decorrer do tempo, com a amp dados, serviços de TI e posteriormente instituição dos sistemas digitais, o licenciamento mostrou-se bastante defasado frente ao ambiente

A JF1, historicamente, utiliza a modalidade de licenciamento de software de backup por volumetria, a qual encontra-se conformidade aos requisitos de utilização junto ao fabricante. Diante o cenário, surge a necessidade de adequação de licenciamento ao a atualmente implantado no âmbito da JF1. Com a consolidação da infraestrutura por meio da virtualização, o modelo de licenciamento por clientes mostra-se bastante interessante tanto economicamente, quanto tecnicamente, visto que a flexibilidade e escalabilidade de ambien em processador, bem como as licenças para clientes não possuem limitação de quantidade de armazenamento. Configura-se, entret modalidade presente em todos os fabricantes, sendo tendência de mercado unificação nessa modalidade. O direcionamento para licenci poderia acarretar indevida restrição de competitividade.

A adoção de serviços em nuvem vem sendo uma tendência em diversos órgãos ou empresas públicas, aumentando confiabilidade. Dessa forma, esta contratação visa adequar a solução de backup institucional aos novos cenários que se desenham para a serviços de infraestrutura e compatibilidade com armazenamento em nuvem, sem preterir, entretanto, do armazenamento local, desempenho e dos custos decorrentes de restaurações a partir da nuvem.

Após realização de Consulta Pública (Consulta N. 1/2020 - SEI12985772) para prosseguimento dessa contratação, bem como de cotações de preços junto aos fornecedores, percebeu-se grande resistência quanto à precificação dos serviços de migração, inicialme desta contratação. Tal serviço de migração implica, de certa forma, na diminuição da concorrência e favorecimento do fabricante Veritas, realizar o serviço, por ser a solução atualmente implantada na JF1. Diante o cenário a equipe técnica, no decurso desse planejamento, op item de migração de forma a viabilizar maior concorrência e tentar gerar maior participação no certame.

Devido a limitações em seus diversos sistemas, novos e legados, a JF1 tem enfrentado limitações ou problemas com relação destacar alguns ambientes: RED (Repositório Eletrônico de Documentos), e-proc, JCR (módulo do PJe para arquivos anexos dos processos digital da ASCOM, bancos de dados Oracle, Postgres, sistemas de arquivos NAS dos storages, dentre outros. Nesse cenário, torna-se altar atualização da solução atual e com suporte vigente, de forma a fazer frente a tais situações desafiadoras.

Relativamente aos serviços de treinamento, necessário considerar que parcela da equipe técnica é carente de treinament

atual, sendo necessário o nivelamento e cobertura da defasagem de conhecimento sobre ela, além da possibilidade de outra solução se certame, requerendo por si a capacitação de toda a equipe responsável pela administração das cópias de segurança na 1ª Região. Tais trein se, adicionalmente, por motivos de essencial necessidade de descentralização das atividades de backup às diversas seccionais da JF1.

A não contratação de uma solução de backup enseja desconformidade do licenciamento bem como riscos à salvaguarda das da JF1, onde seria retirada toda a garantia, disponibilidade, resposta a perdas de dados, confiabilidade dos dados, e deixaria a infraestr Tribunal Regional Federal da Primeira Região (TRF1), bem como suas respectivas seccionais sem proteção quanto ao backup dos dados inst

Por tudo exposto, busca-se com a presente contratação:

a) Redução dos riscos de interrupção dos serviços e sistemas em decorrência da implantação de mudanças na infraestrutura

b) Aumentar a segurança e eficiência dos backups dos dados de todos os sistemas do TRF6;

c) Aumentar e manter os serviços com elevado padrão de desempenho, qualidade e confiabilidade;

d) Assegurar a sustentabilidade dos serviços que envolvem a infraestrutura de TI;

e) Fornecer níveis de disponibilidade condizentes com as necessidades do TRF6, provendo ininterruptamente os serviços d horas por dia nos 365 dias do ano e possuir recursos que minimizem ocasionais indisponibilidades;

f) Fornecer níveis de desempenho condizentes com as necessidades do TRF6, provendo serviços de backup com tempos acarretem impactos na percepção dos usuários desses serviços;

g) Fornecer níveis de segurança às informações do TRF6 condizentes com os requisitos de integridade e confiabilidade d recursos que permitam operacionalização de melhores práticas relativas a essas questões;

h) Existência de serviços especializados para realizar os diagnósticos e todas as ações de suporte para restabelecer o plen recursos de proteção de dados no menor tempo de espaço possível;

i) Estar em conformidade com a Portaria CJF n. 540/2021, que dispõe sobre a institucionalização da política de backup e rest do Conselho da Justiça Federal e dá outras providências;

j) Prover maior segurança para os usuários acerca dos dados armazenados pelo TRF6.

II - Demonstração da previsão da contratação no plano de contratações anual, sempre que elaborado, de modo a indicar o seu alinhamento com o planejamento da Administração

- Resolução CNJ nº 370, de 28 de janeiro de 2021 - Estratégia Nacional de Tecnologia da Informação e Comunicação do Poder Judiciário (ENTIC-JUD);
- Resolução CJF nº 685, de 15 de dezembro de 2020 - Plano Estratégico de Tecnologia da Informação da Justiça Federal
- Portaria PRESI 125/2023 - Plano Estratégico Regional da Justiça Federal da 6ª Região para o ciclo 2023-2026.

Macrodesafio: Fortalecimento da Estratégia Nacional de TIC e de Proteção de DadosObjetivos Estratégicos da Justiça Federal:1) Aperfeiçoar e assegurar a efetividade dos serviços de TI para a Justiça Federal

Indicadores	Metas
1 - Índice de satisfação dos clientes internos com os serviços de TI.	1 - Atingir, até 2025, 85% de satisfação dos clientes internos de TI.
2 - Índice de satisfação dos clientes externos com os serviços de TI.	2 - Atingir, até 2026, 80% de satisfação dos clientes externos de TI.

III - Requisitos da Contratação

Definição dos requisitos (Art. 18, § 1º, III, da Lei n. 14.133/2021)

1. Requisitos de Negócio

   1.1. Assegurar a efetividade dos serviços de TI para o TRF6, através da continuidade dos serviços de cópias de segurança do ambiente de forma satisfatória, conforme a Política de Backup;

   1.2. Assegurar a restauração dos dados requisitados pelos usuários do TRF6 de acordo com a sua Política de Backup;

   1.3. A solução deve permitir armazenar a quantidade de dados necessária para cumprir com a retenção dos dados de acordo com a Política de Backup.

2. Requisitos de Garantia

   2.1. A garantia da solução deve permitir reparar eventuais falhas e substituir peças com defeito por outras de configuração idêntica ou superior;

   2.2. A garantia da solução deve permitir a atualização dos produtos licenciados assim que novas versões e releases dos softwares que fizerem parte da solução contratada estiverem disponíveis.

3. Requisitos Técnicos

   3.1. Os serviços de suporte deverão ser capazes de atender às demandas de compatibilidade da solução de backup com a infraestrutura computacional existente no TRF6.

4. Requisitos de Suporte

   4.1. Será prestado serviço de suporte técnico durante toda a vigência do contrato, com direito a atualizações de versões da solução que incorporem correções de defeitos e melhorias implementadas pelo fabricante.

5. Requisitos de Sustentabilidade Ambiental

   5.1. A CONTRATADA será responsabilizada por qualquer prejuízo que venha causar ao TRF6 por ter suas atividades suspensas, paralisadas ou proibidas por falta de cumprimento de normas ligadas ao software e ainda aos serviços elencados no presente Termo de Referência;

   5.2. A CONTRATADA deverá comprovar que os produtos ofertados atendem aos critérios de segurança, compatibilidade eletromagnética e eficiência energética, previstos no art. 3º, inciso II, do Decreto n. 7.174, de 12 de maio de 2010, regulamentado pela Portaria INMETRO n. 170, de 10 de abril de 2012;

   5.3. Só será admitida a oferta de bens de informática e/ou automação que não contenham substâncias perigosas em concentração acima da recomendada na diretiva RoHS (Restriction of Certain Hazardous Substances), tais como mercúrio (Hg), chumbo (Pb), cromo hexavalente (Cr (VI)), cádmio (Cd), bifenil polibromados (PBBs), éteres difenil-polibromados (PBDEs), conforme o art. 5º, inciso IV, da IN MPOG 01, de 19 de janeiro de 2010;

   5.4. As comprovações dos dois itens anteriores, quando exigidas pela CONTRATANTE, poderá ser feita mediante apresentação de certificação emitida por instituição pública oficial ou instituição credenciada, ou por qualquer outro meio de prova, em especial laudo pericial, que ateste que os bens fornecidos cumprem com as exigências do edital, conforme art. 42, inciso III, da Lei 14.133, de 1º de abril de 2021;

   5.5. A CONTRATADA deverá, para a execução do contrato, fornecer aos empregados os equipamentos de segurança que se fizerem necessários, para a execução de serviços, conforme disposto no art. 6°, inciso IV, da Instrução Normativa SLTI/MPOG n. 01, de 19 de janeiro de 2010;

   5.6. A CONTRATADA deverá se atentar às normas em vigor atinentes à sustentabilidade expressas na 2ª edição do Manual de Sustentabilidade de compras e contratos do Conselho da Justiça Federal, instituído pela Portaria CJF n. 96, de 10 de fevereiro de 2023;

   5.7. A CONTRATADA deverá respeitar a legislação vigente e as normas técnicas, elaboradas pela ABNT e pelo INMETRO para aferição e garantia de aplicação dos requisitos mínimos de qualidade e acessibilidade do software e ainda dos serviços elencados no Termo de Referência.

6. Requisitos Legais e Normativos Aplicáveis ao Objeto da Contratação

   6.1. Política de Backup do CJF, da Portaria CJF (CJF-POR-2021/00540);

   6.2. Lei n. 14.133, de 1º de abril de 2021;

   6.3. Resolução CNJ 468, de 15 de julho de 2022; e

   6.4. Portaria CJF n. 232, de 30 de maio de 2023.

IV - Estimativas das quantidades para a contratação, acompanhadas das memórias de cálculo e dos documentos que lhes suporte, que considerem interdependências com outras contratações, de modo a possibilitar economia de escala

A pesquisa de preços realizada pelo CJF levantou os valores abaixo detalhados:

CUSTOS UNITÁRIOS (R$)										
Item	Descrição	Unidade de Medida	Quantitativo Total	Petacorp	Stobtech	Roost	Ata de RP TRF3 (PE. 36/2022) - 36 meses	TRF5 - Contrato n. 20/2022	TJDFT (PE n. 059/2022)	MINIST DA SA (PE 34/20 1 me
1	Subscrição de licenças de software para proteção de dados para 60 meses	Front End Terabyte	2.045	40.000,00	58.930,00	44.000,00	37.036,75		34.365,00	6.37
2	Subscrição de solução de backup para o Microsoft 365 por 60 meses	Usuários	21.160	350,00	622,10	498,00				298
3	Appliance de backup para armazenamento de dados para curta retenção com garantia por 60 meses	Equipamento	20	1.000.000,00	1.614.000,00	1.187.000,00	351.638,48			
4	Expansão do Appliance de backup para armazenamento de dados para curta retenção com garantia por 60 meses	Expansão de Equipamento	28	360.000,00	884.700,00	742.000,00	90.291,09			
5	Appliance de backup para armazenamento de dados para longa retenção com garantia por 60 meses	Equipamento	6	2.400.000,00	2.888.120,00	2.731.000,00	1.492.946,65			
6	Expansão de Appliance de backup para armazenamento de dados para longa retenção com garantia por 60 meses	Expansão de Equipamento	6	180.000,00	274.020,00	233.000,00	788.766,55			
7	Serviço de instalação e configuração	Serviço	19	40.000,00	77.000,00	200.000,00	3.523.614,76	25.000,00		
8	Transferência de conhecimento	Turma	4	15.000,00	22.000,00	35.000,00	44.202,91	12.000,00		
9	Suporte técnico especializado de toda a solução por 60 meses	Serviço	19	180.000,00	845.000,00	648.000,00	782.681,65		1.690.000,00	846.0

Atualmente, a infraestrutura corporativa de dados do TRF6 a ser protegida é composta pelo seguinte cenário:

1. Ambiente de processamento e virtualização:
    1.1. VMware vSphere nas versões 6.7.0 e 7.0.3 licenciados pelo TRF1 para os hosts abaixo:
        1.1.1. Pool SJMG - 06 hosts com 02 sockets de 08 Cores cada, totalizando 192 Cores;
        1.1.2. Pool TRF6 - 04 hosts com com 04 sockets de 12 Cores cada, totalizando 256 Cores;
        1.1.3. Pool SSJs - 25 cidades com 02 hosts com 20 Cores cada, totalizando 1000 Cores.
    1.2. A volumetria estimada de dados a serem protegidos do ambiente virtual é de aproximadamente 150 TB considerando marge segurança.
2. Ambiente de armazenamento e storage:
    2.1. Storage Huawei OceanStore 5300v5 com capacidade de armazenamento de 542 TB;
    2.2. Storage Dell Unity 880 com capacidade de armazenamento de 1,6 PB;
    2.3. A volumetria estimada de dados a serem protegidos do ambiente físico é de aproximadamente 400 TB, incluindo uma marge segurança de aproximadamente 10% do total em utilização.

O serviço de proteção de dados do TRF6 atualmente é representado pelo seguinte cenário:

1. Hardware:
    1.1. 02 unidades Dell PowerEdge R730;
    1.2. 01 Unidade Robô IBM TS4300 Tape Library (12 Drives).
2. Servidores
    2.1. Master Server (virtual);

2.2. Medias Servers (02 físicos, 02 virtuais).

3. Software:

3.1. Veritas Netbackup 10.0.

4. Clientes de Backup

4.1. 37 Clientes/Servidores.

5. Tipos de Políticas

5.1. Standard;

5.2. Oracle;

5.3. MS-Windows;

5.4. VMware.

Considerando que o TRF6 centraliza em seu Datacenter os sistemas que atendem ao 1º e 2º graus, além de atender às unic administrativas, para cada novo sistema criado ou modificado, surgem novas demandas de criação de equipamentos virtuai desenvolvimento, homologação e produção. Assim, para cada ambiente fornecido é necessária a inclusão do novo ativo nas políticas de ba do TRF6.

Considerando que a atual solução é de propriedade do TRF1 e não comporta o volume de dados e a necessidade de atende às áreas de negócio do TRF6 com uma solução robusta de cópia de segurança corporativa de todos os servidores virtuais, storages e aplica torna-se necessária a aquisição de uma nova solução de proteção de dados que ofereça um melhor serviço de continuidade, integrida garantia de restauração contínua dos dados sem a perda dos mesmos.

Ademais, a aquisição dos elementos de curta e longa retenção se mostra essencial porque que a atual solução de backup r uma solução dedicada à funcionalidade, já que é executada em servidores de rede e com software obsoleto, além de não suportar o volum dados necessários para a proteção do ambiente. A precariedade representa grande risco de perda de dados e consequentemente inco risco inaceitável para o TRF6.

Para o elemento de curta retenção, a demanda atual do TRF6 demanda um equipamento com 05 (cinco) expansõe armazenamento, de forma a totalizar um armazenamento combinado de 370 TB. Considerando que a contratação original previa apena (duas) expansões, torna-se necessária a aquisição de mais 03 (três) unidades por meio de adesão à própria Ata de Registro de Preços.

Em relação à longa retenção, deve-se adquirir uma appliance não incluída na contratação original mediante adesão à própri de Registro de Preços.

As boas práticas ainda indicam que o elemento de longa retenção deve ser colocado em local distinto, sendo indicada a insta no Ed. ERA.

Pelo exposto, serão adquiridos a volumetria de 400 TB Front End, 01 equipamento de curta retenção com mais 05 expansõe armazenamento, 01 equipamento de longa retenção com no mínimo 600 TB e os serviços de suporte e treinamento. A proteção para soluç Office 365 não será adquirida inicialmente, em razão do funcionamento sem backup do serviço desde a implantação do TRF6 e em face da disponibilidade garantida pelo serviço.

V - Levantamento de mercado, que consiste na análise das alternativas possíveis, e justificativa técnica e econômica da esc do tipo de solução a contratar

Com base em opções disponíveis no mercado, foram levantadas as diferentes soluções de TIC que podem atender às necessidades do TRF6

5.1. Solução nº 1 - Utilizar software livre / software público

5.1.1. No universo de softwares livres, existem diversas soluções. Ocorre que todo uso de software livre demanda esforços técnic desenvolvimento e customização da solução.

5.1.2. Cumpre registrar que o quadro de servidores da SECTI é reduzido e a demanda de serviços gerada pelos sistemas do sobrecarregou, sobremaneira, os trabalhos desta Diretoria, sem, contudo, completar o quadro funcional que já vinha defasado de de obra especializada.

5.1.3. É inegável que uma prestação de serviços eficiente está condicionada à existência de um contingente de pessoal capacita em número suficiente para atender à demanda de usuários dos nossos serviços, pois a insuficiência de pessoal além de contribuir que o serviço prestado seja ineficiente e moroso, faz com que haja acúmulo e sobrecarga de trabalho nos poucos servi existentes. Apesar de ser cediço que tal situação não é adequada, deve-se reforçar que os servidores da Secretaria de Tecnolog Informação cumprem sua missão institucional com inegável zelo e esforço, pois, uma vez que não há possibilidade de desligam dos sistemas informatizados que operam, a equipe tem trabalhado no decorrer dos sete dias da semana.

5.1.4. Pelo exposto e considerando que o TRF6 não conta com profissionais especializados em quantidades necessárias pa operacionalização das atividades de desenvolvimento e customização dos softwares livres, a alternativa não atende à necessidade

5.2. Solução nº 2 - Utilizar a atual solução de backup

5.2.1. Não é possível seguir com a atual solução de backup, uma vez que o licenciamento pertence ao TRF1 e já não aten volumetria necessária.

5.3. Solução nº 3 - Adquirir nova solução de backup

5.3.1.Em levantamento de mercado realizado pelo CJF, incluindo o estudo realizado acerca de soluções utilizados por outros ent Administração Pública, foram encontradas diversas potenciais soluções.

5.3.2. Diante disso, a equipe de planejamento, realizou um comparativo, dos principais requisitos, com base em dados disponibiliz no site de cada fabricante. As soluções
identificadas como líderes de mercado foram comparadas conforme descritivo a seguir:

Figure 1: Magic Quadrant for Enterprise Backup and Recovery Software Solutions

Source: Gartner (July 2021)

5.3.3. Os principais pontos a serem especificados:

ITEM	MOTIVAÇÃO
Integração com VMware	Ambiente utilizado atualmente
Integração com Oracle	Ambiente utilizado atualmente
Integração com Kubernetes	Ambiente utilizado atualmente
Integração com Openshift	Ambiente utilizado atualmente
Integração com snapshot - Storages	Ambiente utilizado atualmente
Integração com clone - Storages	Ambiente utilizado atualmente
Integração com replicação - Storages	Ambiente utilizado atualmente
Integração com ambiente Docker	Ambiente utilizado atualmente
Integração com Office 365	Ambiente utilizado atualmente
Envio de backup para Nuvem	Possibilidade para realizar backup fora do ambiente do CJF
Gerenciamento centralizado	Maior eficiência operacional
Appliance de Backup	Proteção Local para atender o 3-2-1

5.4. Análise e comparação entre as soluções de TIC avaliadas:

Requisito	ID da Solução	Sim	Não	A
A Solução encontra-se implantada outro órgão ou entidade Administração Pública Federal?	Solução 1	X		
	Solução 2			
	Solução 3			
A Solução encontra-se implantada em outro órgão ou entidade da Justiça Federal?	Solução 1		X	
	Solução 2	X		
	Solução 3		X	
A Solução está disponível no Portal do Software Público Brasileiro?	Solução 1			
	Solução 2		X	
	Solução 3			
A Solução é um software livre ou software público?	Solução 1	X		
	Solução 2		X	
	Solução 3		X	
A Solução é aderente às políticas, premissas e especificações técnicas definidas pelos Padrões e-PING, e-MAG?	Solução 1			
	Solução 2			
	Solução 3			
A Solução é aderente às regulamentações da ICP-Brasil? (quando houver necessidade de certificação digital)	Solução 1			
	Solução 2			
	Solução 3			
A Solução é aderente às orientações, premissas e especificações técnicas e funcionais do Modelo de Requisitos para Sistemas Informatizados de Gestão de Processos e Documentos do Judiciário – MoReq-Jus?	Solução 1			
	Solução 2			
	Solução 3			

5.5. Justificativa da solução de TIC escolhida, considerando o ciclo de vida do objeto

5.5.1. Ao adotar o licenciamento por front end terabyte, garante-se a proteção dos dados, independentemente de onde est armazenados. Isso é especialmente valioso em ambientes complexos, nos quais os dados podem estar distribuídos em v localidades, como servidores locais, sistemas de armazenamento em rede (NAS) e até mesmo em ambientes de nuvem. abordagem abrangente permite a obtenção de uma solução de backup unificada, independentemente da localização dos da garantindo-se a proteção adequada em todos os cenários;

5.5.2. É importante destacar que os principais fabricantes de solução de backup, tais como Dell, Commvault, Veeam e Veritas, ad o formato de licenciamento por terabyte. Tratam-se de fornecedores líderes do setor e que oferecem soluções de backup robust confiáveis. Ao optar pelo licenciamento por front end terabyte, garante-se o alinhamento da estratégia de backup com as prá recomendadas pelos líderes do mercado, o que proporciona maior confiabilidade e suporte contínuo ao longo do tempo;

5.5.3. Uma das vantagens significativas do licenciamento por front end terabyte é a ausência de restrições em relação às mudanç arquiteturas do ambiente computacional. À medida que a infraestrutura de TIC é atualizada, como em casos de adoção de r tecnologias de virtualização, containers ou outras inovações, não será necessária a aquisição de licenças adicionais para cada má virtual ou elemento da arquitetura.

5.5.3.1. O licenciamento por front end terabyte oferece a liberdade de adaptar o ambiente computacional sem implica custosas em termos de licenciamento;

5.5.4. Com tal modelo de licenciamento, o TRF6 estará preparado para lidar com cargas de trabalho hospedadas em nuvem, ocorre atualmente com o Eproc. À medida que a computação em nuvem continua a ganhar popularidade e as organizações mi suas operações para plataformas de nuvem pública ou privada, é fundamental ter uma solução de backup que possa pro efetivamente esses dados.

5.5.4.1. O licenciamento por front end terabyte fornece capacidade e flexibilidade, permitindo-se o aproveitamento dos bene da nuvem sem preocupações excessivas em relação ao licenciamento;

5.5.5. Em contrapartida, embora o licenciamento baseado no número de máquinas virtuais seja uma opção comum, é impor considerar algumas desvantagens associadas à abordagem, já que o licenciamento baseado no número de máquinas virtuais impor restrições à escalabilidade de nossa infraestrutura. À medida que são adicionados novos serviços ao ambiente, precis adquirir licenças adicionais para cada máquina virtual que será criada para disponibilização do serviço em questão.

5.5.5.1. A adição pode resultar em custos significativos à medida que a infraestrutura cresce, além de complexi administrativa para acompanhar e gerenciar todas as licenças individuais. Gerenciar licenças para máquina virtual pode se t um processo complicado e propenso a erros de dimensionamento, pois é necessário acompanhar e manter registros pre das estratégias de negócio para a utilização de novas aplicações ou criação de novos serviços, o que demanda tempo e esf Tal complexidade pode aumentar à medida que o número de máquinas virtuais aumenta, dificultando o gerenciamento efic do ambiente de backup.

5.5.6. O licenciamento baseado no número de máquinas virtuais pode restringir a flexibilidade de adaptação e modificaçã ambiente computacional. Caso seja necessária a adição ou remoção de máquinas virtuais, é possível ocorram limitações imp pelas licenças individuais. Tais limitações podem gerar obstáculos ao dimensionamento e à otimização de nossa infraestru dificultando a implementação de mudanças e inovações tecnológicas.

5.5.7. De tal forma, o licenciamento por front end terabyte oferece vantagens significativas em termos de prot independentemente do local de armazenamento, do alinhamento com os principais fabricantes de solução de backup, da flexibili em mudanças de arquitetura e da preparação para cargas de trabalho em nuvem. Por outro lado, o licenciamento baseado no nú de máquinas virtuais apresenta desvantagens relacionadas à escalabilidade, além da complexidade no gerenciamento e das limita na adaptação do ambiente computacional.

VI - Estimativa do valor da contratação, acompanhada dos preços unitários referenciais, das memórias de cálculo e documentos que lhe dão suporte, que poderão constar de anexo classificado, se a Administração optar por preservar o sigilo até a conclusão da licitação

Item	Descrição	Unidade de Medida	Quantidades	Custo Unitário (R$)	Custo Total (R$)	Observações
1	Subscrição de licenças de software para proteção de dados para 60 meses	Front End Terabyte	400	22.400,00	8.960.000,00	A volumetria estimada de dados a sere protegidos do ambiente físico é de aproximadamente 400 TB, incluindo un margem de segurança de aproximadame 10% do total em utilização.
2	Subscrição de solução de backup para o Microsoft 365 por 60 meses	Usuários		1.194,50		
3	Appliance de backup para armazenamento de dados para curta retenção	Equipamento	1	400.000,00	400.000,00	
4	Expansão do Appliance de backup para armazenamento de dados para curta retenção	Expansão de Equipamento	5	324.000,00	1.620.000,00	Necessidade de adesão de mais 03 unidad Ata de Registro de Preços, em razão da falta de previsão do quantita necessário (70 TB + 5 * 60 TB, totalizando, assim, 37
5	Appliance de backup para armazenamento de dados para longa retenção	Equipamento	1	1.998.000,00	1.998.000,00	Necessidade de adesão à Ata de Registro Preços, em razão da falta de previsão do item
6	Expansão de Appliance de backup para armazenamento de dados para longa retenção	Expansão de Equipamento		162.000,00		
7	Serviço de Instalação e configuração, migração, adequação e transferência de conhecimento	Serviço	1	25.000,00	25.000,00	
8	Transferência de conhecimento	Turma	1	12.000,00	12.000,00	
9	Suporte técnico especializado de toda a solução por 60 meses	Serviço	1	140.000,00	140.000,00	
Valor Total a ser Adquirido (R$)					**13.155.000,00**	

VII - Descrição da solução como um todo, inclusive das exigências relacionadas à manutenção e à assistência técnica, qua for o caso

Detalhamento das Soluções - Especificação Técnica da Solução de Proteção e Segurança de Dados

1. Subscrição de Licenças de Software para Proteção de Dados

1.1. O licenciamento ofertado deve atender o modelo de subscrição durante o período de vigência do contrato, pelo prazo d (meses) meses;

1.1.1. Durante o período, deve permitir o suporte e atualização da solução sem custos adicionais;

1.1.2. Após findado o período, a solução deverá ainda operar com todas as funcionalidades, com exceção do supo atualização.

1.2. A solução ofertada não pode ser do tipo comunidade, software livre, ou possuir componentes e módulos sem suporte ofici fabricante; Todos os componentes de software descritos deverão ser de um único FABRICANTE;

1.3. Todos os componentes da solução de Backup e Restore deverão ser integrados e que ofereçam um módulo únic gerenciamento;

1.4. A solução ofertada deverá possuir todos os produtos na versão estável mais atual do produto, não serão aceitos pro obsoletos ou fora de linha de produção do fabricante;

1.5. Todas as funcionalidades e requisitos elencados neste documento, independentemente de qualquer quantidade de utilizaçã referido serviço, deve estar disponível sem nenhum tipo de cobrança adicional;

1.6. Deverão ser fornecidas licenças na modalidade Front End Terabyte;

1.7. A licença deverá incluir todas as funcionalidades solicitadas no presente termo, com suporte para backup, restore, tecnolog compressão de dados nativa e tecnologia de desduplicação de dados nativa, onde o licenciamento deverá possuir capacidade ilim de retenções, cópias dos dados protegidos, replicações para outros ambientes para fins de recuperação de desastres e suportar t infraestrutura da CONTRATANTE detalhada no Edital, sem nenhum ônus a durante a vigência do contrato. A funcionalidad compressão e desduplicação por software poderá ser realizada através de componente separado de software ou appliance virtual desde que seja homologado pelo fabricante do software de backup.

1.8. A solução de Proteção de Dados a ser ofertada deverá atender integralmente os requisitos especificados neste Termo, devend fornecida com todas as licenças que forem necessárias para entrega 100% funcional da solução, arquitetura e características gera software;

1.9. Possuir arquitetura em múltiplas camadas permitindo desempenho e escalabilidade horizontal:

1.9.1. Camada de gerência;

1.9.2. Camada do serviço de mídia/unidade de disco de retenção dos dados;

1.9.3. Camada de clientes/agentes multiplataforma de backups.

1.10. Deve possuir catálogo ou banco de dados contendo as informações sobre todos os dados e mídias onde os backups f armazenados; esse banco de dados ou catálogo deve ser próprio e fornecido em conjunto com o produto;

1.11. A solução de Backup e Recovery deverá permitir a possibilidade de múltiplas políticas de *disaster recovery* para prevenir per dados e cópia automática do catálogo do backup, sincronização entre as cópias do catálogo do backup, replicação entre appliance mesmo domínio de backup e replicação entre appliances em domínios de backup diferentes;

1.12. Deve possuir mecanismo de verificação e checagem de consistência da base de dados no intuito de garantir a integridade dados;

1.13. Possuir mecanismo de reconstrução do catálogo ou banco de dados centralizado em caso de perda do mesmo, se necessidade de recatalogar as cópias de backup ;

1.14. Deve fazer uso de banco de dados relacional para guardar o catálogo de Jobs, arquivos e mídias dos backups;

1.15. Deve suportar servidor de gerência e catálogo instalados em conjunto nas seguintes plataformas: Linux, Windows e/ou appl virtual OVA;

1.16. Deverá permitir a configuração de servidores de gerência e catálogo no mesmo servidor ou instância, e suportar arquitetur cluster para promover alta disponibilidade dos serviços de gerenciamento; A implementação dos serviços de gerenciamento, cat e cluster deverá ser suportado nas seguintes plataformas: Red Hat Enterprise Linux, Suse Enterprise Linux e Windows ou virtualizadores;

1.17. Deve suportar servidores movimentadores de dados nas seguintes plataformas: Linux e Windows e/ou appliance virtual OVA;

1.18. Os servidores movimentadores de dados devem suportar balanceamento de carga para distribuir a carga entre eles de f automática;

1.19. Os servidores movimentadores de dados devem suportar configuração de recurso automático de*failover*, ou seja, perm configuração de mais de um servidor movimentador de dados em uma política de proteção, de forma que a indisponibilidade d servidor seja suprida por outro servidor movimentador de dados disponível de forma automática; Esta funcionalidade deveráser n do produto, e não pode ser construída com o uso de soluções baseadas em softwares de cluster de terceiros;

1.20. Deve permitir o backup e restore de arquivos abertos, garantindo a integridade do backup;

1.21. Deve ser capaz de gerenciar múltiplos e diferentes dispositivos de armazenamento e backup (bibliotecas e drives de f dispositivos de disco em bloco), conectados localmente DAS (Direct Attached Storage) ou compartilhados via rede SAN (Storage Network) para armazenamento de dados;

1.22. Possuir a capacidade de dividir o fluxo de dados proveniente de um servidor em vários dispositivos de gravação (*mu streams*);

1.23. Possuir a capacidade de reiniciar backups e restore a partir do ponto de falha, após a ocorrência da mesma;

1.24. Deve possuir mecanismo de instalação e atualização de clientes e agentes de backup de forma remota, por intermédi interface de gerenciamento ou via script, permitindo a instalação de múltiplos clientes de backup simultaneamente;

1.25. Possuir a capacidade de realizar a instalação de atualizações no servidor de backup e clientes;

1.26. Possuir ambiente de gerenciamento de backup e restore via interface gráfica e linha de comando;

1.27. Possuir função de agendamento do backup através de calendário;

1.28. Possuir interface gráfica para gerenciamento, monitoramento e criação de políticas de backup e restore;

1.29. Possuir capacidade de estabelecer níveis de acesso diferenciados e configuráveis para atividades de administração e operaçã software de backup;

1.30. Permitir a programação de tarefas de backup automatizadas em que sejam definidos prazos de retenção dos arquivos;

1.31. Possuir função para definição de prioridades de execução de Jobs de backup ou clients;

1.32. Deverá permitir o agendamento de jobs de backup, sem utilização de utilitários de agendamento dos hosts;

1.33. Possuir a função de Backup sintético que permite a criação de uma única imagem de backup a partir de um backup f qualquer quantidade de backups incrementais. O restore será efetuado da nova imagem full sintética;

1.34. Possuir políticas de ciclo de vida nativas, gerenciar camadas de armazenamento e transferir automaticamente os dado backup entre camadas através do seu ciclo de vida;

1.35. Permitir a realização do backup completo de servidor para recuperação de desastres;

1.36. Permitir restaurar o backup de recuperação de desastres para hardware diferente do original - para ambiente Windows;

1.37. Permitir o controle da banda de tráfego ou otimização de rede durante a execução do backup e/ou do restore;

1.38. Suportar integração com OST (OpenStorage) Disk Appliances através de OpenStorage API;

1.39. Deverá suportar imutabilidade de dados para armazenamentos apresentados via OpenStorage Technology OST;

1.40. Ser capaz de recuperar dados para servidores diferentes do equipamento de origem;

1.41. Ser capaz de utilizar qualquer tecnologia utilizada pela Solução de Armazenamento como destino dos backups armazenamento diretamente anexado (DAS), armazenamento em rede NAS e rede SAN;

1.42. Possuir a função de Disk Staging, ou seja, que permita o envio dos dados para disco e posteriormente do disco para outro tip mídia (disco ou fita);

1.43. Permitir que Logical Unit Numbers (LUNs) sejam apresentadas aos servidores da camada de mídia como destino para realiz de backups;

1.44. Permitir o compartilhamento de LUNs entre vários servidores movimentadores de dados de mesmo sistema operacional situações de recuperação do ambiente;

1.45. A Solução de Proteção de Dados deve suportar e estar licenciada para backup e restore de file systems montados em dispos Network-Attached Storage (NAS) através do suporte ao protocolo NDMP versão 4 ou superiores; ou recursos similares para garan backup do NAS;

1.46. Permitir integração do controle de acesso com sistemas de diretório NIS, NIS+ e/ou Active Directory;

1.47. Permitir a replicação de imagens de um servidor de gerência para outro ambiente, possibilitando a inserção das informaçõ catálogo da imagem de origem para o catálogo do destino, de forma automática e sem a necessidade de licenciamento adicional;

1.48. Possuir Interface única para gerenciamento de todos os servidores independente do S.O. que hospeda esse serviço (Windo Linux); ou ao menos com a separação entre estrutura de backup da Central de Serviços e estrutura de backup das Unidades remot

1.49. Deverá implementar monitoramento e administração remotos da solução de backup a partir de qualquer servidor ou estaçã trabalho;

1.50. A Solução de Backup deverá permitir operações de Backup e Restore através de rede local (LAN_based e Storage Area Net SAN_based ou LAN_free);

1.51. Deverá possibilitar a verificação de erros de leitura nas fitas utilizadas;

1.52. Deverá permitir liberação das fitas magnéticas quando todos os arquivos contidos nas mesmas tenham suas datas de rete expiradas;

1.53. As fitas liberadas devem ficar disponíveis automaticamente para uso de outras tarefas de backup;

1.54. A Solução de Backup deverá, a partir de uma única interface, gerenciar operações de Backup e Restore de diferentes siste operacionais (clientes);

1.55. Para servidores Windows, deverá ser possível a recuperação das imagens de recuperação de desastres mesmo em um hard diferente do original ou em ambiente

virtual;

1.56. A funcionalidade especificada anteriormente deverá suportar em um único servidor de gerência ou servidor de mídia v versões de Windows – Windows 2012, 2012R2, 2016, 2019);

1.57. Deverá permitir a verificação da integridade dos dados armazenados através de algoritmos de checksum e/ou autocorr Funcionalidade poderá ser atendida pelo appliance do item 3 e/ou pelo componente especificado no item 1.7;

1.58. Deverá possuir capacidade de realizar desduplicação de dados na camada do cliente, servidor de backup e appliance desduplicação; A solução deverá permitir a desduplicação de qualquer capacidade (de acordo com o volume identificado e licenc e em qualquer forma de desduplicação (cliente, servidor de backup e appliances) nativamente, não sendo aceitas composiçõe produtos de terceiros ou fora da solução contratada, podendo ser provida tanto por software quanto pelo appliance do item 3 e/ou componente de software especificado no item 1.7;

1.59. Deverá suportar desduplicação de blocos na origem (client-side), de forma que o cliente envie apenas novos blocos de c criados e/ou modi□□cados a partir do último backup full; podendo ser provida tanto por software quanto pelo appliance do item 3 pelo componente de software especificado no item 1.7;

1.60. Deverá suportar desduplicação Global de blocos de tamanho fixo e/ou variável;

1.61. Não serão aceitas soluções de desduplicação Global parciais, aplicadas por Jobs, políticas de backup independentes ou ap para cenários de replicação de dados via WAN; podendo ser provida tanto por software quanto pelo appliance do item 3 e/ou componente de software especificado no item 1.7;

1.62. A solução de backup deverá ser capaz de gerenciar a réplica do backup desduplicado entre servidores de backup e appliance desduplicação; podendo ser provida tanto por software quanto pelo appliance do item 3 e/ou pelo componente de soft especificado no item 1.7;

1.63. Deverá possuir a capacidade de desduplicação global de dados no nível de segmentos ou blocos de dados repetidos, ambientes físicos e virtuais, mesmo em localidades remotas. Não serão aceitas soluções que utilizem mecanismos de desduplic parcial aplicados a ambientes isolados ou por jobs; podendo ser provida tanto por software quanto pelo appliance do item 3 e/ou componente de software especificado no item 1.7;

1.64. Permitir o envio de dados desduplicados para a nuvem, caso seja necessário o fornecimento de recursos adicionais de softv hardware e licenciamento os mesmos deverão constar detalhados na proposta; podendo ser provida tanto por software quanto appliance do item 3 e/ou pelo componente de software especificado no item 1.7;

1.65. Deverá suportar desduplicação de dados para object storage, para no mínimo AWS S3 e Microsoft Azure Google Cloud Sto podendo ser provida tanto por software quanto pelo appliance do item 3 e/ou pelo componente de software especificado no item 1

1.66. Deverá suportar pool de desduplicação global em Cloud-tier, podendo ser provida tanto por software quanto pelo applian item 3 e/ou pelo componente de software especificado no item 1.7;

1.67. Deverá prover mecanismos de segurança RBAC nativos em cloud para gerenciamento de snapshots;

1.68. Deverá suportar workloads nativos em Cloud para integração com gerenciamento de snapshots;

1.69. Deverá suportar restore granular baseado em Cloud Snapshots;

1.70. Deverá suportar compartilhamento de cópias de backup em Clouds Azure e AWS S3;

1.71. Deverá suportar deploy e integração diretamente para public cloud marketplaces (AWS/Azure/Google Cloud Platform);

1.72. Deverá suportar Cloud snapshot orchestration e estar habilitado suporte para application-aware snapshot, single-file recov integração de snapshot entre múltiplas regiões;

1.73. Deverá possuir a capacidade de desduplicação de dados no nível de segmentos ou blocos de dados repetidos de ambi Oracle; podendo ser provida tanto por software quanto pelo appliance do item 3 e/ou pelo componente de software especificad item 1.7;

1.74. Deverá suportar desduplicação de blocos na origem (client-side), para ambientes Oracle; podendo ser provida tanto por soft quanto pelo appliance do item 3 e/ou pelo componente de software especificado no item 1.7;

1.75. Deverá possuir a capacidade de Replicação de Dados entre “pools” de desduplicação de maneira otimizada, enviando som blocos únicos; podendo ser provida tanto por software quanto pelo appliance do item 3 e/ou pelo componente de software especif no item 1.7;

1.76. Deverá possuir a capacidade de realizar balanceamento de carga automático entre servidores ou appliance de desduplicação

1.77. Deverá possibilitar a distribuição automática de carga entre os servidores que executarão o serviço de proteção de dado seja, os dados oriundos dos clientes de backup deverão ser distribuídos de forma automática entre os servidores de backup da solu Em caso de falha de um dos servidores de backup, o cliente automaticamente irá encaminhar seus dados através de outro servid backup ativo. Esta funcionalidade deverá ser nativa do produto, não sendo admitidas soluções baseadas em softwares de clust terceiros;

1.78. Deverá possuir a capacidade de criptografar os dados armazenados de forma desduplicada; podendo ser provida tant software quanto pelo appliance do item 3 e/ou pelo componente de software especificado no item 1.7;

1.79. As políticas de ciclo de vida da informação devem permitir a replicação das cópias de backup de forma otimizada, fazendo da tecnologia de desduplicação de dados da solução no mesmo site ou entre sites distintos; podendo ser provida tanto por soft quanto pelo appliance do item 3 e/ou pelo componente de software especificado no item 1.7;

1.80. Deverá fazer uso de tecnologia de replicação dos dados (não somente os dados protegidos – cópias de backup – mas tambe catálogo do software de backup necessário para a recuperação do dado) do site principal para o site de desastre, de forma que er evento de desastre, os sites sejam independentes no processo de recuperação;

1.81. Deverá possuir tecnologia de desduplicação de dados inline por padrão; podendo ser provida tanto por software quanto appliance do item 3 e/ou pelo componente de software especificado no item 1.7;

1.82. Deverá permitir que depois de um backup full inicial, os backups subsequentes sejam feitos apenas através do envio diferenças desduplicadas e que esses backups sejam consolidados como se fosse um backup full com a última data de envio; pod ser provida tanto por software quanto pelo appliance do item 3 e/ou pelo componente de software especificado no item 1.7;

1.83. Deverá possuir a capacidade de proteção da base de hashes de desduplicação com cópia externa; podendo ser provida tant software quanto pelo appliance do item 3 e/ou pelo componente de software especificado no item 1.7;

1.84. Para soluções que não possuem a funcionalidade requisitada acima será permitido a entrega de um equipamento adicional de garantir que a base hashes de desduplicação terá uma cópia externa ao equipamento principal; podendo ser provida tant software quanto pelo appliance do item 3 e/ou pelo componente de software especificado no item 1.7;

1.85. Deverá possuir e implementar o fator duplo de autenticação - 2FA para o console de administração gráfica e linha de com por meio do provedor de identidade baseado em SAML ou cartões inteligentes CAC / PIV ou certificados de usuário Criptografia; aceito também autenticação da console de administração via SSO com token para verificação de usuário, até que o token expire;

1.86. Deverá permitir escolher se a criptografia será realizada no agente, com o tráfego de dados via rede já criptografado c servidor de backup;

1.87. Deverá possuir capacidade nativa de efetuar criptografia dos backups em no mínimo 256 bits nos Clientes de Backup e dispositivos de mídia que suportem criptografia;

1.88. Deverá implementar criptografia TLS 1.2 ou superior durante o tráfego dos dados (in-transit) e no armazenamento (at-rest todos os backups, restaurações, replicação automática de imagens e desduplicação; podendo ser provida tanto por software qu pelo appliance do item 3 e/ou pelo componente de software especificado no item 1.7;

1.89. Deverá implementar criptografia (in-transit) para os metadados de catálogo de backup; podendo ser provida tanto por soft quanto pelo appliance do item 3 e/ou pelo componente de software especificado no item 1.7;

1.90. Deverá possuir validação de criptografia FIPS 140-2 para no mínimo os workloads, podendo ser provida tanto por software qu pelo appliance do item 3 e/ou pelo componente de software especificado no item 1.7;

1.91. Deverá possibilitar enviar notificações, quando configurado, dos eventos por e-mail;

1.92. Possuir mecanismo de auditoria, permitindo a emissão de relatórios onde constem, no mínimo, as seguintes informações:

1.92.1. Data e hora da operação, Usuário que realizou a operação, Ação realizada (em caso de modificação de configura informar qual a configuração anterior e a modificação realizada);

1.92.2. Auditoria e controle de acesso devem ser funcionais para operações realizadas via interface gráfica e linha de comand

1.93. Deverá prover monitoramento via interface gráfica e em tempo real dos Jobs sendo executados, incluindo visão de hierárquico dos jobs;

1.94. Deverá suportar operações de backup e restore em paralelo;

1.95. Deverá possuir a funcionalidade de proteção contínua de dados (CDP) para todo o ambiente VMware com no mínimo os segu requisitos:

1.95.1. Não poderá impactar as VMs durante a execução da proteção contínua de dados (CDP);

1.95.2. Deverá proteger continuamente os dados das VMs do ambiente VMware e fornecer backup ou CDP (*continuous protection*) de baixo RPO (até 30 minutos) por meio de interface de administração java ou web.

1.96. Deverá suportar armazenamento nos cloud storages: Amazon S3, Microsoft Azure e Google Cloud Storage;

1.97. Deverá suportar a instalação do software de backup em Cloud instances;

1.98. Deverá suportar desduplicação de dados em Clouds a fim de reduzir o consumo de rede e armazenamento em nuvem, caso necessário o fornecimento de recursos adicionais de software, hardware e licenciamento os mesmos deverão constar detalhad proposta; podendo ser provida tanto por software quanto pelo appliance do item 3 e/ou pelo componente de software especificad item 1.7;

1.99. Deverá possuir a capacidade de gravar informações de catálogo nos backups enviados para, ao menos, Microsoft Azu Amazon S3;

1.100. Deverá possuir nativamente na console de gerenciamento unificado integração com módulos de proteção de dados workloads local;

1.101. Deverá permitir a orquestração de sistemas virtuais VMware de forma automatizada para recuperação de desastres co mínimo:

1.101.1. Permitir a recuperação de ambiente VMware para desastres orquestrada, automatizada e em escala para o próprio center, ambientes híbridos e multicloud;

1.101.2. Permitir a recuperação de ambiente VMware de forma automatizada e orquestrada para aplicativos de várias camad nuvem e no local com APIs ou interface própria para otimizar o tempo e os recursos;

1.101.3. Deverá ter a capacidade de testar a consistência do backup, emitindo relatório de auditoria ou efetuando teste recuperação por um plano de DR, para garantir a capacidade de recuperação seguintes parâmetros: sistema operac aplicação e máquina virtual;

1.101.4. Deve permitir a recuperação granular de desastres, ou seja, deverá ser possível realizar o *failover* e migraçã máquinas virtuais, aplicações individuais, um serviço composto por múltiplos componentes e até mesmo do site inteiro; pod ser provida tanto por software quanto pelo appliance do item 3 e/ou pelo componente de software especificado no item 1.7;

1.101.5. Deve possuir operações de resiliência incluindo: testes de recuperação/simulação, migrações, failover e failback;

1.101.6. Deve possuir funcionalidade para simulação de desastres, ou seja, permitir a verificação de uma operação de fai para o site secundário sem afetar o ambiente de produção no site principal; podendo ser provida tanto por software quanto appliance do item 3 e/ou pelo componente de software especificado no item 1.7;

1.101.7. Deve permitir a criação de planos de continuidade customizados para execução automatizada de uma sequênc passos para recuperação de desastres; podendo ser provida tanto por software quanto pelo appliance do item 3 e/ou componente de software especificado no item 1.7;

1.101.8. Deve permitir que seja configurado a execução de scripts customizados no plano de continuidade; podendo ser pr tanto por software quanto pelo appliance do item 3 e/ou pelo componente de software especificado no item 1.7;

1.101.9. Deverá permitir a restauração do ambiente VMware em grande escala caso o ambiente VMware de produção tenha comprometido, reduzindo assim o tempo de retorno e disponibilidade do ambiente VMware.

1.102. Deverá suportar controle de acesso baseado em função (RBAC);

1.103. Deverá permitir e estar licenciado o envio de dados desduplicados para a nuvem;

1.104. Deverá possibilitar a replicação para armazenamento seguro imutável, WORM (Write Once Read Many), com ima automaticamente prontas para recuperação, ou seja, caso o site primário tenha seus dados comprometidos, deverá ser pos replicar os dados do site secundário para o primário de forma automática, evitando assim erros com operações manuais; podend provida tanto por software quanto pelo appliance do item 3 e/ou pelo componente de software especificado no item 1.7;

1.105. Deverá suportar armazenamento seguro imutável, WORM (*Write Once Read Many*), para evitar que seus dados s criptografados, modificados ou excluído. E todos os dados salvos nessas instâncias deverão ser protegidos com as seguintes me de segurança, podendo ser provida tanto por software quanto pelo appliance do item 3 e/ou pelo componente de software especif no item 1.7;

1.105.1. Deverá garantir a funcionalidade WORM (Write Once Read Many) em todos os tipos de dados existentes no ambien CONTRATANTE, incluindo ambiente de servidores físicos, virtuais e nuvem; podendo ser provida tanto por software quanto appliance do item 3 e/ou pelo componente de software especificado no item 1.7;

1.105.2. Deverá garantir a proteção das cópias de backup para que elas sejam somente leitura e não possa ser modifi corrompida ou criptografada após o backup; podendo ser provida tanto por software quanto pelo appliance do item 3 e/ou componente de software especificado no item 1.7;

1.105.3. Deverá garantir a propriedade da imagem de backup e não ser possível excluir antes da expiração dos dados; pod ser provida tanto por software quanto pelo appliance do item 3 e/ou pelo componente de software especificado no item 1.7;

1.105.4. Deverá possuir detecção de anomalias no site principal de produção;

1.105.5. Deverá possuir mecanismos de proteção contra *ransomware*, devendo, mas não se limitando a:

1.105.5.1. Deverá possuir detecção de anomalias;

1.105.5.2. Deverá permitir a exclusão do backup em caso de uma anomalia encontrada.

1.105.6. Detecção e alerta sobre mudanças inesperadas nos dados de backup, com no mínimo os seguintes metadados, atribut recursos da tarefa de backup:

1.105.6.1. Tamanho da imagem de backup;

1.105.6.2. Taxa de desduplicação;

1.105.6.3. Tempo de conclusão do trabalho de backup.

1.106. Qualquer desvio incomum nesses atributos de trabalho de backup deverá ser considerado uma possível anomalia notific por meio de console WEB e REST-API;

1.107. Deverá suportar o backup e o restore de diferentes sistemas operacionais tais como:

1.107.1. Windows (8/10/2012/2012 R2/2016/2019/2022);

1.107.2. Oracle Linux (7 e 8);

1.107.3. Red Hat Enterprise Linux (7 e 8);

1.107.4. Suse Enterprise Server (12 e 15);

1.107.5. Oracle Solaris (11);

1.107.6. AIX (7.1 e 7.2);

1.107.7. Ubuntu (16, 18 e 20).

1.108. Deverá suportar ambientes virtuais como VMware vSphere (6.7 e superiores) e Hyper-V (2012/2016/2019);

1.109. Para ambientes com VMware vSphere devrá ser comprovadamente compatível com o VADP (vStorage API for Data Protec para realizar operações de Backup e Restore de ambientes VMware versão 6.5 e superior;

1.110. Para ambientes Microsoft Hyper-V, deverá suportar Microsoft Hyper-V Server 2012/R2, Microsoft Hyper-V Server 20 Microsoft Hyper-V Server 2019;

1.111. Deverá suportar VMware vCloud, possuindo integração com vCloud Director API possibilitando backup automático das máq virtuais e recuperação completa;

1.112. Possuir suporte a backup e restore de máquinas virtuais VMware 6.5 ou superior através de vStorage API com as segu características:

1.113. Deverá permitir que através de uma única rotina de Backup a qual enviou os seus dados para disco ou tape seja pos recuperar a imagem completa da máquina virtual Windows e Linux (vmdk), e também arquivos de maneira granular se necessidade de scripts, área temporária ;

1.114. Deverá suportar o uso da funcionalidade CBT (Change Block Tracking) para as operações de backup;

1.115. Deverá permitir a recuperação granular de arquivos através da execução de um único backup;

1.116. Deve permitir o descobrimento automático das máquinas virtuais nos ambientes VMware, com capacidade de realizar 8 avançados com critérios que incluam pelo menos:

1.116.1. Nome da máquina virtual;

1.116.2. vApp;

1.116.3. Tag name.

1.117. Deverá possuir a capacidade de balanceamento de carga automática dos backups através de múltiplos backups hosts;

1.118. Deverá suportar VMware vSphere 6.5 ou superiores;

1.119. Deverá permitir restaurar e iniciar a execução de uma máquina virtual instantaneamente, diretamente a partir do repositório de backup, sem a necessidade de manter réplicas ou snapshots disponíveis para o processo de recuperação instantâne

1.120. Prover backup e recursos, permitindo que somente blocos utilizados sejam copiados no processo de backup;

1.121. Permitir realizar restauração, através de um único backup, de Máquina virtual completa ou arquivos de dentro da máq virtual para ambientes Windows e Linux;

1.122. Possuir a capacidade de restaurar a VM de origem em um ponto no tempo enviando apenas a diferença dos blocos entre de origem e imagem de backup para ambiente VMware através da integração com o VADP;

1.123. Deverá permitir a visualização, monitoração e recuperação de máquinas virtuais através de plugin integrado ao vCent vSphere 6.5 Web Client ou superior;

1.124. Deverá possuir capacidade de realizar backup de maneira off-host, sem a necessidade de instalação de agentes nas máq virtuais;

1.125. Deverá possuir capacidade de realizar backup de máquinas virtuais em estado online e offline;

1.126. Deverá possuir a capacidade de movimentação dos dados de backup e restore através de SAN e LAN utilizando os métod transporte SAN (LAN-free), NBD e HotAdd;

1.127. Deverá possuir a capacidade de realizar backup de máquinas virtuais existentes em um vApp;

1.128. Deverá possuir a capacidade de recuperação da imagem da máquina virtual, para máquinas que possuam discos VMFS ou F

1.129. Deverá suportar integração com vCloud Director API possibilitando backup automático das máquinas virtuais e recuper completa;

1.130. Deverá suportar a recuperação de máquinas virtuais que utilizem identificadores do tipo: hostname, display name;

1.131. Deverá possuir a funcionalidade de restauração instantânea de várias máquinas virtuais do ambiente VMware simultanean a partir de uma imagem de backup, garantindo assim uma rápida recuperação do ambiente em caso de desastre;

1.132. Deverá ser possível recuperar uma máquina virtual várias vezes de pontos de recuperação diferentes;

1.133. Possuir suporte a backup e restore de máquinas virtuais Hyper-V, com as seguintes características:

1.133.1. Deverá possuir a capacidade de realizar backup On-Host e off-host das máquinas virtuais Windows e Linux;

1.133.2. Deverá possuir a capacidade de realizar backup de maneira Full, Incremental ou Diferencial sem a necessidad instalação de agentes nas máquinas virtuais;

1.133.3. Deverá suportar ambientes configurados com Cluster Shared Volumes;

1.133.4. Deverá permitir que através de uma única rotina de Backup a qual enviou os seus dados para disco ou tape seja pos recuperar a imagem completa da máquina virtual Windows e Linux (vhd), e também arquivos de maneira granular s necessidade de scripts, área temporária ou montagem dos arquivos vhd;

1.133.5. Deverá possuir a capacidade de recuperação das máquinas virtuais para uma área temporária de disco;

1.133.6. Deverá suportar Microsoft Hyper-V 2012, 2016 e 2019.

1.134. Deverá suportar os seguintes bancos de dados, utilizando agente específico:

1.134.1. Microsoft SQL Server versões 2012, 2014, 2016, 2017 e 2019;

1.134.2. Oracle/Oracle RAC versões 11g, 12c, 18c, 19c e 21c;

1.134.3. Microsoft Exchange 2013, 2016 e 2019;

1.134.4. Microsoft Sharepoint 2013, 2016 e 2019;

1.134.5. MySQL 5 e 8;

1.134.6. PostgreSQL 9, 10, 11, 12 e 13;

1.134.7. MariaDB 10;

1.134.8. SAP e SAP HANA;

1.134.9. Microsoft Active Directory.

1.135. Deverá suportar backup do Oracle Database, incluído arquitetura Oracle RAC, através da integração com RMAN;

1.136. Deve suportar backup e restore via Agentes Linux para arquiteturas Oracle Real Application Clusters (RAC);

1.137. Deverá manter a sincronia entre os catálogos de backups do Oracle RMAN e da solução ofertada;

1.138. Deverá suportar Apache Hadoop e Apache HBase;

1.139. Deverá suportar DAG (DataBase Availability Groups) do MS Exchange;

1.140. Deverá suportar backup do Information Store de Microsoft Exchange, com possibilidade de restore granular, ou seja, de e-m únicos, itens de calendário e também de caixa postal de algum usuário;

1.141. Deverá suportar backup do Microsoft Active Directory, com possibilidade de restore granular;

1.142. Deverá suportar backup completo do Sharepoint, com possibilidade de recuperação de uma ou mais databases, docume individuais, sites, subsites, listas e itens/documentos individuais;

1.143. Deverá permitir o backup e restauração nativamente de aplicativos Kubernetes com no mínimo as seguintes caracterís podendo ser utilizado módulo/interface adicional de software para backup em disco com desduplicação:

1.143.1. Deverá suportar proteção nativa de ambientes Kubernetes integrado com o software de backup;

1.143.2. Permitir backup e restauração de aplicativos Kubernetes na forma de namespaces;

1.143.3. Configuração do cluster Kubernetes e gerenciamento seguro de credenciais;

1.143.4. Descoberta automática e sob demanda de ativos do Kubernetes;

1.143.5. RBAC na granularidade do cluster e nível de namespace;

1.143.6. Backups baseados em plano de proteção em nível de namespace;

1.143.7. Opções de recuperação versáteis, como namespace completo, um recurso personalizado individual ou um vo persistente individual;

1.143.8. Gerenciamento do ciclo de vida da imagem com retenção e limpeza personalizáveis;

1.143.9. Deverá possuir descoberta inteligente e automática de ativos;

1.143.10. Deverá permitir executar backups baseados em snapshot sem a utilização de agentes.

1.144. Deverá possuir controle de fluxo de recursos e recuperação de local alternativo;

1.145. Deverá prover relatórios gerenciais de backup com no mínimo as seguintes informações:

1.145.1. Backups com sucesso;

1.145.2. Backups com falha;

1.145.3. Volumetria de backup realizado;

1.145.4. Restore com sucesso;

1.145.5. Restores com falha;

1.145.6. Volumetria de restore realizado;

1.145.7. Clientes de backup configurados;

1.145.8. Ocupação no destino de backup;

1.145.9. Licenciamento e capacidade.

1.146. Possuir interface web para gerenciamento, monitoramento, emissão de alertas, emissão de relatórios sobre operaçõe backup e restore e emissão de relatórios, com as seguintes características:

1.146.1. Relatórios sobre capacidade e tendência de crescimento do ambiente;

1.146.2. Se houver múltiplos ambientes de backup, com independência operacional e localizados em diferentes Data Cer deverá possuir nativamente uma única interface web deverá ser capaz de monitorar e agregar informações de diversos Servi da Camada de Gerenciamento para emissão dos relatórios;

1.146.3. Relatórios para verificar o nível de serviço, ou seja, visualização de que aplicações estão com políticas de backup ati e executadas periodicamente;

1.146.4. Deverá permitir exportar relatórios;

1.146.5. Base de dados de relatórios para suportar armazenamento de dados históricos superior a 30 dias.

2. Subscrição de Solução de Backup para o Microsoft 365

2.1. Deverão ser fornecidas licenças no modelo de subscrição para 4.000 (quatro mil) usuários, incluindo todas as funcionalic solicitadas para proteção de dados do Microsoft Office 365;

2.2. Para fins de licenciamento, deverão ser considerados apenas usuários ativos e com licença da Microsoft aplicada;

2.3. A solução de Proteção de Dados a ser ofertada deve atender integralmente os requisitos especificados neste Termo, devend fornecida com todas as licenças e infraestrutura que forem necessárias para entrega funcional da solução;

2.4. Deverá ser fornecido backup e recuperação para Exchange Online, OneDrive, SharePoint Online e Teams, bem como lo auditoria do 365;

2.5. Deverá possibilitar exportar dados para o formato PST;

2.6. Deverá prover a proteção das cargas de trabalho por meio de conexões seguras;

2.7. Deverá ser possível definir o escopo e a programação do backup de acordo com as necessidades da CONTRATANTE;

2.8. Deverá após a implementação permitir que os backups sejam agendados automaticamente;

2.9. Deverá suportar recuperações completas e granulares em vários níveis;

2.10. Deverá ser possível recuperar o dado no local, em um local novo ou alternativo, por meio do Microsoft 365 ou para de externo;

2.11. Deverá prover monitoramento do status e cobertura de backup;

2.12. Deverá preservar dados para casos de litígio de acordo com a política especificada;

2.13. Deverá ser possível pesquisar por metadados, tais como nomes de usuário, arquivos, pastas e datas;

2.14. Deverá manter os dados seguros com criptografia AES de 256 bits integrada;

2.15. Deverá prover segurança e com restrições de IPs;

2.16. Deverá ser possível consultar e relatar o histórico de atividades dos usuários;

2.17. Deverá ser possível aplicar períodos de retenção imutáveis;

2.18. Deverá ser possível selecionar regiões de hospedagem em território nacional;

2.19. Deverá prover controle de acesso baseado em função, sendo possível configurar e controlar os acessos de vários tipo usuários com no mínimo, as seguintes opções:

2.19.1. Papéis de acesso pré-definidos;

2.19.2. Papéis de acesso customizados.

2.20. Deverá ser oferecida no modelo SaaS (Software como serviço) pelo fabricante, não necessitando de nenhuma infraestrutura ou IaaS (Infraestrutura como serviço) para seu pleno funcionamento;

2.21. Toda a infraestrutura de hardware, software e prestação de serviço na nuvem deverão ser fornecidos pela CONTRATADA, ou a CONTRATANTE irá contratar o serviço e toda a infraestrutura necessária será de responsabilidade da CONTRATADA;

2.22. Nos casos de replicações para locais externos (On-premise ou nuvem), a infraestrutura de destino é de responsabilidad CONTRATANTE;

2.23. Deverá possuir integração nativa com o software para proteção de dados, provendo console de monitoramento centralizado;

2.24. Deverá prover até 3 (três) cópias locais de segurança em ambiente Cloud, garantindo a salvaguarda dos dados em cas falhas de hardware e garantindo a disponibilidade do mesmo;

2.25. O fabricante da solução de proteção de dados para Microsoft 365 deverá comprovar através de documentações ofici segurança física e lógica de seus data centers assim como a garantia da privacidade dos dados;

2.26. O fabricante da solução de proteção de dados para Microsoft 365 deverá entregar tal proteção na modalidade SaaS (Soft como Serviço) e comprovar através de documentações oficiais;

2.27. Deverá proteger as cargas de trabalho por meio de conexões seguras;

2.28. Deverá permitir definir o escopo e o agendamento do backup de acordo com as necessidades e politicas de retençã CONTRATANTE;

2.29. Deverá adicionar os usuários novos nas políticas de backups programados automaticamente;

2.30. Deverá permitir recuperar o dado no local, em um local novo ou alternativo, através do Microsoft 365, ou para destino extern

2.31. Deverá ser possível monitorar e relatar o status e cobertura do backup;

2.32. Deverá possuir funcionalidade que garanta a segurança dos dados com criptografia AES de 256 bits integrada, fim a fim;

2.33. Deverá possuir integração do Azure AD ou similar de outras clouds públicas;

2.34. Deverá possuir a funcionalidade para restringir os IPs, garantindo que somente os IPs cadastrados terão acesso;

2.35. Deverá possuir logs de auditoria que seja possível consultar e relatar os históricos de atividades de usuários e processo sistema;

2.36. Deverá preservar dados para casos de litígio;

2.37. Deverá ser possível criar e gerenciar casos para litígio e privacidade de dados;

2.38. Deverá ser possível pesquisar por nomes de usuário, arquivos, pastas e datas;

2.39. Deverá ser possível aplicar políticas de retenção e garantir que os dados estarão imutáveis;

2.40. Deverá ser possível selecionar regiões de hospedagem, sendo pelo menos 1 data center no Brasil;

2.41. Deverá possuir até 3 (três) cópias com réplicas síncronas de dados para alta disponibilidade dos dados;

2.42. Deverá possui uma console de gerenciamento acessível via web browser;

2.43. Suportar controle de acesso com “single sign-on” via AD FS 2.0 ou Azure AD ou similar de outras clouds públicas;

2.44. Suportar duplo fator de autenticação para acesso a console;

2.45. Deve suportar Single-Tenant para salvaguarda dos dados de backup da Contratante;

2.46. Suportar proteção de dados de, no mínimo, os seguintes itens do Microsoft 365:

2.46.1. E-mail;

2.46.2. Calendário;

2.46.3. Contatos;

2.46.4. Tarefas;

2.46.5. Notas;

2.46.6. OneDrive;

2.46.7. Arquivos;

2.46.8. Pastas;

2.46.9. Permissões;

2.46.10. SharePoint Online (Qualquer tipo de conteúdo dos sites, incluindo permissões e todos os metadados);

2.46.11. Teams;

2.46.12. Sites de equipes;

2.46.13. Membros;

2.46.14. Permissões de membros;

2.46.15. Canais;

2.46.16. Postagens;

2.46.17. Arquivos;

2.46.18. Wiki.

2.47. Realizar a imagem (backup) do ambiente Microsoft 365, no mínimo, de 2 vezes ao dia;

2.48. Deverá reter as imagens (backup) por todo período de subscrição sem custo adicional;

2.49. Deverá incluir novos usuários automaticamente, dentro da quantidade de licenças contratadas;

2.50. Deve suportar operação de recuperação das informações protegidas;

2.51. Disponibilizar, no mínimo, as seguintes formas de recuperação dos dados:

2.51.1. Recuperação para o local de origem;

2.51.2. Novo local ou alternativo, através do M365;

2.51.3. Fazer download do arquivo.

2.52. Disponibilizar logs de auditoria para as operações de descoberta legal, auditorias e investigações com pelo menos:

2.52.1. Administrador - Todas as atividades realizadas por usuários administrativos e privilegiados no portal de administração;

2.53. Deverá suportar funcionalidade de criptografia durante todo o processo de proteção dos dados;

2.54. A solução deverá suportar salvaguardar os dados em diferentes regiões e domínios na Cloud;

2.55. Deverá suportar a proteção dos metadados;

2.56. Deverá suportar restore granular para local de origem dos dados e demais destinos alternativos;

2.57. Suportar auditoria;

2.58. Suportar MFA2 - Múltiplo fator de autenticação;

2.59. Suportar role-based access control (RBAC);

2.60. Deve suportar retenções ilimitadas de backup durante o período contratado;

2.61. Deve suportar imutabilidade dos dados

2.62. Suportar regras de permitido/bloqueado por endereçamento IP;

2.63. Suportar Point-in-time restore;

2.64. Suportar criptografia fim a fim de no mínimo 256 Bits.

3. Appliance de Backup para Armazenamento de Dados para Curta Retenção

3.1. Deverá obrigatoriamente ser fornecida solução de armazenamento de dados de backup em disco, baseado em “Appliance”, qu define por subsistema específico de ingestão e tratamento de dados de backup, por meio de tecnologias de desduplicação, replica segurança da informação. A solução deve possuir console de gerenciamento unificado com base de catálogo, funcionalidade movimentação de dados através de gerenciadores de mídia, e requisitos de segurança e proteção;

3.2. Para atendimento dos requisitos técnicos no presente termo visando plena interoperabilidade e segurança dos dados de ba não serão aceitas soluções tradicionais de armazenamento de dados baseado em Storages, servidores com discos internos e solu de hiperconvergência;

3.3. Não serão aceitas soluções baseadas em (Virtual Appliance) e dispostas sob Hypervisors;

3.4. Não serão aceitas soluções de Appliance baseadas em arquiteturas de referência compostas por servidores x86, que não s fornecidas pelo mesmo fabricante da solução de software de backup ofertada;

3.5. Todos os componentes da solução deverão ser fornecidos pelo mesmo fabricante. Serão aceitos também soluções que, de f exclusiva, o software e o hardware sejam OEM (*Original Equipment Manufacturer*) licenciado, com part number próprio PROPONENTE fabricante, e com a devida autorização, bem como a comercialização do produto do próprio de forma pública;

3.6. Deverá ser fornecido no mínimo, 70 TB de capacidade considerando base 2 (1 TB igual a 1024 gigabytes) em RAID-6, considerar ganhos com desduplicação e compressão de dados;

3.7. Será permitido a utilização de até 10% da área de armazenamento seja utilizada para armazenar dados de controle, ponteir desduplicação, sistema operacional, catálogo, replicação e quaisquer outros dados;

3.8. O appliance deve suportar taxa de ingestão de dados de, no mínimo 57 TB/hora, considerando a desduplicação de dad origem (client-side);

3.9. Para atendimento dos requisitos de performance sem degradação, será admitida apenas a composição de Appliances do m modelo e versão, visando atingir a taxa de ingestão;

3.10. Deverá ser novo, sem uso, e constar no site do fabricante como um appliance de backup em disco em linha de produção atu

3.11. Deverá ser do mesmo fabricante do software de proteção de dados para a solução ofertada, garantindo total interoperabili entre o hardware e software de backup, devendo ser comprovado através de documentação oficial;

3.12. Permitir a utilização de todas as funcionalidades, tecnologias e recursos especificados, irrestrita e sem necessidad licenciamentos ou ônus adicionais;

3.13. Deve ser composto, de processamento, portas de conectividade e armazenamento integrado, dedicado única e exclusivame

execução das atividades ingestão, desduplicação e replicação dos dados;

3.14. Possuir interface de administração GUI e CLI;

3.15. Possuir mecanismo de proteção dos dados armazenados, através de RAID (Redundant Array of Independent Disks) de for suportar a falha simultânea de no mínimo dois discos, sem interrupção do serviço. A solução deve ser dimensionada e configurada suportar a perda de qualquer componente sem impacto para o serviço;

3.16. Possuir discos de Hot Spare para o appliance e gavetas de expansão de disco da solução, sem necessidade de intervenção p manual;

3.17. Permitir a substituição dos componentes redundantes sem interrupção do serviço (*hot swapping*);

3.18. Possuir ao menos 512 GB de memória, permitindo expansão. Não serão aceitas como memória a utilização de tecnologias F SSD ou qualquer outra tecnologia de extensão de cache;

3.19. Possuir no mínimo: 4 (quatro) portas 1GbE (um gigabit ethernet Base-T), 04 portas 25Gb SFP (vinte e cinco gigabit ethernet (quatro) portas de 16Gb FC (Fibre Channel) para interconexão e integração com os servidores clientes;

3.20. A replicação de dados de backup entre appliances deverá suportar tecnologia de otimização para economia de largura de b do link;

3.21. Deverá suportar replicação dos dados em disco para outro appliance. A replicação deverá ser assíncrona e ocorrer em pe gerenciado pelo software de backup;

3.22. Deverá ser fornecido licenciamento para replicação dos dados armazenados no dispositivo de armazenamento para dispositivo de mesma categoria e nuvem em formato desduplicado;

3.23. Deverá permitir que o software de proteção de dados seja executado diretamente no appliance, garantindo interoperabilidade entre hardware e software;

3.24. Caso não seja suportado a instalação do software de backup diretamente no appliance, a CONTRATADA deverá fornecer todo recursos de software, hardware e licenciamento para atender ao requisito técnico. Não será permitido a utilização de recurso infraestrutura existente na CONTRATANTE;

3.25. Deve possuir tecnologia de proteção contra ataques de sequestro de dados (ransomware attack), diretamente no appli Todos os recursos complementares para atendimento do requisito técnico, dos quais: hardware, software e licenciamento deven fornecidos;

3.25.1. Deve possuir recursos de imutabilidade dos dados através de Write Once Read Many – WORM garantindo a imutabili para todo e qualquer dado de backup enviado para armazenamento no appliance, sendo este de produção ou outro appli complementar e necessário a arquitetura;

3.25.2. Deverá possuir funcionalidade de criptografia dos backups em no mínimo 256 bits;

3.25.3. Deverá suportar imutabilidade de dados, considerando os repositórios de backup integrados e gerenciados pelo applia

3.26. Deve exigir a autenticação dupla (2FA-Two Factor Authentication);

3.27. Deverá ser bloqueado qualquer usuário root ou administrador com acesso ao sistema operacional do appliance;

3.28. O relógio de conformidade de retenção deverá ser independente do relógio do sistema operacional para evitar, em cas ataque cibernético, a alteração do relógio do sistema operacional e a expiração das cópias de backup , ou seja, deverá suportar W SEC Rule 17a-4;

3.29. O Appliance deverá possuir a funcionalidade de configurar servidor de gerência e catálogo e gerenciador de mídia repositório de dados de backup num mesmo equipamento, facilitando assim as atividades de instalação, atualização e gerenciam da solução; Será facultado a utilização de servidores externos para suprir essa necessidade sem custos adicionais ao Contratante;

3.30. Deverá permitir apenas imagens do sistema operacional assinaladas e desenvolvidas pelo próprio fabricante, evitando assim um ataque cibernético corrompa ou substitua o sistema operacional do appliance;

3.31. Deverá permitir a implementação da função de segurança RBAC;

3.32. Deverá possuir uma única console gráfica de gerenciamento para todos os appliances, permitindo monitorar e administr recursos dos equipamentos além de possibilitar que sejam realizados upgrades e aplicações de patches;

3.33. Deverá implementar a conformidade ao Guias Técnicos de Implementação de Segurança (STIGs) que fornecem orienta técnicas para aumentar a segurança dos sistemas e software para ajudar a prevenir ataques malicioso com no mínimo os segu requisitos:

3.33.1. Deverá implementar conformidade de senhas seguras, não permitindo utilização de senhas fáceis ou sequenciais;

3.33.2. Deverá reduzir os privilégios da conta do usuário root;

3.33.3. Deverá habilitar a auditoria para operações de baixo nível, como comandos do sistema operacional e chamada sistema;

3.33.4. Deverá desativar a opção de reinicializar Ctrl-Alt-Delete;

3.33.5. Deverá desabilitar o login root para SSH;

3.33.6. Deverá bloquear a conta por no mínimo 15 minutos após três tentativas de login incorretas;

3.33.7. Deverá implementar o fator duplo de autenticação SAML ou similar;

3.33.8. Deverá implementar criptografia segura TLS1.2, durante o tráfego dos dados (in-transit) e no armazenamento (at-rest todos os backups, restaurações, replicação automática de imagens e desduplicação;

3.33.9. Deverá possuir o padrão FIPS 140-2 que especifica os requisitos de segurança e criptografia;

3.33.10. Deverá permitir o bloqueio proativo de comportamentos indesejados de acesso a recursos antes que eles possar acionados pelo sistema operacional do appliance;

3.33.11. Deverá permitir o bloqueio de acesso aos binários do sistema operacional do appliance, exceto por aplicativos, usuá grupos de usuários identificados e confiáveis;

3.33.12. Deverá possuir recurso que bloqueie ou seja aprovado por mais de uma função ou setor o appliance de executar redefinição de armazenamento (redefinição de fábrica / nova imagem permitida) evitando que um ataque cibernético exe essa função para expirar todos os dados de backup.

3.34. Deverá permitir a verificação de integridade de dados para garantir que as restaurações de dados sejam bem-sucedidas;

3.35. Deverá permite a conexão do appliance diretamente com a TAPE utilizando portas Fibre Channel, funcionalidade conhecida c tape-out; ou que essa integração seja feita pelo software de backup;

3.35.1. Caso não seja suportado a funcionalidade conhecida como Tape-Out diretamente no appliance, a CONTRATADA de fornecer todos os recursos de software, hardware e licenciamento para atender ao requisito técnico. Não será permiti utilização de recursos de infraestrutura existente na CONTRATANTE.

3.36. Os componentes de FAN e power supply devem ser redundantes;

3.37. Permitir o uso de compartilhamento da área de armazenamento com suporte a desduplicação a qualquer plataforma funcionalidade CIFS ou NFS;

3.38. Permitir o uso de compartilhamentos NFS para proteção de bancos de dados Oracle com a utilização do Oracle RMAN, co seguintes características:

3.38.1. Permitir a gravação dos dados a partir do servidor Oracle diretamente via RMAN em um compartilhamento NF appliance;

3.38.2. O produto do backup estará disponível para restauração diretamente no RMAN, utilizando os dados disponíveis no dis appliance;

3.38.3. Permitir que a os dados copiados diretamente do RMAN sejam duplicados em cópias complementares para disco.

3.39. Permitir replicar os dados através de rede IP (WAN/LAN);

3.40. Suportar os protocolos IPv4 e IPv6;

3.41. Possuir auto suporte do tipo call home para seus componentes de hardware e software, tais como: CPU, disco, f ventiladores, temperatura, capacidade de utilização, firmware, entre outros;

3.42. Permitir sua instalação em rack padrão 19'';

3.43. Possuir alimentação elétrica por fontes internas ao equipamento, redundantes e hot-swappable, com faixa de operação de te de entrada compreendida, no mínimo, entre 200V a 240V, monofásica (P+N+T), com seleção automática ou manual por meio de c seletora de tensão, devendo obedecer ao padrão IEC 320 C13-C14 ou similar que utilize plugues no padrão C14;

3.44. Prover 'software' para total gerenciamento, administração e configuração do sistema de forma local ou remota, que perm também a análise de desempenho e implementação das políticas de segurança física, lógica, e de acesso de usuários;

3.45. Possuir todos os acessórios necessários para a plena configuração, operacionalização, utilização e gerenciament equipamento;

3.46. Os softwares, drives e firmwares necessários devem estar em suas últimas versões;

3.47. Não serão aceitas soluções compostas por componentes de fabricantes diferentes;

3.48. Possuir tecnologia de desduplicação de dados, ou seja, não armazenar mais de uma vez dados que sejam duplicados;

3.49. A desduplicação deve segmentar automaticamente os dados em blocos de tamanho fixo e/ou variável;

3.50. A funcionalidade de desduplicação de dados deverá ser executada inline com a ingestão dos dados, ou seja, deverá acon antes dos dados serem gravados nos discos, eliminando a necessidade de armazenamento intermediário para cache dos dados;

3.51. A desduplicação deve ser global, ou seja, identificar dados duplicados tanto do mesmo servidor-cliente de origem do ba como outros servidores-cliente armazenados no mesmo dispositivo de backup, armazenando na solução somente blocos de d únicos;

3.52. Permitir o envio de dados desduplicados para a nuvem pública, privada ou híbrida. Todos os recursos adicionais necessário licenciamento de software e hardware devem ser fornecidos para atender a volumetria total de dados a ser protegida, e const proposta técnica o detalhamento dos produtos;

3.53. Permitir suporte à replicação dos dados no formato desduplicado, com controle e atualização do catálogo do aplicativ backup.

4. Expansão do Appliance de Backup para Armazenamento de Dados para Curta Retenção

4.1. Possuir, no mínimo, 60 TB (sessenta terabytes) de capacidade utilizável, considerando base 2 (1 TB igual a 1024 gigabytes RAID-6 e sem considerar ganhos com desduplicação e compressão de dados;

4.2. Deve ser novo, sem uso, e constar no site do fabricante como uma expansão de appliance de backup em disco em linh produção atual;

4.3. Deve obrigatoriamente ser compatível com o Appliance de backup para armazenamento de curta retenção do ITEM 3, qu entende como um subsistema com o propósito específico de ingestão dos dados de backup para armazenamento de curta rete com desduplicação e replicação;

4.4. Permitir a utilização de todas as funcionalidades, tecnologias e recursos especificados, irrestrita e sem necessidad licenciamentos ou ônus adicionais;

4.5. Possuir mecanismo de proteção dos dados armazenados, seja através de RAID (*Redundant Array of Independent Disks*) de for suportar a falha simultânea de no mínimo dois discos quaisquer, sem interrupção do serviço. A solução deve ser dimensiona configurada para suportar a perda de qualquer componente sem impacto para o serviço;

4.6. Possuir discos Hot Spare para o appliance e gavetas de expansão de disco da solução, sem necessidade de intervenção p manual;

4.7. Permitir a substituição dos componentes redundantes sem interrupção do serviço (hot swapping);

4.8. Permitir sua instalação em rack padrão 19'';

4.9. Possuir alimentação elétrica por fontes internas ao equipamento, redundantes e hot-swappable, com faixa de operação de te de entrada compreendida, no mínimo, entre 200V a 240V, monofásica (P+N+T), com seleção automática ou manual por meio de c seletora de tensão, devendo obedecer ao padrão IEC 320 C13-C14 ou similar que utilize plugues no padrão C14;

4.10. Possuir todos os acessórios necessários para a plena configuração, operacionalização, utilização e gerenciament equipamento, sem necessidade de aquisições futuras de licenças ou softwares de ativação;

4.11. Os softwares, drives e firmwares necessários devem estar em suas últimas versões;

4.12. Não serão aceitas soluções compostas por componentes de fabricantes diferentes;

4.13. tecnologia de desduplicação de dados, ou seja, não armazenar mais de uma vez dados que sejam duplicados;

4.14. A desduplicação deve segmentar automaticamente os dados em blocos de tamanho fixo e variável;

4.15. A funcionalidade de desduplicação de dados deverá ser executada em linha com a ingestão dos dados, ou seja, deverá acon antes dos dados serem gravados nos discos, eliminando a necessidade de armazenamento intermediário para cache dos dados;

4.16. A desduplicação deve ser global, ou seja, identificar dados duplicados tanto do mesmo servidor-cliente de origem do ba como outros servidores-cliente armazenados no mesmo dispositivo de backup, armazenando na solução somente blocos de d únicos;

4.17. O equipamento deverá ser configurado em alta disponibilidade, portanto ser composto de no mínimo 2 (dois) nós configu como cluster ativo/ativo, ou ativo/passivo ou seja, na eventualidade de queda de um nó, o outro deverá manter as atividade movimentador de dados de Backup sem paradas.

5. Appliance de Backup ou Objeto para Armazenamento de Dados para Longa Retenção

5.1. Possuir, no mínimo, 600 TB (seiscentos terabytes) de capacidade utilizável considerando base 2 (1 TB igual a 1024 gigabytes RAID-6, sem considerar ganhos com desduplicação e compressão de dados;

5.2. Deve fazer uso de sistemas de armazenamento de Backup em disco ou objeto, baseado em "Appliance", que se entende com subsistema de ingestão dos dados desduplicados para armazenamento de dados de longa retenção e replicação;

5.3. O "Appliance" deve ser composto, de processamento e armazenamento integrado para ingestão de dados desduplicad replicação;

5.4. Deve ser novo, sem uso, e constar no site do fabricante como um Appliance de Backup em disco para armazenamento de dad longa retenção em linha de produção atual;

5.5. Deve ser possuir compatibilidade, comprovada através de documentação oficial do fabricante, com o software de backup ofer garantindo total integração entre o hardware e software de Backup, permitindo a utilização de todas as funcionalidades e garan assim o desempenho, segurança e a estabilidade desejada para o ambiente;

5.6. Permitir a utilização de todas as funcionalidades, tecnologias e recursos especificados, irrestrita e sem necessidad licenciamentos ou ônus adicionais;

5.7. Deve ser composto, de processamento, portas de conectividade e armazenamento integrado, dedicado única e exclusivamer execução das atividades ingestão, armazenamento dos dados desduplicados e replicação dos dados;

5.8. O equipamento deverá ser configurado em alta disponibilidade, portanto ser composto de no mínimo 2 (dois) nós configu como cluster ativo/ativo, ou seja, na eventualidade de queda de um nó, o outro deverá manter as atividades de movimentad dados de Backup sem paradas;

5.9. Deverá possuir gerenciamento de falhas e alarmes embarcado no próprio "Appliance", não devendo utilizar servidores exte para tais funcionalidades;

5.10. O sistema de armazenamento deve permitir replicar os dados através de rede IP (WAN/LAN);

5.11. O sistema de armazenamento deve permitir suporte à replicação dos dados no formato desduplicado;

5.12. A solução deve verificar constantemente e automaticamente os dados armazenados, sem a utilização de scripts e composições feitas exclusivamente para esse órgão;

5.13. Deve possuir interface de administração WEB GUI e CLI;

5.14. O sistema de armazenamento deverá suportar tecnologia RAID ou Erasure Code para proteção de falhas em disco;

5.15. O Sistema de armazenamento de Backup disco deverá conter disco de "hot spare" ou área definida para a proteção dos d caso ocorra perda de um disco; O disco de "hot spare" será usado para substituir e reconstruir automaticamente o dado de Backup

5.16. Permitir a substituição dos componentes redundantes sem interrupção do serviço (hot swapping);

5.17. O sistema de armazenamento de Backup ou objeto deve ser escalável à no mínimo 2,5 PB (dois e meio Petabytes) úteis, considerar ganhos com desduplicação e compressão de dados;

5.18. Deve ser fornecido com no mínimo 1 (uma) porta de 1 GB (um gigabit) Ethernet para monitoramento, 4 (quatro) portas 1 (dez gigabit ethernet fibra) ou 25GbE (vinte e cinco gigabit ethernet fibra) para interconexão e integração com os servidores client

5.19. Deve possui pelo menos 2 (duas) CPUs 10-core cada (dez cores cada CPU) totalizando um mínimo de 20 (vinte) cores;

5.20. O sistema de armazenamento de Backup deve possuir no mínimo 768GB (setecentos e sessenta e oito gigabytes) de mer RAM;

5.21. Deve suportar a tecnologia de imutabilidade ou WORM (*write once ready many*) para armazenamento dos dados de Backup;

5.22. O sistema de armazenamento deverá suportar protocolos Amazon S3, CIFS e NFS;

5.23. Os componentes de controladoras RAID, FAN e power supply devem ser redundantes;

5.24. Não serão aceitas soluções compostas por componentes de fabricantes diferentes e/ou que não estejam homologad fornecidas pelo próprio fabricante do appliance e/ou objeto.

5.25. Todos os componentes de hardware da solução deverão possuir fontes de alimentação redundantes;

5.26. Todos os equipamentos devem ser montáveis em rack padrão 19'';

5.27. Deve suportar armazenamento via LAN e WAN, sem a necessidade de adquirir outras soluções para as localidades remotas;

5.28. Possuir alimentação elétrica com fontes internas ao equipamento, redundantes e hot-swappable;

5.29. Os equipamentos fornecidos deverão prover 'software' de administração e gerenciamento para total administraç configuração do sistema de forma local ou remota, que permitam também a análise de desempenho e implementação das polític segurança física, lógica, e de acesso de usuários;

5.30. A solução deve ser fornecida com todos os acessórios necessários para a plena configuração, operacionalização, utiliza gerenciamento do equipamento, sem necessidade de aquisições futuras de licenças ou softwares de ativação, tais como:

5.31. Softwares e manuais necessários para o gerenciamento;

5.32. Os softwares, drives e firmwares necessários devem estar em suas últimas versões;

5.33. Cabos lógicos de gerenciamento/console;

5.34. Cabos de energia elétrica padrão IEC 320 plug C13/C14 e IEC 320 C14/C19;

5.35. Possuir licença para replicação dos dados armazenados no dispositivo de armazenamento para outro dispositivo de m natureza em formato desduplicado;

5.36. Deve possuir proteção contra ataques de sequestro de dados (Ransomware attack) diretamente no Appliance, com as segu características:

5.37. Deve possuir recursos de imutabilidade dos dados através de Write Once Read Many – WORM garantindo a imutabilidade p armazenamento no Appliance;

5.38. O relógio de conformidade de retenção deverá ser independente do relógio do sistema operacional para evitar, em cas ataque cibernético, a alteração do relógio do sistema operacional e a expiração das cópias de backup

5.39. Deverá permitir apenas imagens do sistema operacional assinaladas e desenvolvidas pelo próprio fabricante, evitando assi um ataque cibernético corrompa ou substitua o sistema operacional do Appliance;

5.40. Deverá possuir o padrão FIPS 140-2 que especifica os requisitos de segurança e criptografia;

5.41. Possuir auto suporte do tipo call home para seus componentes de hardware e software, tais como: CPU, disco, f ventiladores, temperatura, capacidade de utilização, firmware, entre outros;

5.42. A desduplicação deve ser global, ou seja, todos os dados armazenados no repositório de longa retenção deverão estar em b duplicados.

5.43. Permitir o envio de dados desduplicados para a nuvem.

6. Expansão de Appliance de Backup ou Objeto para Armazenamento de Dados para Longa Retenção

6.1. Possuir, no mínimo, 600 TB (seiscentos terabytes) de capacidade utilizável considerando base 2 (1 TB igual a 1024 gigabytes RAID-6 ou erasure coding, sem considerar ganhos com desduplicação e compressão de dados;

6.2. Deve obrigatoriamente ser compatível com o Appliance de backup para armazenamento de longa retenção do ITEM 5,qu entende como o propósito de ingestão dos dados de backup para armazenamento de longa retenção dos dados desduplicad replicação;

6.3. Permitir a utilização de todas as funcionalidades, tecnologias e recursos especificados, irrestrita e sem necessidad licenciamentos ou ônus adicionais;

6.4. Deve ser novo, sem uso, e constar no site do fabricante como uma expansão de appliance de backup ou de objeto em disco armazenamento de dados de longa retenção em linha de produção atual;

6.5. Permitir a utilização de todas as funcionalidades, tecnologias e recursos especificados, irrestrita e sem necessidad licenciamentos ou ônus adicionais;

6.6. Deverá possuir gerenciamento de falhas e alarmes embarcado no próprio “Appliance”, não devendo utilizar servidores exte para tais funcionalidades;

6.7. O sistema de armazenamento deve permitir replicar os dados através de rede IP (WAN/LAN);

6.8. O sistema de armazenamento deve permitir suporte à replicação dos dados no formato desduplicado;

6.9. Deve possuir interface de administração WEB GUI e CLI;

6.10. O sistema de armazenamento deverá suportar RAID-1 para Sistema Operacional e RAID-6 ou erasure coding para dados d sistema de proteção de falhas em disco;

6.11. O Sistema de armazenamento de backup disco deverá conter disco de "hot spare" ou área para a proteção de dados caso o perda de um disco. O disco de "hot spare" será usado para substituir e reconstruir automaticamente o dado de backup;

6.12. Permitir a substituição dos componentes redundantes sem interrupção do serviço (hot swapping);

6.13. Deve suportar a tecnologia de imutabilidade ou WORM (*write once ready many*) para armazenamento dos dados de backup;

6.14. Os componentes de controladoras RAID, FAN e *power supply* devem ser redundantes;

6.15. Não serão aceitas soluções compostas por componentes de fabricantes diferentes; e/ou que não sejam homologada fornecidas pelo próprio fabricante appliance de backup ou objeto;

6.16. Todos os componentes de hardware da solução deverão possuir fontes de alimentação redundantes;

6.17. Todos os equipamentos devem ser montáveis em rack padrão 19’’;

6.18. Deve suportar armazenamento via LAN e WAN, sem a necessidade de adquirir outras soluções para as localidades remotas;

6.19. Possuir alimentação elétrica com fontes internas ao equipamento, redundantes e *hot-swappable*;

6.20. A solução deve ser fornecida com todos os acessórios necessários para a plena configuração, operacionalização, utilizaç gerenciamento do equipamento, sem necessidade de aquisições futuras de licenças ou softwares de ativação, tais como:

6.20.1. Softwares e manuais necessários para o gerenciamento;

6.20.2. Os softwares, drives e firmwares necessários devem estar em suas últimas versões;

6.20.3. Cabos lógicos de gerenciamento/console;

6.20.4. Cabos de energia elétrica padrão IEC 320 plug C13/C14 e IEC 320 C14/C19;

6.20.5. Possuir licença para replicação dos dados armazenados no dispositivo de armazenamento para outro dispositiv mesma natureza em formato desduplicados.

6.21. Deverá possuir o padrão FIPS 140-2 que especifica os requisitos de segurança e criptografia;

6.22. Possuir auto suporte do tipo call home para seus componentes de hardware e software, tais como: CPU, disco, f ventiladores, temperatura, capacidade de utilização, firmware, entre outros;

6.23. Permitir o envio de dados desduplicados para a nuvem.

7. Serviço de Instalação e Configuração

7.1. As atividades de entrega, instalação e configuração dos softwares e equipamentos da solução deverão ocorrer na sed CONTRATANTE e a execução deve ser realizada em horários que não coincidam com o expediente do CONTRATANTE;

7.2. O CONTRATANTE poderá autorizar a realização de atividades durante o horário de expediente se, ao seu exclusivo crit entender que não oferece risco ao funcionamento dos serviços e sistemas em produção;

7.3. O processo de entrega, instalação e configuração dos componentes da solução deverá ser acompanhado e supervisionado equipe técnica indicada pelo CONTRATANTE;

7.4. Entregar os equipamentos novos e 1º uso juntamente com todos os itens acessórios de hardware e de software necessár perfeita instalação e funcionamento, incluindo cabos, conectores, interface, suportes, drivers de controle, programas de configur conforme especificações constantes no ANEXO I - ESPECIFICAÇÕES TÉCNICAS DA SOLUÇÃO do Termo de Referência;

7.5. Entregar os equipamentos devidamente protegidos e embalados, originais lacrados, sem danos de transporte e manuseio;

7.6. Entregar os equipamentos e softwares, às suas expensas, bem como instalar e realizar todos os testes necessários à verificaçã perfeito funcionamento dos produtos fornecidos;

7.7. Entregar toda a documentação técnica em meio eletrônico, completa e atualizada, contendo os manuais e guias de utilização;

7.8. Caso a implantação de qualquer elemento da solução cause interferência na correta operação da rede de dados do CONTRATA a CONTRATADA deverá alocar profissionais com qualificação suficiente para corrigir o problema ou retornar ao ambiente à conc anterior à implantação;

7.9. A execução dos serviços de entrega, instalação e configuração dos softwares e equipamentos da solução deverá contempla mínimo, os seguintes itens:

7.9.1. Instalação física e ativação dos componentes da solução;

7.9.2. Integração à rede do CONTRATANTE, sem interrupção no funcionamento normal dos serviços de TI. Caso exis

necessidade de interrupção de qualquer equipamento ou serviço em produção para a integração da solução, o prazo realização e a duração da janela de manutenção deverão ser acordados com o CONTRATANTE;

7.9.3. Instalação e configuração dos softwares e funcionalidades exigidas na especificação técnica dos elementos que compõ solução fornecida, bem como quaisquer outras disponíveis adicionalmente nos diversos componentes da solução med solicitação da equipe do CONTRATANTE;

7.9.4. Realização de testes de operação da solução que comprovem o funcionamento dos recursos de tolerância a falhas diversos componentes da solução, quando aplicável;

7.9.5. Atualização do Plano de Implantação com todas as informações que representem a topologia física e lógica e a configu final aplicadas.

8. Serviço de Transferência de Conhecimento

8.1. A CONTRATADA deverá realizar a transferência de conhecimento para a equipe técnica do CONTRATANTE por meio de treinam nas tecnologias da solução para até 10 participantes com carga horária total de no mínimo 20 (vinte) horas;

8.2. O serviço de transferência de conhecimento será solicitado sob demanda, mediante de emissão de ordem de serviço espe para este serviço conforme ANEXO III - CRONOGRAMA DE IMPLANTAÇÃO;

8.3. A transferência de conhecimento deverá iniciar no prazo máximo de 15 (quinze) dias corridos após a emissão da ordem de se específica para esta etapa conforme ANEXO III - CRONOGRAMA DE IMPLANTAÇÃO;

8.4. A transferência de conhecimento deverá ser realizada na sede do CONTRATANTE ou em ambiente alternativo indicado CONTRATADA, desde que seja previamente justificado e autorizado pelo CONTRATANTE;

8.5. O programa para a transferência de conhecimento deverá abordar as principais funcionalidades de administração e operaçã solução e ser previamente aprovado pelo CONTRATANTE, e eventuais mudanças de conteúdo solicitadas deverão constar no mat didático;

8.6. O material didático da transferência de conhecimento deverá ser disponibilizado em formato eletrônico, sem custo adicional p CONTRATANTE, devendo ainda estar, preferencialmente, em língua portuguesa (Brasil), podendo ser em idioma estrangeiro (inc tendo em vista que é comum soluções de Tecnologia da Informação serem desenvolvidas por empresas estrangeiras e mat bilíngue;

8.7. Deverá ser emitido certificado de participação ao final do curso a cada participante, detalhando programa e carga horária;

8.8. O cronograma efetivo da transferência de conhecimento será definido em conjunto com o CONTRATANTE, após a emissã Ordem de Serviço na primeira reunião de planejamento;

8.9. Caso a transferência de conhecimento não seja satisfatória com relação à profundidade do conteúdo apresentado ou domíni temas por parte do instrutor, a CONTRATADA deverá complementar, sem ônus adicional, o repasse dos pontos considerados CONTRATANTE como insatisfatórios;

8.10. A transferência de conhecimento deverá ser realizada por técnicos qualificados e certificados pelos fabricantes dos softwa equipamentos da solução ofertada.

9. Serviço de Suporte Técnico

9.1. O serviço de suporte técnico para os softwares e equipamentos da solução deverá ser executado pela CONTRATADA diretamente pelo fabricante, durante o prazo de 48 (quarenta e oito) meses, contados a partir da data de emissão do Term Recebimento Definitivo dos serviços de entrega, instalação e configuração dos softwares e equipamentos da solução;

9.2. O serviço de suporte técnico da solução consiste em:

9.2.1. Atuar, mediante abertura pelo CONTRATANTE de chamado técnico de suporte, no local de instalação da solução, visan solução de problemas que afetem de forma isolada ou conjunta, qualquer elemento da solução, permitindo o retorno à con normal de operação;

9.2.2. Atuar, mediante abertura pelo CONTRATANTE de chamado técnico de suporte, por meio de contato telefônico ou c recurso de comunicação, visando o esclarecimento de dúvidas em relação a qualquer elemento da solução;

9.2.3. Realizar visitas técnicas preventivas no local de instalação da solução (on-site), com frequência mensal, e com duraçã pelo menos 1 (uma) hora a cada visita, visando assegurar o melhor desempenho da solução;

9.2.4. Substituir peças e componentes, cujos problemas sejam decorrentes do desgaste pelo uso normal dos equipamentos outras de configuração idêntica ou superior, originais e novas.

9.3. CONTRATANTE realizará a abertura de chamados técnicos de suporte por ligação telefônica, por e-mail ou via Internet, em per integral, 24 (vinte e quatro) horas por dia, 07 (sete) dias por semana;

9.4. A CONTRATADA deverá informar o procedimento para abertura de chamado técnico de suporte no documento Plan Implantação;

9.5. Se a Central de Suporte estiver localizada fora de Brasília, a CONTRATADA deverá informar o DDG (discagem direta gratuita 08 O acesso à área restrita de suporte em endereço eletrônico (WEB site) deverá estar disponível, também, 24 (vinte e quatro) hora dia, 07 (sete) dias por semana;

9.6. Quando da abertura de chamado técnico de suporte pelo CONTRATANTE, a CONTRATADA deverá informar o número do cham para fins de controle;

9.7. A CONTRATADA deverá enviar mensalmente, ou disponibilizar acesso por meio de portal internet, relação consolidada chamados abertos no mês, mencionando: data e hora de abertura do chamado técnico, número do chamado técnico, probl verificados, técnico responsável pelo atendimento;

9.8. A CONTRATADA deverá disponibilizar acesso a base de conhecimento do fabricante dos componentes da solução, contempl toda a documentação técnica (guias de instalação/configuração atualizados, FAQs, com pesquisa efetuada através de ferramenta busca) e atualizações;

9.9. A CONTRATADA deverá realizar a cada ocorrência, como escopo das atividades de visitas técnicas preventivas, as tarefas de c e análise de logs dos produtos, realizar o levantamento de configurações aplicadas nos softwares e equipamentos da sol buscando compará-las às melhores práticas e recomendações dos fabricantes, avaliar aspectos de segurança e desempenh solução, finalizando com a elaboração de relatório técnico com as informações coletadas e as recomendações a serem aplica solução;

9.10. As visitas técnicas preventivas deverão ser realizadas por técnico(s) plenamente qualificado(s), com certificação emitida fabricantes dos softwares e equipamentos da solução ofertada, e deverão ser prestadas com acompanhamento da equipe técni CONTRATANTE;

9.11. A contagem de prazo para a realização das visitas técnicas preventivas será iniciada após emissão do Termo de Recebim

Definitivo, devendo ocorrer automaticamente em dia e hora previamente agendada com o CONTRATANTE e serão consider concluídas após o entrega do relatório técnico de atendimento e aceite pelo CONTRATANTE. A cada visita deverá ser gerado rela técnico com sugestões e ajustes para a melhoria de desempenho, funcionalidade e segurança;

9.12. A CONTRATADA deverá prestar as informações e os esclarecimentos que venham a ser solicitados pelos técnicos CONTRATANTE, em relação à instalação, configuração e problemas detectados, atendendo de imediato as solicitações;

9.13. Níveis mínimos do serviço de suporte técnico:

9.13.1. Quando da abertura de chamado técnico de suporte, os chamados deverão ser categorizados em 3 (três) nívei seguinte forma:

Criticidade	Descrição	Prazo máximo para início de atendimento (contados a partir da abertura do chamado)	Prazo máximo para restauração de serviço (contados a partir da abertura do chamado)
Severidade 1 (Alta)	Atuação ON-SITE em ocorrências que causem indisponibilidade ou restrição de funcionalidade da solução prejudicando a operação normal e que gerem impacto ao negócio.	Em até 2 (duas) horas deve ter um técnico da CONTRATADA ON-SITE.	Em até 4 (quatro) horas
Severidade 2 (Média)	Atuação REMOTA visando sanar problemas que criem restrições a operação normal da solução não gerando impacto ao negócio.	Em até 6 (seis) horas um técnico da CONTRATADA entra em contato	Em até 12 doze) horas
Severidade 3 (Baixa)	Atuação REMOTA visando sanar problemas que não afetem a operação normal da solução ou dúvidas de operação e configuração.	Em até 12 (doze) horas um técnico da CONTRATADA entra em contato.	Em até 36 (trinta e seis horas)

10. Sustentação do contrato

10.1. Recursos materiais e humanos necessários à execução contratual

10.1.1. Recursos orçamentários estimados:

10.1.2. Equipe de fiscalização:

10.1.2.1. Gestor do contrato: dedicação estimada em aproximadamente 30 min/dia;

10.1.2.2. Fiscal técnico da SECTI: dedicação estimada em aproximadamente 30 min/dia;

10.1.2.3. Fiscal administrativo da DIGER: dedicação estimada em aproximadamente 30 min/semana.

10.2. Continuidade do fornecimento da solução de TIC em eventual interrupção contratual

10.2.1. Evento: Indisponibilidade orçamentária

10.2.1.1. Ação de Contingência: Aguardar a disponibilidade orçamentária para o prosseguimento da contratação.

10.2.1.2. Responsável: DIGER

10.2.2. Evento: Fornecedor impedido de prosseguir com a prestação do serviço

10.2.2.1. Ação de Contingência: revisar o termo de referência e realizar uma nova licitação.

10.2.2.2. Responsável: equipe de planejamento da contratação / SECTI / DIGER / SECOF.

10.2.3. Evento: Falência da contratada ou do fabricante dos equipamentos

10.2.3.1. Ação de Contingência: Iniciar a contratação de nova empresa para prestar suporte técnico como extensã garantia do equipamento

10.2.3.2. Responsável: equipe de planejamento da contratação / SECTI / DIGER / SECOF.

10.3. Atividades de transição contratual e de encerramento do contrato

10.3.1. Atividade: documentar e armazenar, no TRF6, todos os trabalhos/serviços produzidos pela CONTRATADA.

10.3.1.1. Responsável: Equipe de fiscalização

10.3.1.2. Período: Durante a vigência do contrato

10.3.2. Atividade: contratar nova fornecedora para a continuidade do serviço.

10.3.2.1. Responsável: Equipe de planejamento da contratação

10.3.2.2. Período: Iniciar o planejamento com 1 ano de antecedência do término do contrato

11. Estratégia de Independência

11.1. Não se aplica, uma vez que o TRF6 depende de uma nova solução de backup e dos serviços de suporte técnico e garant solução de backup.

VIII - Justificativas para o parcelamento ou não da contratação

( ) Não se aplica em razão da licitação ser dispensável ou inexigível.

( ) Não é possível o parcelamento, pois trata-se de apenas 1 (um) item. (ADJUDICAÇÃO: MENOR PREÇO POR ITEM).

( ) É possível a contratação da solução de forma divisível observado o §2 do art. 40 da Lei n. 14.133/2021 (ADJUDICAÇÃO: MENOR PREÇO ITEM).

(X) Todos ou alguns itens da solução devem ser agrupados para o fornecimento por um único fornecedor, observado o §3º do art. 40 da L 14.133/2021

(ADJUDICAÇÃO: MENOR PREÇO GLOBAL).

Justificativa:

O objeto do certame não será parcelado, uma vez que as soluções que compõem o objeto formam um conjunto indissociável, composto interligação dos serviços que funcionam harmonicamente.

As melhores práticas na implantação de uma nova solução de backup se baseiam na integração das soluções e serviços, que indissociáveis e apresentam inter-relação entre si, de forma que assegurem o alinhamento e a coerência em termos de qualidade téc resultando assim, no perfeito atendimento dos princípios da celeridade, economicidade e eficiência.

Somente a execução de forma integrada das soluções e dos serviços garante a qualidade das entregas, evitando transferênci responsabilidades, nos casos de eventuais problemas causados por serviços prestados por mais de uma empresa contratada.

É importante também, se observar o posicionamento do Egrégio Tribunal de Contas da União, nos autos do Acórdão n. 1916/2009 – Ple sobre a matéria:

> "15. Acerca da alegada possibilidade de fragmentação do objeto, vale notar que nos termos do art. 40, § 3º, da 14.133/2021, exige-se o parcelamento do objeto licitado sempre que isso se mostre técnica e economicamente vi respeito da matéria, esta Corte de Contas já editou a Súmula n. 247/2004, in verbis: "É obrigatória a admissão da adju por item e não por preço global, nos editais das licitações para a contratação de obras, serviços, compras e alienaçõe objeto seja divisível, desde que não haja prejuízo para o conjunto ou complexo ou perda de economia de escala, tendo e o objetivo de propiciar a ampla participação de licitantes..." (grifos não constam do original).
>
> Depreende-se, portanto, que a divisão do objeto deverá ser implementada sempre que houver viabilidade técnica e eco para a sua adoção.
>
> Nesse ponto, calha trazer à baila o escólio de Marçal Justen Filho: "O fracionamento em lotes deve respeitar a integ qualitativa do objeto a ser executado. Não é possível desnaturar um certo objeto, fragmentando-o em contratações div que importam o risco de impossibilidade de execução satisfatória." (Comentários à Lei de Licitações e Co Administrativos. 10. ed. São Paulo: Dialética, 2004. p. 209). "

Ainda, de acordo com a Lei 14.133/2021 em seu art. 40 § 3º:

O parcelamento não será adotado quando:

I - a economia de escala, a redução de custos de gestão de contratos ou a maior vantagem na contratação recomendar a comp item do mesmo fornecedor;

II - o objeto a ser contratado configurar sistema único e integrado e houver a possibilidade de risco ao conjunto do objeto pretendi

III - o processo de padronização ou de escolha de marca levar a fornecedor exclusivo.

Por tudo exposto e em virtude da especificidade do objeto, pode-se afirmar que é tecnicamente inadequado o seu desmembramento pena de não se atender ao objetivo buscado. Sob o ponto de vista econômico, não há elementos nos autos que permitam concluir d adoção do parcelamento do objeto, seria, no caso concreto, mais vantajoso para o TRF6.

IX - Demonstrativo dos resultados pretendidos em termos de economicidade e de melhor aproveitamento dos recu humanos, materiais e financeiros disponíveis

Busca-se com a presente contratação:

a) Redução dos riscos de interrupção dos serviços e sistemas em decorrência da implantação de mudanças na infraestrutura de TI;

b) Aumentar a segurança e eficiência dos backups dos dados de todos os sistemas do TRF6;

c) Aumentar e manter os serviços com elevado padrão de desempenho, qualidade e confiabilidade;

d) Assegurar a sustentabilidade dos serviços que envolvem a infraestrutura de TI;

e) Fornecer níveis de disponibilidade condizentes com as necessidades do TRF6, provendo ininterruptamente os serviços de backup dur 24 horas por dia nos 365 dias do ano e possuir recursos que minimizem ocasionais indisponibilidades;

f) Fornecer níveis de desempenho condizentes com as necessidades do TRF6, provendo serviços de backup com tempos de resposta não acarretem impactos na percepção dos usuários desses serviços;

g) Fornecer níveis de segurança às informações do TRF6 condizentes com os requisitos de integridade e confiabilidade do Trib provendo recursos que permitam operacionalização de melhores práticas relativas a essas questões;

h) Existência de serviços especializados para realizar os diagnósticos e todas as ações de suporte para restabelecer o pleno funcionam dos recursos de proteção de dados no menor tempo de espaço possível;

i) Estar em conformidade com a Portaria CJF n. 540/2021, que dispõe sobre a institucionalização da política de backup e restauraçã arquivos do Conselho da Justiça Federal e dá outras providências;

j) Prover maior segurança para os usuários acerca dos dados armazenados pelo TRF6.

X - Providências a serem adotadas pela Administração previamente à celebração do contrato, inclusive quanto à capacitaçã servidores ou de empregados para fiscalização e gestão contratual

Não se aplica.

XI - Contratações correlatas e/ou interdependentes

Não se aplica.

XII - Descrição de possíveis impactos ambientais e respectivas medidas mitigadoras, incluídos requisitos de baixo consum energia e de outros recursos, bem como logística reversa para desfazimento e reciclagem de bens e refugos, quando aplicáv

12.1. Critérios:

12.1.1. Tenho conhecimento de que: A fabricante e/ou distribuidora, e/ou importadora, e/ou comerciante e/ou consumidora deste o deve possuir Cadastro Técnico Federal de Atividades Potencialmente Poluidoras e/ou Utilizadoras de Recursos Ambientais (CTF/APP)?

a) (X) Não. ( ) Sim. Identifique a(s) categoria(s) da Ficha Técnica de Enquadramento (FTE): _____

b) ( ) a fabricante, e/ou distribuidora, e/ou importadora, e/ou comerciante, e/ou consumidora deste objeto não se enquadra nas FT CTF/APP.

12.1.2. Os produtos/objetos são constituídos de material (marque quantos itens forem necessários):

( ) renovável ( ) reciclado ( ) atóxico ( ) biodegradável (X) não se aplica

12.1.3. Os objetos são considerados produtos perigosos, segundo a Gestão de Resíduos Sólidos do TRF6/SJMG:

(X) Não. ( ) Sim. Quais? _____

12.1.4. Os objetos da aquisição devem estar em conformidade com os seguintes regulamentos técnico/legal: (marque quantos itens f necessários):

( ) Etiqueta Nacional de Conservação de Energia

( ) Certificado de Conformidade de Potência Sonora de Produtos Eletrodomésticos

( ) Certificado de Vistoria de Veículo

( ) Ficha de Informações de Segurança de Produtos Químicos

( ) Documento de Origem Florestal

( ) Autorização para o Exercício da Atividade de Revenda de GLP

( ) Outro(s). Especificar: _____

12.1.5. Há outros critérios de sustentabilidade, além dos relacionados acima:

(X) Não. ( ) Sim. Descreva: _____

12.2. Deverão ser consideradas as diretivas do Plano de Logística Sustentável do TRF6, normativos internos e a legislação vigente.

12.2.1. A aquisição ou contratação demandará ou resultará em (marque quantos itens forem necessários)

(X) geração de resíduo.

( ) consumo de papel.

( ) consumo de outros materiais de expediente (caneta, grampos, clips, pastas etc).

( ) consumo de café ou açúcar.

( ) consumo de água mineral envasada.

( ) gastos com correspondências.

( ) instalação de computador ou impressora.

( ) aparelho de telefone fixo ou móvel.

(X) consumo de energia elétrica.

( ) consumo de água.

( ) serviços de engenharia (instalações elétricas, hidráulicas, ponto de rede, ponto de telefone, divisórias).

( ) obras civis (reforma ou construção de edificação).

( ) serviço de limpeza - aumento da área a ser limpa no TRF6.

( ) serviço de vigilância - aumento no número de postos.

( ) quantidade de veículos na frota do TRF6.

( ) gasto com contratos de veículos (manutenção, peças, insumos, seguro, lavagem, terceirização, exceto motorista).

( ) consumo de combustível.

( ) ação de qualidade de vida.

( ) ação de capacitação socioambiental.

( ) não demandará ou resultará em nenhum dos itens acima.

XIII - Posicionamento conclusivo sobre a adequação da contratação para o atendimento da necessidade a que se destina

Com base nas informações levantadas ao longo deste estudo técnico, declaramos que a solução apresentada é viáv prosseguir e ser concretizada, pois é a que melhor atende os requisitos técnicos e funcionais pretendidos pela área demandante.

Certificamos que somos responsáveis pela elaboração do presente documento que compila os Estudos Técnicos Preliminar que este traz os conteúdos previstos na Lei nº 14.133/2021.

Na redação foram observadas as diretrizes estabelecidas no Guia de Contratações de TIC, instituídas pela Resolução C 468/2022 (art. 16 da IN STJ/GDG n. 4/2023).

13.1. A Equipe de Planejamento da Contratação foi instituída pela Informação Portaria SJMG-DIREF 287/2022 (SEI TRF1 15035322).

Responsáveis pela elaboração:

Integrante Requisitante	**Integrante Técnico**	**Integrante Administrativo**
Nome: Daniel Santos Rodrigues Diretor da Secretaria de Tecnologia da Informação - SECTI/TRF6 Matrícula: TR44	Nome: Heli Lopes Rios Diretor da Subsecretaria de Infraestrutura - SUINF / SECTI Matrícula: TR38	Nome: Cristiane de Figueiredo Gomes SEPLA/SECOF Matrícula: TR128
O presente planejamento está em conformidade com os requisitos técnicos necessários ao cumprimento do objeto e atende adequadamente às demandas de negócio formuladas. Os benefícios pretendidos são adequados, os riscos envolvidos são administráveis, os custos previstos são compatíveis e caracterizam a economicidade.		

Documento assinado eletronicamente por **Heli Lopes Rios**, **Diretor(a) de Subsecretaria**, em 16/04/2024, às 13:38, conforme art. 1º, § 2º, III, "b", da Lei 11.419/2006.

Documento assinado eletronicamente por **Daniel Santos Rodrigues**, **Diretor(a) de Secretaria**, em 18/04/2024, às 12:59, conforme art. 1º, § 2º, III, "b", da Lei 11.419/2006.

Documento assinado eletronicamente por **Cristiane de Figueiredo Gomes**, **Analista Judiciário**, em 18/04/2024, às 17:35, conforme art. 1º, § 2º, III, "b", da Lei 11.419/2006.

A autenticidade do documento pode ser conferida no site https://sei.trf6.jus.br/sei/controlador_externo.php?acao=documento_conferir&id_orgao_acesso_externo=0 informando o código verificador **0724279** e o código CRC **99FA8E6B**.