

ESTUDO TÉCNICO PRELIMINAR

Autores

Nome	Cargo	Área	e-mail
Vicente da Fonseca Bezerra Júnior	AFRE	COTIN/SAT/SEFAZ	vbezerrajunior@fazenda.ms.gov.br
Cláudio Norikazu Uemura	ATI	COTIN/SAT/SEFAZ	uemura@fazenda.ms.gov.br

Janeiro de 2025

1. NECESSIDADE DA CONTRATAÇÃO

1.1. IDENTIFICAÇÃO DA NECESSIDADE DA CONTRATAÇÃO

- 1.1.1. A Equipe de infraestrutura COTIN elaborou o Estudo Técnico Preliminar com o objetivo de pesquisar uma Solução de Tecnologia da Informação e Comunicação (TIC) que atenda não tão somente os requisitos básicos de uma solução de *backup* e *restore*, mas que também atenda as características e especificações funcionais e não funcionais mais adiante especificadas, tendo como finalidade essencial a de prover maior capacidade, diversidade, garantia e confiabilidade de armazenamento, gravação, recuperação, segura e íntegra dos dados e informações, visando atender as demandas atuais e futuras da SAT – Superintendência de Administração Tributária da Secretaria de Estado de Mato Grosso do Sul, para análise da sua viabilidade e levantamento dos elementos essenciais que servirão para compor o Termo de Referência, de forma que melhor atenda às necessidades da COTIN/SAT/SEFAZ-MS, em conformidade com o Decreto Estadual nº 16.138, de 23 de março de 2023.
- 1.1.2. A contratação será via Licitação na modalidade PREGÃO, na forma ELETRÔNICA, nos termos da Lei nº 14.133, de 2021 e demais legislação aplicável e, ainda, de acordo com as condições estabelecidas no Edital.
- 1.1.3. A referida contratação, após a devida autorização, deverá possuir adequação orçamentária e financeira com a Lei Orçamentária Anual – LOA e compatibilidade com o Plano Plurianual - PPA e Lei de Diretrizes Orçamentárias – LDO

1.2. JUSTIFICATIVAS DA NECESSIDADE DE CONTRATAÇÃO

- 1.2.1. A gestão da Tecnologia da Informação e Comunicação (TIC) está cada vez mais ligada às áreas negociais e finalísticas dos Governos, em qualquer que seja as esferas, Federal, Estadual ou Municipal, gerando impactos significativos dentro das organizações.
- 1.2.2. As atividades de TIC têm cada vez mais interdependências com os demais departamentos e órgãos de Estado, auxiliando e facilitando o alcance de metas e objetivos das diversas áreas de negócio.
- 1.2.3. Os recursos de tecnologia são empregados constantemente na execução de atividades institucionais finalísticas e administrativas governamentais. O desafio é alinhar o investimento em recursos de TIC, seu provimento e sua utilização, à estratégia de negócio do órgão de estado. O foco de uma boa gestão de tecnologia

sempre contempla a melhoria contínua da relação custo/benefício de recursos, o aumento da capacidade produtiva, o provimento do suporte e a melhoria de processos institucionais com formas de geração e agregação de valor.

- 1.2.4. A evolução contínua da infraestrutura e a busca pela melhoria das atividades de suporte avançado à operação e à manutenção dos serviços de TIC constituem requisitos essenciais para o bom funcionamento das atividades e funções apoiadas pelo setor. A crescente automatização de processos e sistemas são elementos estratégicos para o sucesso dos negócios atendidos pelo órgão responsável pela TIC em si.
- 1.2.5. A Coordenadoria de Tecnologia da Informação (COTIN), diretamente subordinada à Superintendência de Administração Tributária (SAT), tem como atribuição precípua a gestão da infraestrutura, das soluções e serviços de Tecnologia da Informação e Comunicação (STIC) pertinentes exclusivamente à assuntos tributários da Secretaria de Estado de Fazenda do Estado de Mato Grosso do Sul (SEFAZ-MS).
- 1.2.6. De antemão é sabido que a COTIN, por meio do processo administrativo n. 11/014.383/2021, realizou a contratação de um empresa especializada no fornecimento e instalação de Solução Integrada para Missão Crítica de Tecnologia da Informação e de Comunicação com alta disponibilidade, composto por ambiente modular seguro certificado ABNT NBR 15.247 e seus subsistemas, serviço mensal de manutenção preventiva e corretiva com monitoramento online, serviço de Moving sob demanda, serviços de substituição das baterias e capacitores dos UPS sob demanda, serviço de substituição do gás NOVEC 1230 sob demanda, serviço de abastecimento de diesel sob demanda, com fornecimento e instalação de peças, acessórios e materiais necessários para instalação e manutenção, em atendimento às necessidades da área tributária da Secretaria de Estado de Fazenda de Mato Grosso do Sul.
- 1.2.7. A solução contratada, comumente conhecida como Sala Cofre, a entrega desta, está prevista para o fim do ano de 2024, deste modo, será necessário equipar a Sala com equipamentos de TIC como servidores de rede, sistemas de armazenamento, switches de rede, roteadores, aceleradores de conteúdo, equipamentos de proteção de rede como firewalls, ips, ids, além de ter serviços de sustentação da infraestrutura e backup.

- 1.2.8. Os serviços a serem contratados possuem natureza continuada, uma vez que são altamente relevantes para manter a infraestrutura que suporta, na manutenção da qualidade dos serviços nos sistemas informatizados legados e dos dados corporativos e no atendimento às soluções tecnológicas singulares operadas pela Coordenadoria de Tecnologia da Informação (COTIN), é importante frisar que a ausência de qualquer atividade dos serviços afetará toda a infraestrutura de TIC a ser implantada no datacenter da COTIN.
- 1.2.9. A Coordenadoria Especial de Tecnologia da Informação (COTIN), vem progressivamente investindo na adoção de boas práticas no gerenciamento da infraestrutura de TIC, e a presente contratação será o reflexo deste contínuo investimento, pois permitirá a manutenção da adoção de metodologias capazes de garantir a correta prestação dos serviços e o atendimento eficiente aos usuários.
- 1.2.10. A Superintendência de Administração Tributária (SAT), a quem a COTIN atende diretamente, recente de soluções de TIC mais exclusivas, dedicadas e adequadas ao seu fim, cuja natureza primordial é a de garantir rapidez e segurança nos procedimentos e dados pertinentes às atividades de tributação, fiscalização e arrecadação do Estado, neste sentido, a segurança no ambiente de tecnologia da informação é imprescindível para as organizações. Uma das partes mais importantes no âmbito da Segurança da Informação é a capacidade não só de armazenar e reter os dados, mas principalmente a de recuperação de dados em caso de perda física ou lógica.
- 1.2.11. Para isso, é indispensável um ambiente de backup eficiente e que atenda a demanda de recuperação das informações, mantendo dados históricos importantes.
- 1.2.12. Os procedimentos de Cópias de Segurança e Restauração (Backup/Restore) têm por objetivo a prevenção ao caos organizacional decorrente do “desaparecimento” de sistemas, dados processuais ou de usuários e/ou informações de arquivos/software em caso de sinistros ou falhas, garantindo eficientemente suas restaurações de forma rápida e segura.
- 1.2.13. Necessita então a COTIN/SAT/SEFAZ de uma solução de serviços gerenciados de proteção de dados, que possa garantir não tão somente seu armazenamento seguro, mas também sua guarda (retenção) de forma replicada (redundância).

- 1.2.14. Esta solução de Backup deve ser abrangente sobre todas as suas formas e versões de armazenamento dos dados, alcançando sistemas de arquivos e bancos de dados heterogêneos;
- 1.2.15. Além de ser lastreada na horizontal dos dados, deve também alcançar e gerir de forma fácil e integrada todas as versões desses sistemas de arquivos e bancos de dados, ou seja, ser uma interface de gestão e monitoramento única e amigável.
- 1.2.16. Além disso, e principalmente, deve-se garantir a restauração desses dados (Restore), de forma confiável e rápida.
- 1.2.17. A terceirização (outsourcing) dos serviços de plataforma de backup, mostra-se altamente benéfica para a COTIN, pois permite e possibilita aos servidores da COTIN mais disponibilidade para a operacionalização e segurança da TIC a fim de melhor atender as necessidades apresentadas pelo Estado. Destacamos que a COTIN não dispõe de quadro próprio de pessoal especializado em TIC em quantidade suficiente para a execução dos serviços operacionais.
- 1.2.18. O gerenciamento de serviços de TIC são essenciais e compostos de várias atividades integradas e interdependentes, incluindo a sustentação de infraestrutura de tecnologia para organização, desenvolvimento, implantação e execução continuada de tarefas, neste caso de operação de backup e restore.
- 1.2.19. Considerando que a COTIN se utilizará de rotinas baseadas na biblioteca de gerenciamento de serviços ITIL, sendo este um modelo organizacional de gestão de TIC difundido e conceituado mundialmente, é de suma importância a contratação de empresa com estrutura compatível com esta metodologia, a fim de garantir a continuidade do processo de maturidade na gestão de serviços.
- 1.2.20. A adoção de um modelo de suporte técnico centralizado em uma Central de Serviços (NOC) faz parte das boas práticas de gestão de serviços de TI recomendadas pela biblioteca ITIL. Esse modelo possibilita a solução de dúvidas e solicitações de todos os usuários com tempestividade, padrões e, consequentemente, melhor qualidade.
- 1.2.21. O emprego do modelo ITIL em uma organização proporciona a redução de custos operacionais, já que desestimula a utilização de uma vasta equipe, privilegiando ser atendido por um quadro restrito e bem capacitado, de alta produtividade e custo otimizado. O modelo busca também contornar de forma otimizada situações de paralisação de serviços de TIC causados pela ocorrência de incidentes.

- 1.2.22. Além disso, possibilitará a continuidade da sua modernização tecnológica e funcional, possibilitando o crescimento e a melhoria da qualidade dos atendimentos às demandas dos usuários finais, relacionadas ao apoio técnico, no uso dos recursos computacionais e serviços disponibilizados pela área de TIC.
- 1.2.23. Salienta-se que, a presente contratação irá trazer uma série de benefícios a SEFAZ/MS, SAT e COTIN, agregando valor aos serviços e produtos desenvolvidos, com garantia de transferência de tecnologia ao órgão através da elaboração e melhoria dos processos de atendimento e com a construção da base de conhecimento de incidentes, problemas e causas raiz.
- 1.2.24. Nesse sentido, é imprescindível a aquisição de uma solução de backup e restore, que tenha estas características e especificações funcionais e não funcionais, a fim de prover maior capacidade, diversidade, garantia e confiabilidade de armazenamento, gravação, recuperação, segura e íntegra dos dados e informações, visando atender as demandas atuais e futuras.
- 1.2.25. Também se faz necessário que tal solução seja acompanhada de serviços que garantam o funcionamento pleno, a continuidade e disponibilidade do ambiente e a resiliência deste frente a eventuais sinistros, e neste sentido, este estudo prevê ainda o serviço de operação, monitoramento, suporte técnico, treinamento, dentre outros, dada a complexidade e sensibilidade dos mesmos dentro da estrutura de Data Center, sem os quais o Estado estaria sujeito aos riscos de falha, interrupção ou degradação da qualidade necessária à sua estrutura de trabalho, por não garantir o correto e pronto restabelecimento dos dados, informações e aplicações que são o patrimônio imaterial da COTIN/SAT/SEFAZ-MS, o que levaria a um caos técnico-administrativo sem mensuração racional, gerando prejuízos financeiros, de imagem institucional e social, de cunho legal, dentre outros.

1.3. CLASSIFICAÇÃO DO OBJETO DA CONTRATAÇÃO COMO SOLUÇÃO DE TIC

- 1.3.1. O Decreto Estadual n. 16.138 de 23 de março de 2023, em seu Art. 1º, V, assim considera:

“Art. 1º Este Decreto estabelece medidas de planejamento, de padronização e de coordenação das licitações e das contratações públicas, no âmbito dos órgãos da Administração Direta, das autarquias e das fundações do Poder Executivo Estadual, que tenham por finalidade:

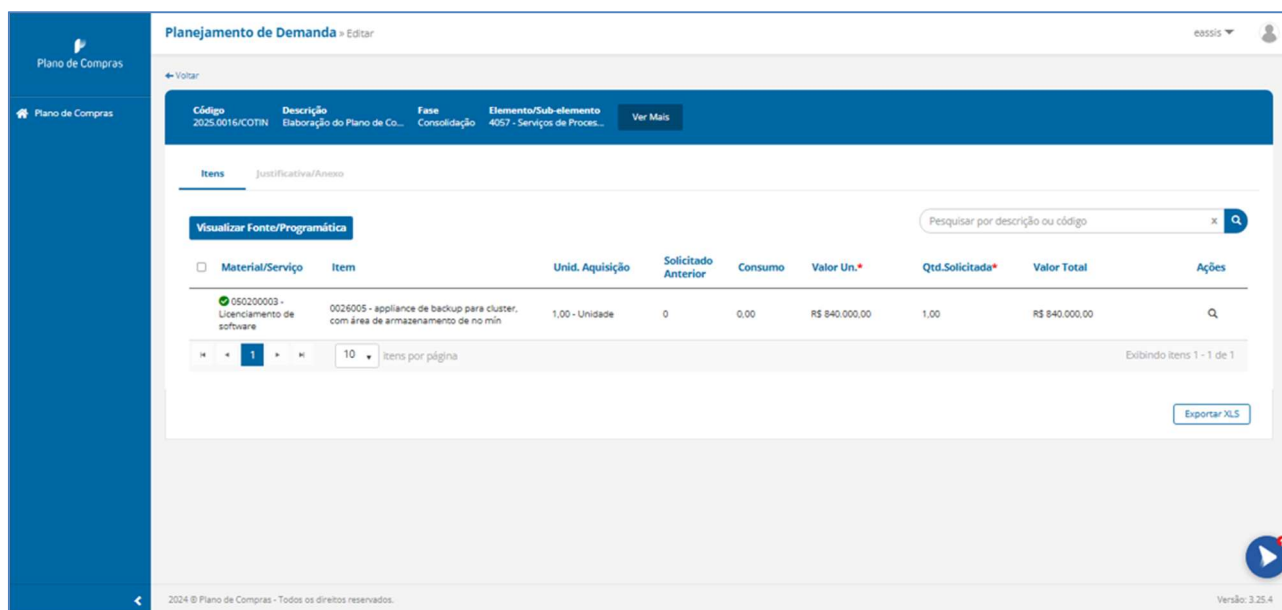
(...)

V- contratações de tecnologia da informação e comunicação.”

- 1.3.2. Em virtude disto, o entendimento acerca da conceituação apresentada se baseia na utilização de bens (hardware), sistemas de informação (software) e/ou serviços de TIC, tendo como finalidade o processamento de dados e informações digitais para o alcance dos resultados pretendidos pela contratação.
- 1.3.3. Considerando que a solução em estudo engloba elementos com as características descritas acima, de modo a atender à necessidade que a desencadeou, pode-se afirmar que esta contratação compreende uma solução de tecnologia, e assim sendo deverá seguir as diretrizes estabelecidas no Decreto Estadual supracitado.

2. DEMONSTRAÇÃO DA PREVISÃO DO PLANO ANUAL DE CONTRATAÇÃO

- 2.1. A presente contratação foi contemplado no **Plano de Compras Anual- PCA/2024 (ID do Item n. 0026005)** e se dará por meio de **Pregão Eletrônico**, observando os preceitos de direito público, além dos dispositivos legais pertinentes, notadamente às normas e procedimentos administrativos em conformidade com o **inciso I, do Art. 28, da Lei Federal n. 14.133, de 01 de abril de 2021**, do **art. 1º do Decreto Estadual n. 16.118, de 3 de março de 2023** e da **Lei n. 8.078/1990 - Código de Defesa do Consumidor (CDC)**, bem como às condições estabelecidas no Termo de Referência, conforme telas emitidas do Plano de Compras abaixo:



The screenshot displays the 'Planejamento de Demanda' (Demand Planning) interface. It features a sidebar with 'Plano de Compras' and a main content area with a table of items. The table includes columns for 'Código', 'Descrição', 'Fase', 'Elemento/Sub-elemento', and 'Ver Mais'. Below this, there's a section for 'Itens' with a search bar and a table of item details. The table shows one item: '050200003 - 0026005 - appliance de backup para cluster, com área de armazenamento de no mín'. The table also includes columns for 'Unid. Aquisição', 'Solicitado Anterior', 'Consumo', 'Valor Un.*', 'Qtd.Solicitada*', 'Valor Total', and 'Ações'. The interface includes pagination controls and an 'Exportar XLS' button.

Código	Descrição	Fase	Elemento/Sub-elemento	Ver Mais
2025.0016/COTIN	Elaboração do Plano de Co...	Consolidação	4057 - Serviços de Proces...	

Material/Serviço	Item	Unid. Aquisição	Solicitado Anterior	Consumo	Valor Un.*	Qtd.Solicitada*	Valor Total	Ações
050200003 - Licenciamento de software	0026005 - appliance de backup para cluster, com área de armazenamento de no mín	1,00 - Unidade	0	0,00	R\$ 840.000,00	1,00	R\$ 840.000,00	

Planejamentos de Demandas > Pesquisar

Planos de Compras

Agenda Planejamento

Novo

cotin

<input type="checkbox"/>	Exercício	Descrição	Demandante	Elemento/Subelemento	Situação	Ações
<input type="checkbox"/>	2025	Elaboração do Plano de Contratações Anual para o exercício de 2025.	COTIN - SEFAZ	4011 - Locação de Softwares	Consolidado	+
<input type="checkbox"/>	2025	Elaboração do Plano de Contratações Anual para o exercício de 2025.	COTIN - SEFAZ	5235 - EQUIPAMENTOS DE PROCESSAMENTO DE DADOS	Consolidado	+
<input type="checkbox"/>	2025	Elaboração do Plano de Contratações Anual para o exercício de 2025.	COTIN - SEFAZ	3901 - Assinatura de Periódicos	Consolidado	+
<input type="checkbox"/>	2025	Elaboração do Plano de Contratações Anual para o exercício de 2025.	COTIN - SEFAZ	4003 - Serviços Técnicos de Profissionais de TIC-PJ	Consolidado	+
<input type="checkbox"/>	2025	Elaboração do Plano de Contratações Anual para o exercício de 2025.	COTIN - SEFAZ	4057 - Serviços de Processamento de Dados	Consolidado	+

1 2 5 itens por página

Exibindo itens 1 - 5 de 6

2024 © Plano de Compras - Todos os direitos reservados. Versão: 3.25.4

- 2.2. O Plano de contratações anuais da Secretaria de Fazenda do Estado do Mato Grosso do Sul, pode ser consultado no link: pncp.gov.br/app/pca/02935843000105/2024.
- 2.3. Oportuno destacar que, no âmbito do Estado de Mato Grosso do Sul, foi editado o Decreto n. 16.121, de 9 de março de 2023, que dispõe sobre o Plano de Contratação Anual, no âmbito dos órgãos da Administração Direta e das entidades autárquicas e fundacionais do poder Executivo Estadual, nos termos da Lei Federal n. 14.133 de 1º de abril de 2021, e dá outras providências.
- 2.4. Ademais, cumpre esclarecer que não cabe ao órgão gerenciador adentrar na análise de cada previsão elaborada e aprovada pelas entidades, cabe somente analisar se os itens solicitados estão presentes no Plano de Contratações Anual (PCA) de 2024, conforme art. 17 do Decreto Estadual 16.121/2023.
- 2.5. Conforme preconiza o dispositivo legal, o PCA visa a racionalização das contratações e isso quer dizer que o objetivo é fazer uma programação da necessidade de determinada contratação, através da previsão de consumo, a partir do prognóstico da sua utilização provável e necessária.
- 2.6. No presente caso, além de estar previsto no PCA, houve o envio do Instrumento de Oficialização de Pedido (fls.10), sendo devidamente autorizado pelos órgãos competentes.

3. REQUISITOS DO NEGÓCIO

- 3.1. A Solução esperada gira em torno da contratação de Serviços gerenciados de proteção de dados compostos por *software* e repositório de *backup (on-premise)*, instalação, configuração e suporte, por 36 (trinta e seis) meses.

Item	Descrição	Quantidade mensal	Unidade
001	Solução de serviços gerenciados de proteção de dados com repositório local incluso	400	Terabytes

- 3.1.1. Considerando que a COTIN se utilizará de rotinas baseadas na biblioteca de gerenciamento de serviços ITIL, sendo este um modelo organizacional de gestão de TIC difundido e conceituado mundialmente, é de suma importância a contratação de empresa com estrutura compatível com esta metodologia, a fim de garantir a continuidade do processo de maturidade na gestão de serviços.
- 3.1.2. A CONTRATADA deverá executar os serviços especializados de armazenagem de dados (*backup*) juntamente e principalmente com os serviços de restauração (*Restore*) de forma integrada e compatível com todo o ambiente tecnológico da COTIN/SAT/SEFAZ-MS.
- 3.1.3. Deverão ser definidos Acordos de Nível de Serviços (SLA) que garantam a atividade e operação plena dos serviços em tempo e em conformidade com as necessidades da COTIN/SAT/SEFAZ-MS.
- 3.1.4. A implementação da solução deve contemplar as etapas de planejamento, instalação, migração de dados, homologação, treinamentos de pessoal nas funcionalidades específicas da ferramenta utilizada e suporte técnico compatível para a execução adequada do objeto contratado.
- 3.1.5. A execução das atividades deverá manter uma cogestão técnica da COTIN, respeitando a estrutura funcional do órgão e atribuições inatas.
- 3.2. REQUISITOS DA SOLUÇÃO
- 3.2.1. Especificações Gerais
- 3.2.1.1. A solução de serviços gerenciados de proteção de dados é composta por etapas, que serão objeto de Termo de Recebimento Definitivo para registro do marco:

- 3.2.1.1.1. Instalação e Configuração: prazo máximo 90 (noventa) dias após a assinatura do contrato;
- 3.2.1.1.2. Operação: iniciar-se-á após a primeira proteção de dados ser realizada.
- 3.2.1.2. Todos os requisitos da contratação devem ser entregues licenciados e palavras como deve, permite, suporta, efetua, proporciona, possui etc. significam que a funcionalidade deve ser entregue operacional, sem ônus adicional à CONTRATANTE;
- 3.2.1.3. Os *softwares* utilizados não poderão ter sido mencionados pelo fabricante em qualquer relatório referente à existência de data futura de fim de fornecimento, garantia ou assistência técnica na data de assinatura do contrato. Para aferir esta informação a CONTRATADA deve indicar o endereço na *Internet* do sítio do fabricante, onde deverá constar o produto e/ou material como em produção;
- 3.2.1.4. Todas as capacidades são especificadas em seu requisito mínimo, podendo ser entregue capacidade superior. Todos os requisitos devem garantir a compatibilidade às versões especificadas e superiores;
- 3.2.1.5. Todos os serviços devem ser executados de forma completa e integral para a solução a ser fornecida e todos os seus elementos adicionais;
- 3.2.1.6. Todos os *softwares* integrantes da solução ofertada devem ser fornecidos na versão mais nova comercializada na data de assinatura do contrato;
- 3.2.1.7. As fibras óticas e interfaces GBIC/SFP utilizadas devem ser/suportar o tipo Multimodo. A solução fornecida deve adaptar-se perfeitamente ao ambiente computacional da COTIN e ser comprovadamente compatível e interoperável com seus elementos componentes;
- 3.2.1.8. Deverão ser fornecidos:
 - 3.2.1.8.1. Cordões óticos multimodo categoria OM-3 e *Patch cords ethernet* cat 6a, em número suficiente para suportar os equipamentos ofertados;
 - 3.2.1.8.2. PDUs, cabos, tomadas *steck* (macho e fêmea) e demais elementos necessários ao atendimento dos requisitos do Edital;

- 3.2.1.9. Os serviços devem ser prestados por técnico certificado pelo fabricante dos itens. Caso não haja programa de certificação do fabricante, serão aceitos técnicos que tenham realizado treinamentos oficiais;
- 3.2.1.10. Os componentes da solução devem possuir compatibilidade com:
 - 3.2.1.10.1. Os sistemas operacionais Microsoft Windows Server, versão 2012 e superiores. A compatibilidade será verificada por meio de consulta ao Windows Server Catalog (<http://www.windowsservercatalog.com/>);
 - 3.2.1.10.2. Os sistemas operacionais RedHat Enterprise Linux, versão 6 e superiores;
 - 3.2.1.10.3. Os sistemas operacionais Oracle Linux 7.x ou superiores. A compatibilidade será verificada por meio de consulta ao Oracle Hardware/Software Compatibility List;
 - 3.2.1.10.4. Os *softwares* VMware ESXi, versão 7 e superiores. A compatibilidade será verificada por meio de consulta ao VMware Compatibility Guide (<http://www.vmware.com/resources/compatibility/>).
- 3.2.1.11. Para os itens de compatibilidade em que o Sistema Operacional/*software* não é mais suportado pelo fabricante (*EOS*), não será exigida a sua presença na matriz de compatibilidade;
- 3.2.1.12. Será aceita a apresentação de matriz de compatibilidade obtida no sítio do fabricante da solução a ser aferida;
- 3.2.1.13. Não serão aceitas propostas sem a comprovação “ponto-a-ponto” para todos os itens técnicos. Somente serão aceitas comprovações por meio de declaração do fabricante ou da licitante para 10% (dez por cento) do total de itens e subitens do objeto (requisitos do Termo de Referência). As declarações do fabricante ou da licitante devem ser emitidas por representante legal do emissor, assinadas digitalmente ou com firma reconhecida em cartório;
 - 3.2.1.13.1. As declarações da licitante serão exclusivas para comprovação de itens de serviço e não se aplicam a exigências técnicas dos produtos que compõem a solução.

3.2.1.14. Serão aceitos na língua inglesa apenas os documentos de comprovação de ordem técnica.

3.2.2. Serviços gerenciados de proteção de dados com repositório local incluso:

3.2.2.1. O serviço deverá ser entregue na métrica de “*front-end terabyte*”, ou seja, *terabytes* consumidos na origem por mês;

3.2.2.2. Não será aceita nenhuma outra forma de licenciamento para o serviço que não o especificado para efeito de monitoração da métrica do serviço;

3.2.2.3. O consumo mínimo do serviço será de 200 *Terabytes* mensais;

3.2.2.4. Baseado no consumo mensal, deverá ser utilizado *software* de gestão de *backup* e repositório para armazenamento de dados de *backup*;

3.2.2.5. A medição dos serviços será demonstrada por meio da apresentação de relatório detalhado do consumo extraído da ferramenta utilizada;

3.2.2.6. O volume protegido não poderá exceder o máximo contratado sem autorização, que se materializará por meio da assinatura de ordem de serviço, que deverá ser emitida mensalmente e representará as adições de proteção feitas no período;

3.2.2.6.1. O faturamento das adições e reduções será feito *pró-rata* contado da data de início da proteção, à proporção de 1/30 avos do valor mensal do TB, por dia protegido;

3.2.2.6.2. Respeitado o consumo mínimo, o volume poderá ser aumentado ou reduzido por meio da adição/redução de capacidade em blocos de 1 *Terabyte*. A fração de TB será contada como uma unidade integral de TB;

3.2.2.6.3. Os recursos materiais necessários a atender a demanda, caso a variação constatada seja inferior a 20% (vinte por cento) daquela aferida no período anterior, deverão ser providos de forma imediata;

3.2.2.6.4. Os recursos materiais necessários a atender a demanda, caso a variação constatada seja igual ou superior a 20% (vinte por cento) daquela aferida no período anterior, deverão ser providos no prazo máximo de 45 (quarenta e cinco) dias;

3.2.2.6.5. O pagamento dos serviços somente será devido após a emissão da ordem de serviço.

3.2.2.7. O faturamento do consumo mínimo somente será iniciado depois de finalizada a etapa de instalação, momento em que a CONTRATADA terá 60 (sessenta) dias para proteger 200 TB de frontend;

3.2.2.8. A tabela abaixo descreve a proporção de backup por tipo de dados, observada no ambiente computacional da CONTRATANTE:

Tipo de Dados	Proporção
BANCO DE DADOS	15%
HADOOP	26%
MINIO (S3)	33%
AMBIENTE DE VIRTUALIZAÇÃO VMWARE	26%

3.2.2.9. Essa proporção poderá variar em até 10% sem prejuízo final do cálculo de armazenamento;

3.2.2.10. Devem ser considerados os seguintes períodos de retenção:

Tipo de backup	Retenção	Repositório
Diário	15 dias	Disco Curta e Longa Retenção
Semanal	5 semanas	Disco Curta e Longa Retenção
Mensal	13 meses	Disco Longa Retenção
Anual	5 anos	Disco Longa Retenção

3.2.2.11. O disco se refere ao repositório de curta ou longa retenção ofertado pela CONTRATADA;

3.2.2.12. Para efeito de dimensionamento da solução, deverá ser considerada janela de *backup* diária de 8 horas, em dias de semana e 12 horas em finais de semana, com taxa de alteração dos dados diária de 5% (cinco por cento);

3.2.2.13. Deve ser fornecido equipamento de repositório de *backup* com capacidade de armazenamento para suportar o volume de consumo

mensal de *backup*, de acordo com as métricas de tipo de dados e retenção em disco definidas neste Termo de Referência;

3.2.2.14. De acordo com o consumo mínimo garantido de 200TB, a tabela abaixo demonstra a capacidade a ser fornecida para o repositório de *backup* conforme premissas estabelecidas inicialmente;

3.2.2.14.1. É esperado que a volumetria do repositório de *backup* apresente crescimento proporcional ao crescimento do consumo de *frontend*;

3.2.2.14.2. De acordo com a tabela de proporção de *backup* por tipo de carga de trabalho, o volume de dados a ser fornecido como repositório de *backup* deverá considerar o cálculo inicial para 200TB:

Tipo de <i>backup</i>	Retenção	Repositório	Taxa de Alteração	Volume de Dados
Diário	15 dias	Disco de curta e longa retenção	$200 \times 0,05 = 10\text{TB}$	$10 \times 15 = 150\text{TB}$
Semanal	5 semanas	Disco de curta e longa retenção	-	$200 \times 5 = 1.000\text{TB}$
Mensal	13 meses	Disco de longa retenção	-	$200 \times 13 = 2.600\text{TB}$
Anual	5 anos	Disco de longa retenção	-	$200 \times 5 = 1.000\text{TB}$
VOLUME DE ARMAZENAMENTO EM DISCO DE CURTA RETENÇÃO				1.150TB
VOLUME DE ARMAZENAMENTO EM DISCO DE LONGA RETENÇÃO				4.750TB

3.2.2.15. Para os equipamentos a serem utilizados como repositório de *backup* deve ser considerada taxa de redução de dados global de acordo com a métrica ofertada pelo fabricante da solução;

3.2.2.15.1. A redução deverá ser realizada em linha (on-line), otimizando e reduzindo o espaço em *racks* ocupados no *Datacenter* assim como o consumo elétrico da solução, racionalizando os recursos da CONTRATANTE;

3.2.2.15.1.1. Caso a deduplicação seja implementada após o processamento (post processing) ou em paralelo,

deverá ser ofertado o volume de dados todo necessário sem considerar desduplicação.

- 3.2.2.15.2. A redução deverá ser global por *pool* de deduplicação, considerando todo o volume de dados, não sendo permitido que a redução seja aplicada apenas no *job* ou aplicação, otimizando e reduzindo o espaço em *racks* ocupados no *Datacenter* assim como o consumo elétrico da solução, racionalizando os recursos da CONTRATANTE;
- 3.2.2.15.3. A redução ofertada será de total responsabilidade da CONTRATADA, caso, em algum momento do contrato, respeitando as premissas deste Termo de Referência, o equipamento não possua capacidade suficiente para a demanda, deverá ser entregue armazenamento adicional em um prazo de, até, 10 dias a contar da identificação do problema sob pena de multa e glosa de acordo com os níveis de serviço;
- 3.2.2.16. Para a medição da quantidade de *Terabytes* de *frontend*, deve-se considerar a somatória da área utilizada e efetivamente protegida (espaço em uso e protegido por política de *backup*) de todos os discos/volumes presentes em todos os servidores que serão protegidos por *backup*. A somatória deste valor deve ser convertida para a unidade *Terabytes*;
- 3.2.2.17. Deve, a partir de uma única interface, gerenciar operações de *backup* e *restore* de diferentes sistemas operacionais (clientes) e de diferentes serviços (agentes);
- 3.2.2.18. Todos os componentes de software deverão ser do mesmo fabricante, integrados e que ofereçam um módulo único de gerenciamento. Não será aceito mais de um software de Backup e Restore para atendimento dos requisitos técnicos especificados;
- 3.2.2.19. Deverá incluir todas as funcionalidades solicitadas no presente termo, com suporte para backup, restore e tecnologia de desduplicação global de dados, onde o licenciamento deverá possuir capacidade ilimitada de retenções, cópias dos dados protegidos, replicações para

outros ambientes para fins de recuperação de desastres e suportar toda a infraestrutura da CONTRATANTE, sem nenhum ônus a durante a vigência do contrato;

3.2.2.20. Deverá permitir múltiplas políticas de disaster recovery para prevenir perda de dados e cópia automática do catálogo do backup, sincronização entre as cópias do catálogo do backup, replicação entre appliances no mesmo domínio de backup e replicação entre appliances em domínios de backup diferentes;

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

3.2.2.21.1. Camada de gerência;

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

3.2.2.21.3. Camada de clientes/agentes multiplataforma de backups.

3.2.2.22. Deve suportar servidor de gerência e catálogo instalados em conjunto nas seguintes plataformas: Linux e Windows. Não serão aceitos catálogos instalados em plataformas (sistemas operacionais) diferentes da utilizada no servidor de gerência.

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

3.2.2.24. Deve permitir a realização de operações de *backup* e *restore* para os seguintes clientes:

3.2.2.24.1. Microsoft Windows 10 e superior;

3.2.2.24.2. Microsoft Windows Server 2012 R2, 2016, 2019 e 2022, todos x64;

3.2.2.24.3. Red Hat Enterprise Linux versões 8 e superior; e

3.2.2.24.4. SuSe Linux Enterprise Server versão 12.

- 3.2.2.25. Não será oferecido pela CONTRATANTE nenhum componente de hardware que não relacionados a conectividade e segurança;
- 3.2.2.26. Não será permitido pela CONTRATANTE a utilização de nenhum componente da sua infraestrutura de virtualização;
- 3.2.2.27. Deve possuir painel de status de tarefas de *backup* que permita realizar operações e acompanhar o andamento das tarefas;
- 3.2.2.28. **Deve permitir a proteção de servidores para as seguintes aplicações e banco de dados, realizada por meio de integração direta e com a utilização de agentes específicos:**
 - 3.2.2.28.1. Microsoft SQL Server versões 2012 e superior;
 - 3.2.2.28.2. Microsoft SharePoint versões 2013 e superior. Deve suportar *backup* completo do *Sharepoint*, com possibilidade de recuperação de uma ou mais *databases*, documentos individuais, *sites*, *subsites*, listas e itens/documentos individuais;
 - 3.2.2.28.3. MySQL versões 5 e superior;
 - 3.2.2.28.4. Oracle/Oracle RAC versões 11G e superior;
 - 3.2.2.28.5. Windows Server Cluster.
- 3.2.2.29. **Deve realizar criptografia de dados, sendo exigidas as seguintes características:**
 - 3.2.2.29.1. Criptografar dados para geração de cópias de *backup* já executados, com o objetivo de criptografar dados de *backups* realizados em mídias;
 - 3.2.2.29.2. Criptografar os dados colocados em *backup* utilizando os algoritmos mais comuns de mercado, que utilizem chaves de, pelo menos, 256 (duzentos e cinquenta e seis) bits.
- 3.2.2.30. Deve permitir a utilização de servidores de gerenciamento em cluster de alta disponibilidade;
- 3.2.2.31. Deve integrar-se com o Microsoft *Active Directory* e permitir a associação de usuários externos (*AD*) com usuários e grupos de usuários internos da solução, inclusive importando a hierarquia de subgrupos do *AD*. Esta associação deve permitir a criação de perfis de

usuários que possibilite o controle de níveis de acesso aos servidores, repositórios de armazenamento e outros objetos pertencentes à solução;

- 3.2.2.32. Deve permitir o gerenciamento das operações de *backup* e *restore* de forma centralizada e distribuída;
- 3.2.2.33. Deverá possuir e implementar o fator duplo de autenticação - 2FA para o console de administração gráfica e linha de comando por meio do provedor de identidade baseado em SAML ou cartões inteligentes CAC / PIV ou certificados de usuário;
- 3.2.2.34. Deve possuir catálogo com banco de dados centralizado contendo as informações sobre todos os dados e mídias onde os backups foram armazenados, esse banco de dados para o catálogo deve ser próprio e fornecido em conjunto com o produto.
- 3.2.2.35. A base de dados para armazenamento do catálogo deve possuir funcionalidades de recuperação rápida em caso de desastre, fornecido por ferramentas especificamente desenhadas para esta função;
- 3.2.2.36. Deve possuir mecanismo de reconstrução do catálogo ou banco de dados centralizado em caso de perda destes, sem a necessidade de recatalogar as imagens de *backup*;
- 3.2.2.37. Deve possibilitar replicação do catálogo interno em tempo real ou agendado, para o caso de recuperação de desastres;
- 3.2.2.38. Deve ser capaz de realizar cópia de arquivos abertos sem que a consistência destes seja comprometida;
- 3.2.2.39. Deve permitir operações de *backup* e *restore* por meio da rede local (*LANbased*) e Storage Area Network (*SANbased* ou *LANfree*);]
- 3.2.2.40. Deve permitir a utilização do protocolo IPv6 para todas as operações de rede, inclusive aquelas de transporte dos dados de proteção;
- 3.2.2.41. Deve possuir funcionalidade de paralelizar a gravação de dados de um cliente de *backup* em diferentes caminhos pertencentes a um dispositivo de armazenamento (*multistreaming*);
- 3.2.2.42. Deve possuir funcionalidade de gravação serial e simultânea de vários *streams* de *backup* em um único caminho pertencente a um dispositivo de armazenamento (multiplexação);

- 3.2.2.43. Deve permitir que as tarefas de *backup/restore* sejam realizadas por meio de interface gráfica e por meio de scripts;
- 3.2.2.44. Deve suportar *backup* do *Oracle Database*, também na arquitetura Oracle RAC, utilizando o RMAN;
- 3.2.2.45. Deve descobrir automaticamente instâncias Oracle por meio de consultas periódicas aos clientes de bancos de dados;
- 3.2.2.46. Deve manter a sincronia entre os catálogos de *backups* do Oracle RMAN e da solução ofertada;
- 3.2.2.47. A funcionalidade de descoberta automática de instancias deve ser capaz de gerar os *scripts* RMAN no momento de execução do *backup*;
- 3.2.2.48. Deve suportar *backup* on-line do *Windows Server 2012 Active Directory* e superiores;
- 3.2.2.49. Deve suportar *restore* completo do *Windows Server 20012 Active Directory* e superiores;
- 3.2.2.50. Deve suportar *restore* granular de objetos e de propriedades individuais de objetos do *Windows Server 2012 Active Directory* e superiores;
- 3.2.2.51. Deve permitir envio de alertas por meio de correio eletrônico (*e-mail*) para reportar eventos ocorridos na operação e configuração do *software*;
- 3.2.2.52. Deve possuir API para integração dos alarmes com sistemas externos de monitoramento por meio do protocolo SNMP;
- 3.2.2.53. Deve possuir funcionalidade de agendamento de tarefas de *backup*;
- 3.2.2.54. **Deve permitir operações de *backup* e *restore* de ambientes virtualizados provendo as seguintes funcionalidades:**
 - 3.2.2.54.1. Seleção automática de máquinas virtuais por meio de consultas personalizadas ao *vCenter*;
 - 3.2.2.54.2. Descobrimto automático das máquinas virtuais nos ambientes VMWare;
 - 3.2.2.54.3. Operações de *backup* de sistemas de arquivo de servidores virtuais (VMs) sem a necessidade de instalação de agentes nos próprios servidores virtuais;

- 3.2.2.54.4. Operações de *backup* de sistemas de arquivo de servidores virtuais (VMs) com a instalação de agentes nos próprios servidores virtuais;
- 3.2.2.54.5. *Restore* individual de arquivos e diretórios das máquinas virtuais;
- 3.2.2.54.6. CBT (*Change Block Tracking*) da VMWare para as operações de *backup*;
- 3.2.2.54.7. *Backup* em nível de bloco das máquinas virtuais diretamente no *storage* por meio de *snapshots* gerenciados pela ferramenta de *backup*;
- 3.2.2.54.8. Operações de *restore* granular dos arquivos diretamente nos servidores virtuais, sem a necessidade de instalação de agentes nos próprios servidores virtuais;
- 3.2.2.54.9. Suporte às seguintes tecnologias de virtualização:
 - 3.2.2.54.9.1. VMWare *vSphere*;
 - 3.2.2.54.9.2. Microsoft *Hyper-V*;
 - 3.2.2.54.9.3. *Nutanix Acropolis*;
 - 3.2.2.54.9.4. *Openstack*;
 - 3.2.2.54.9.5. *RehHat RHEV*.
- 3.2.2.55. **Deverá possuir a funcionalidade de proteção contínua de dados (CDP) para todo o ambiente VMware com no mínimo os seguintes requisitos:**
 - 3.2.2.55.1. Não poderá impactar as VMs durante a execução da proteção contínua de dados (CDP)
 - 3.2.2.55.2. Deverá proteger continuamente os dados das VMs do ambiente VMware e fornecer backup de baixo RPO (até 30 minutos) por meio de interface de administração java ou web.
- 3.2.2.56. **Em caso de insucesso ou erros na operação de *backup*:**
 - 3.2.2.56.1. Deve ser capaz de reiniciar uma operação de *backup* ou *restore*, com opção de continuação, ou seja, retomando a cópia dos dados a partir do momento da falha até a sua finalização;

- 3.2.2.56.2. Deve permitir uma re-submissão da tarefa sem que todo o *backup* tenha que ser refeito, ou seja, realizando a operação novamente apenas nos pontos de falha, em caso de *job* completado com erros;
- 3.2.2.56.3. Deve apontar claramente os arquivos que apresentaram falha e o motivo dela.
- 3.2.2.57. Deve permitir identificar e cadastrar arquivos do tipo temporário que possam ser ignorados em eventual falha causada pela presença destes na fase de *scan* e ausência na fase de *backup*;
- 3.2.2.58. Deverá possuir mecanismos de proteção contra ransomware com as seguintes características:
 - 3.2.2.58.1. Deverá suportar imutabilidade em repositórios locais e para plataforma que utilizem protocolo S3;
 - 3.2.2.58.2. Deverá possuir detecção de anomalias nos dados em tempo de execução de backup;
 - 3.2.2.58.3. Deverá possuir mecanismo de detecção de malwares nos dados armazenados no repositório de backup de maneira automática e manual;
 - 3.2.2.58.4. Deverá permitir a exclusão de arquivos infectados encontrados no ato de um restore;
 - 3.2.2.58.5. Detecção e alerta sobre mudanças inesperadas nos dados de backup, com no mínimo os seguintes metadados, atributos ou recursos da tarefa de backup:
 - 3.2.2.58.5.1. Tamanho da imagem de backup;
 - 3.2.2.58.5.2. Número de arquivos de backup;
 - 3.2.2.58.5.3. Dados que são transferidos em KB;
 - 3.2.2.58.5.4. Taxa de deduplicação;
 - 3.2.2.58.5.5. Tempo de conclusão do trabalho de backup.
 - 3.2.2.58.6. Deverá fazer uso de tecnologia de Inteligência Artificial e aprendizagem de máquina para detecção de anomalias;
 - 3.2.2.58.7. Deverá possuir a capacidade de relatar anomalias como um falso positivo através do cálculo de parâmetro com base nos dados históricos disponíveis após uma determinada

frequência oferecendo maior flexibilidade e reduzindo a quantidade de falsos positivos.

- 3.2.2.58.8. Qualquer desvio incomum nesses atributos de trabalho de backup deverá ser considerado uma possível anomalia notificando por meio de console WEB e REST-API.
- 3.2.2.59. A solução deve permitir a realização de backups diretamente para unidades de fita magnética;
- 3.2.2.60. A solução deve ser capaz de realizar a replicação de dados de *backup* armazenados em suas bibliotecas magnéticas para sites remotos, permitindo ainda que o *restore* dos mesmos seja feito por meio das cópias armazenadas remotamente;
- 3.2.2.61. Permitir o envio de dados desduplicados para a nuvem, caso seja necessário fornecer licenciamento adicional deverá constar na proposta;
- 3.2.2.62. A solução deve ser capaz de gerenciar as fitas magnéticas contidas dentro da biblioteca, fitas magnéticas armazenadas no site de *backup* e nos cofres de mídia, fitas armazenadas off-site e fitas em trânsito;
- 3.2.2.63. A solução deve possuir a funcionalidade de migração de dados entre mídias magnéticas (cartuchos de fita);
- 3.2.2.64. Deve permitir a verificação da integridade do conteúdo das fitas por *software*;
- 3.2.2.65. Deve possuir a funcionalidade de criar múltiplas cópias de *backups* armazenados, com a opção de recuperação dos dados por meio da cópia secundária, caso a cópia primária não esteja mais disponível;
- 3.2.2.66. Deve permitir a realização do *backup* em nuvem, realizando a integração com as principais nuvens públicas do mercado;
- 3.2.2.67. Deve suportar os protocolos S3, CIFS e NFS para as operações de backup e restore de dados;
- 3.2.2.68. Deve permitir a replicação de imagens de um servidor de gerência para outro ambiente, possibilitando a inserção das informações de catálogo da imagem de origem para o catálogo do destino, de forma automática;

- 3.2.2.69. Deve permitir a criação de imagens de servidores físicos, Linux e Windows, para recuperação de desastres (funcionalidade conhecida como *bare metal restore* de forma nativa;
- 3.2.2.70. Para servidores Windows, deve ser possível a recuperação das imagens de recuperação de desastres mesmo em um *hardware* diferente do original ou em ambiente virtual;
- 3.2.2.71. A funcionalidade de *baremetal* especificada anteriormente deve suportar em um único servidor de gerência ou servidor de mídia várias versões de Windows – Windows 2012 e superior;
- 3.2.2.72. Deve permitir a verificação da integridade dos dados armazenados por meio de algoritmos de *checksum* e/ou autocorreção;
- 3.2.2.73. Deve emitir relatórios de *backup* e relatórios avançados com longo período de retenção da informação, customizáveis e, com apresentação de gráficos, devendo:
 - 3.2.2.73.1. Extrair informações de volumes de *backups* realizados por período, por localidade, custo por GB, tendência de crescimento, porcentagem de *backups* realizados de máquinas físicas e virtuais, porcentagem de dados desduplicados e por uso dos *tape drives*;
 - 3.2.2.73.2. Extrair atividades de *restore* realizados por período, por localidade, custo por GB, volume de *restore*, quantidade de arquivos restaurados, porcentagem de *restore* realizados de máquinas físicas e virtuais, porcentagem de tarefas realizadas com sucesso e com erros;
 - 3.2.2.73.3. Extrair informações de *gaps* de proteção, ou seja, períodos no qual determinado dado não possui uma cópia devido a uma falha de *backup*;
 - 3.2.2.73.4. Extrair informações de auditoria, identificando claramente as operações realizadas e por qual usuário ela foi realizada. Ainda permitir visualizar todas as operações que determinado usuário realizou;
 - 3.2.2.73.5. Permitir identificar os clientes que mais consomem licenças e recursos de armazenamento do ambiente

- 3.2.2.73.6. Exportar os relatórios para formato *HTML* ou outro formato portátil de visualização amigável;
- 3.2.2.73.7. Personalizar exibições de dados fornecendo contexto para os relatórios de *backup* como linha de negócios, domínio de *backup* e aplicativos;
- 3.2.2.73.8. Permitir identificar tendências de crescimento a partir da coleta de dados históricos.

3.2.2.74. Do repositório de *backup* de curta retenção:

- 3.2.2.74.1. Deverá obrigatoriamente ser fornecida solução de armazenamento de dados de backup em disco, baseado em Appliance, que se define por subsistema específico de ingestão e tratamento de dados de backup, por meio de tecnologias de deduplicação, replicação e segurança da informação.
- 3.2.2.74.2. A solução deve possuir console de gerenciamento unificado com base de catálogo, funcionalidades de movimentação de dados através de gerenciadores de mídia, e requisitos de segurança e proteção;
- 3.2.2.74.3. Para atendimento dos requisitos técnicos no presente termo visando plena interoperabilidade e segurança dos dados de backup, não serão aceitas soluções tradicionais de armazenamento de dados baseado em Storages, servidores com discos internos e soluções de hyperconvergência;
- 3.2.2.74.4. Não serão aceitas soluções de softwares (Virtual Appliance);
- 3.2.2.74.5. O equipamento deverá ser configurado em alta disponibilidade, portanto ser composto de no mínimo 2 (dois) nós configurados como cluster ativo/ativo, ou seja, na eventualidade de queda de um nó, o outro deverá manter as atividades de movimentador de dados de Backup sem paradas.
- 3.2.2.74.6. Todos os componentes da solução deverão ser do mesmo fabricante. Serão aceitos também soluções que, de forma exclusiva, o software e o hardware possa ser um OEM (Original

Equipment Manufacturer) licenciado, com part number próprio do PROPONENTE fabricante, e com a devida autorização e bem como a comercialização do produto do próprio de forma pública.

- 3.2.2.74.7. Possuir mecanismo de proteção dos dados armazenados, através de RAID (Redundant Array of Independent Disks) de forma a suportar a falha simultânea de no mínimo dois discos (RAID 6), sem interrupção do serviço, ou outro mecanismo de proteção como “Erasure Code”.
- 3.2.2.74.8. A solução deve ser dimensionada e configurada para suportar a perda de qualquer componente sem impacto para o serviço.
- 3.2.2.74.9. A solução ofertada deverá possuir discos de Hot Spare para o appliance e gavetas de expansão de disco da solução, sem necessidade de intervenção prévia manual.
- 3.2.2.74.10. Permitir a substituição dos componentes redundantes sem interrupção do serviço (hot swapping).
- 3.2.2.74.11. Todos os componentes de hardware da solução deverão possuir fontes de alimentação redundantes.
- 3.2.2.74.12. Todos os equipamentos devem ser montáveis em rack padrão 19”.
- 3.2.2.74.13. Os componentes de controladoras RAID, FAN e power supply devem ser redundantes.
- 3.2.2.74.14. Deve ser apresentado, na proposta comercial, o resultado do dimensionamento feito na ferramenta de modelagem do fabricante, não sendo aceita declaração para este item;
- 3.2.2.74.15. Possui tecnologias de redução de dados nativas para compressão e deduplicação de dados, operando de forma *in-line* (em linha) e global;
 - 3.2.2.74.15.1. Caso a deduplicação seja implementada após o processamento (post processing) ou em paralelo, deverá ser ofertado o volume de dados todo necessário sem considerar deduplicação.

3.2.2.74.16. O appliance dever suportar taxa de ingestão de dados de, no mínimo, 60 TB/hora considerando deduplicação no destino (server-side) e 200 TB/hora com deduplicação na origem (client-side).

3.2.2.74.17. Possuir no mínimo: 4 (quatro) portas 10GbE Base-X SFP+ (dez gigabit ethernet), 4 (quatro) portas 10GbE BASE-T (dez gigabits ethernet cobre) e 4 (quatro) portas de 32Gb FC (Fibre Channel) para interconexão e integração com os servidores clientes.

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

3.2.2.74.18.1. Deve possuir recursos de imutabilidade dos dados através de Write Once Read Many – WORM garantindo a imutabilidade para o armazenamento no Appliance.

3.2.2.74.18.2. Deve possuir relógio de conformidade de retenção independente do relógio do sistema operacional para evitar, em caso de ataque cibernético, a alteração do relógio do sistema operacional e a expiração das imagens de Backup.

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

3.2.2.75. Do repositório de *backup de longa retenção*:

3.2.2.75.1. Deve obrigatoriamente fazer uso de sistemas de armazenamento de Backup em disco, baseado em “Appliance”, que se entende como um subsistema com o propósito específico de ingestão dos dados de Backup para armazenamento de longa retenção com deduplicação e replicação.

3.2.2.75.2. Para atendimento dos requisitos técnicos no presente termo visando plena interoperabilidade e segurança dos dados de backup, não serão aceitas soluções tradicionais de

armazenamento de dados baseado em Storages, servidores com discos internos e soluções de hyperconvergência.

- 3.2.2.75.3. Não serão aceitas soluções de softwares (Virtual Appliance).
- 3.2.2.75.4. O equipamento deverá ser configurado em alta disponibilidade, portanto ser composto de no mínimo 2 (dois) nós configurados como cluster ativo/passivo, ou seja, na eventualidade de queda de um nó, o outro deverá manter as atividades de movimentador de dados de Backup sem paradas.
- 3.2.2.75.5. Possuir mecanismo de proteção dos dados armazenados, através de RAID (Redundant Array of Independent Disks) de forma a suportar a falha simultânea de no mínimo dois discos (RAID 6), sem interrupção do serviço, ou outro mecanismo de proteção como “Erasure Code”.
- 3.2.2.75.6. A solução deve ser dimensionada e configurada para suportar a perda de qualquer componente sem impacto para o serviço.
- 3.2.2.75.7. A solução ofertada deverá possuir discos de Hot Spare para o appliance e gavetas de expansão de disco da solução, sem necessidade de intervenção prévia manual.
- 3.2.2.75.8. Permitir a substituição dos componentes redundantes sem interrupção do serviço (hot swapping).
- 3.2.2.75.9. Todos os componentes de hardware da solução deverão possuir fontes de alimentação redundantes.
- 3.2.2.75.10. Todos os equipamentos devem ser montáveis em rack padrão 19”.
- 3.2.2.75.11. Os componentes de controladoras RAID, FAN e power supply devem ser redundantes.
- 3.2.2.75.12. Deve ser apresentado, na proposta comercial, o resultado do dimensionamento feito na ferramenta de modelagem do fabricante, não sendo aceita declaração para este item;
- 3.2.2.75.13. Possui tecnologias de redução de dados nativas para compressão e deduplicação de dados, operando de forma *in-line* (em linha) e global;

- 3.2.2.75.13.1. Caso a deduplicação seja implementada após o processamento (post processing) ou em paralelo, deverá ser ofertado o volume de dados todo necessário sem considerar desduplicação.
- 3.2.2.75.14. Deve ser fornecido com no mínimo 1 (uma) porta de 1 GB (um gigabit) Ethernet para monitoramento, 4 (quatro) portas 1GbE (um gigabit ethernet), 4 (quatro) portas 10GbE (dez gigabit ethernet) ou 25GbE (vinte e cinco gigabit ethernet) para interconexão e integração com os servidores clientes.
- 3.2.2.75.15. Deve possuir proteção contra-ataques de sequestro de dados (Ransomware attack) diretamente no Appliance, com as seguintes características:
- 3.2.2.75.15.1. Deve possuir recursos de imutabilidade dos dados através de Write Once Read Many – WORM garantindo a imutabilidade para o armazenamento no Appliance.
- 3.2.2.75.15.2. Deve possuir relógio de conformidade de retenção independente do relógio do sistema operacional para evitar, em caso de ataque cibernético, a alteração do relógio do sistema operacional e a expiração das imagens de Backup.
- 3.2.2.75.15.3. Deve exigir a autenticação dupla (2FA-Two Factor Authentication).
- 3.2.2.76. A solução e todos os seus elementos deverão ser entregues e instalados por técnico certificado pelo fabricante para este fim;
- 3.2.2.77. A solução deve ser configurada e otimizada segundo as melhores práticas do fabricante em termos de desempenho, disponibilidade e segurança;
- 3.2.2.78. Deve ser alocado gerente de projetos, com as certificações PMP ou similar, que irá preparar, acompanhar e corrigir desvios em cronograma de execução das atividades de configuração e migração de dados;

- 3.2.2.79. Os técnicos para as atividades de configuração devem estar disponíveis em horário comercial, compreendido entre 8 h e 18 h, horário de Brasília, nos dias úteis;
- 3.2.2.80. O acesso remoto será configurado para permitir as ações de suporte técnico remotas, de acordo com as normas de segurança da CONTRATANTE, após assinar o Termo de Confidencialidade, Sigilo e Uso do Prestador e passar pelo processo de credenciamento de colaborador;
- 3.2.2.81. Deve ser entregue documentação de *as-built* da solução. Durante toda a duração do contrato, a CONTRATADA se compromete a manter essa documentação atualizada e refletindo as configurações do ambiente
O *as-built* deve conter as seguintes informações:
 - 3.2.2.81.1. Descrição dos serviços implantados;
 - 3.2.2.81.2. Descrição de topologia lógica e de topologia física de equipamentos após a ativação dos serviços;
 - 3.2.2.81.3. Dados dos equipamentos e softwares, incluindo configurações, números de série e versões;
 - 3.2.2.81.4. Parâmetros de configuração, operação, instalação, manutenção, atualização e correto funcionamento dos equipamentos e softwares;
 - 3.2.2.81.5. Definição de responsabilidades;
 - 3.2.2.81.6. Recursos de alta disponibilidade;
 - 3.2.2.81.7. Procedimentos de recuperação de equipamentos;
 - 3.2.2.81.8. Rotinas de backup e restore dos equipamentos, softwares e configurações implantadas;
 - 3.2.2.81.9. Rotinas periódicas configuradas;
 - 3.2.2.81.10. Documentação dos processos de trabalho associados ao item, em esquema de fluxograma, com definição de responsáveis por cada atividade, prazos de execução, rotinas de atualização e revisão periódica de regras;
- 3.2.2.82. A entrega pela CONTRATADA da documentação *as-built* e sua aprovação é condição necessária para a autorização de pagamento das faturas mensais;

3.2.3. Serviço de operação e suporte técnico especializado:

3.2.3.1. O serviço deverá ser precificado de acordo com a complexidade dos serviços de sustentação e suporte técnico especializado do item 1 deste termo de referência;

3.2.3.2. Entende-se por serviços de sustentação e suporte técnico especializado, as ações que visam garantir a disponibilidade e continuidade do ambiente do cliente, contemplando:

3.2.3.2.1. Atendimento e gestão de chamados;

3.2.3.2.1.1. A CONTRATADA deverá disponibilizar canais para abertura de chamados técnicos via central de atendimento telefônico ou portal WEB;

3.2.3.2.1.2. A central de atendimento através de canal telefônico que deverá operar em regime 24x7x365, durante o período de contrato de garantia e suporte;

3.2.3.3. Análise do Ambiente (Health Check);

3.2.3.3.1. Deverá ser capaz de realizar diagnósticos periódicos, trimestrais, do ambiente (remotamente);

3.2.3.3.2. Deverá confeccionar relatório sobre a saúde dos componentes instalados em relação a seu desempenho, segurança e funcionalidades;

3.2.3.3.3. Deverá analisar riscos coletados por ferramentas da fabricante e do conhecimento técnico de especialistas certificados nas soluções envolvidas;

3.2.3.3.4. Gerar relatório com sugestões de melhorias e suas aplicabilidades;

3.2.3.3.5. Identificar, obter e coordenar a instalação de firmware e patches em conjunto com equipe da CONTRATANTE;

3.2.3.3.6. Entregar documentação gerada de forma digital ou impressa;

3.2.3.3.7. A CONTRATANTE poderá solicitar a apresentação do material confeccionado para avaliação e conhecimento da equipe interna do órgão;

3.2.3.4. Gestão de incidentes;

- 3.2.3.4.1. Deverá atuar na análise e tratamento de alertas e eventos;
- 3.2.3.4.2. Acompanhar e investigar incidentes com o objetivo de identificar a causa raiz;
- 3.2.3.4.3. Prover um plano de ação;
- 3.2.3.4.4. Gerenciar a comunicação;
- 3.2.3.4.5. Recomendar solução de contorno, quando possível;
- 3.2.3.4.6. Em caso de eventos identificados pela fabricante, deverá apoiar na aplicação das boas práticas;
- 3.2.3.4.7. Entregar relatório de incidente apontando cronograma de eventos, atuação técnica, configurações implementadas e solução adotada ou próximas atividades;
- 3.2.3.4.8. Acompanhar de forma remota, após conclusão das análises e identificação das causas do incidente, por no mínimo 1 (uma) semana;
- 3.2.3.4.9. Realizar atendimento remoto, caso necessário, para realização de coletas, aplicação de soluções de contorno ou definitivas;

3.2.3.5. Suporte avançado;

- 3.2.3.5.1. Os serviços de suporte avançado devem contemplar o planejamento e arquitetura de mudanças nos componentes para atualização, melhoria e/ou prevenção de incidentes;
- 3.2.3.5.2. Entende-se por serviços de suporte avançado:
 - 3.2.3.5.2.1. Planejamento de mudanças;
 - 3.2.3.5.2.2. Mapeamento e classificação de riscos;
 - 3.2.3.5.2.3. Análise de compatibilidade;
 - 3.2.3.5.2.4. Levantamento de requisitos funcionais e não-funcionais;
 - 3.2.3.5.2.5. Resolução de dúvidas técnicas referentes às soluções contratadas;
- 3.2.3.5.3. Os serviços prestados a nível de suporte avançado ensejam documentação formal em formato eletrônico em formato de parecer ou relatório técnico com exceção das dúvidas técnicas que podem ser tratadas dentro do canal de suporte e garantia;

3.2.3.6. Operação assistida;

3.2.3.6.1. O serviço deve ser prestado tanto para a solução de backup quanto para o seu repositório, independentemente de configuração ou política, e deve prover:

3.2.3.6.1.1. Substituições de hardware ou componente;

3.2.3.6.1.2. Atualizações corretivas e evolutivas de firmware e software;

3.2.3.6.1.3. Ajustes e configurações conforme melhores práticas da tecnologia;

3.2.3.6.1.4. Demais procedimentos destinados a manter os módulos em perfeito estado de funcionamento;

3.2.3.7. Fornecimento de informações e esclarecimento de dúvidas sobre administração, configuração, otimização, troubleshooting ou utilização;

3.2.3.8. A CONTRATADA deve sanar todos os vícios e defeitos da solução;

3.2.3.9. As atividades englobam a realização de operação de administração, instalação, configuração e monitoramento da solução conforme definido no escopo abaixo:

3.2.3.9.1. Infraestrutura de Backup:

3.2.3.9.1.1. Instalação, Configuração e Atualização de Componentes de Servidor Principal e Mídia;

3.2.3.9.1.2. Entrega de Relatório Trimestral Referente a Saúde do Ambiente de Backup;

3.2.3.9.2. Configuração de Disaster Recovery do Servidor Principal:

3.2.3.9.2.1. Criar política de Disaster Recovery do Master Server;

3.2.3.9.2.2. Especificar Path alternativo para salvar o arquivo de DR;

3.2.3.9.2.3. Especificar login e senha para acessar a informação;

3.2.3.9.2.4. Criação de política de DR;

**3.2.3.9.3. Configuração de Política de Backup ou implementação da
Política de Backup do CONTRATANTE:**

- 3.2.3.9.3.1. Instalação do agente;
- 3.2.3.9.3.2. Planejamento dos requisitos para o backup;
- 3.2.3.9.3.3. Planejamento do (s) destino (s) de backup para o agente;
- 3.2.3.9.3.4. Planejamento da janela de backup para o agente;
- 3.2.3.9.3.5. Planejamento do conteúdo que será backupeado pela política;
- 3.2.3.9.3.6. Planejamento da Retenção dos backups para o agente;
- 3.2.3.9.3.7. Alterar Retenção;
- 3.2.3.9.3.8. Alterar Agendamento;
- 3.2.3.9.3.9. Alterar Conteúdo para Backup;
- 3.2.3.9.3.10. Alterar Destino de backup;
- 3.2.3.9.3.11. Criar cópia de Política;
- 3.2.3.9.3.12. Excluir Política;
- 3.2.3.9.3.13. Teste de Backup;
- 3.2.3.9.3.14. Execução de job de backup;
- 3.2.3.9.3.15. Teste de Restore;
- 3.2.3.9.3.16. Execução de job de restore;

3.2.3.9.4. Troubleshooting Avançado:

- 3.2.3.9.4.1. Rever capacidade de Armazenamento;
- 3.2.3.9.4.2. Rever Número de Media Server;
- 3.2.3.9.4.3. Reinstalar componentes da Arquitetura;
- 3.2.3.9.4.4. Atualização de Versão, Hotfix e Patches;
- 3.2.3.9.4.5. Atualização de Hardware do Master Server;
- 3.2.3.9.4.6. Mudança de Repositório de Backup;
- 3.2.3.9.4.7. Atualização de Hardware Appliance;
- 3.2.3.9.4.8. Restaurar ambiente a partir do DR;

3.2.3.9.5. Operações de Catálogo:

- 3.2.3.9.5.1. Expiração de Imagens de Backup;

3.2.3.9.5.2. Duplicação de Imagens de Backup;

3.2.3.9.5.3. Inventário das imagens de Backup;

3.2.3.9.6. Os limites de isenção de responsabilidade da CONTRATADA pela disponibilidade dos serviços que serão aceitos como justificativas para desconsideração de descontos daquilo que a CONTRATADA demonstrar, tecnicamente, devem ser resultado de:

3.2.3.9.7. Ação ativa da CONTRATANTE na Infraestrutura ou do desenvolvimento de suas aplicações;

3.2.3.9.8. Problemas em outros Serviços de Infraestrutura que não estejam sob a responsabilidade da CONTRATADA, mas que afetem aqueles sob sua responsabilidade;

3.2.3.9.9. Bug de software de fabricante para o qual não exista correção, ou solução de contorno já documentada, desde que demonstrada a diligência da CONTRATADA para obter a resolução tempestivamente;

3.2.3.9.10. Problema de hardware de qualquer espécie que não tenha sido causado pelo mau uso pela CONTRATADA;

3.2.3.9.11. Caso fortuito ou de força maior, classificados a critério exclusivo da CONTRATANTE.

3.2.3.10. Gestão de mudanças;

3.2.3.10.1. Deverá documentar e realizar a gestão da informação sobre as configurações do ambiente;

3.2.3.10.2. Toda mudança deve ser documentada e mantida em repositório da CONTRATANTE durante a vigência do contrato;

3.2.3.10.3. Levantamento de requisitos e riscos para mudanças previstas dentro do escopo de licenciamento contratado.

3.2.4. Perfis de Atendimento:

3.2.4.1. A CONTRATADA deve manter, presencialmente, no mínimo 4 (quatro) Analistas de Suporte, os quais deverão realizar uma escala de revezamento com regime de 24x7, nas dependências da CONTRATANTE. Em caso de necessidade de alocação de novos

analistas, estes poderão ser alocados de forma remota. Além disso, 1 (um) Gerente Técnico remoto, deverá estar disponível em horário comercial e realizar no mínimo 12 horas semanais em escala de trabalho presencial e de forma remota sempre que necessário.

- 3.2.4.2. O Gerente Técnico designado pela CONTRATADA deve ter experiência mínima comprovada de 5 (cinco) anos em gerência de suporte técnico ou projetos de suporte, em ambiente de Infraestrutura de Datacenter, especificamente em serviços de proteção de dados ou backup, admitidas as somas de diversas experiências, desde que não simultâneos, para a comprovação do tempo mínimo;
- 3.2.4.3. Adicionalmente a esse requisito, o Gerente Técnico também deverá comprovar certificação de alto nível na plataforma de backup, no caso de o fabricante da solução não dispor de programa de certificação, deve possuir curso oficial da solução contratada;
- 3.2.4.4. As qualificações do Gerente Técnico devem contemplar conhecimento sobre a totalidade dos serviços sob sua responsabilidade, nos termos descritos nos parágrafos anteriores, incluindo o conjunto de suas diversas experiências e/ou certificações. Não será permitida a multiplexação (entendido como simultaneidade no mesmo período) de papéis de Gerência Técnica e Profissional/Analista de Suporte por um mesmo profissional;
- 3.2.4.5. O Analista de Suporte, que atuará no serviço de proteção de dados, deve apresentar Certificações oficiais em Administração e Suporte da solução contratada. Na ausência dessas certificações (no caso de o fabricante da solução não dispor de programa de certificação), deve possuir curso oficial da solução contratada;
- 3.2.4.6. Todos os profissionais da CONTRATADA alocados na prestação do serviço objeto desse contrato deverão atender, adicionalmente aos critérios específicos de seus papéis, ao menos uma das seguintes condições:
- 3.2.4.7. Diploma, devidamente registrado, de conclusão de curso de nível superior, em área de Tecnologia da Informação, fornecido por

instituição de ensino superior, reconhecida pelo Ministério da Educação (MEC); OU

- 3.2.4.8. Diploma, devidamente registrado, de conclusão de qualquer curso de nível superior, fornecido por instituição de ensino reconhecida pelo MEC, acompanhado de certificado de curso de pós-graduação, na área de Tecnologia da Informação de, no mínimo, 360 horas, fornecido por instituição de ensino superior reconhecida pelo MEC, OU
- 3.2.4.9. 3 (três) anos de experiência amplamente comprovada de suporte a infraestrutura de ambiente de DATACENTER, adicionalmente aos anos necessários para comprovação do requisito específico de cada perfil/papel. A título de exemplo desse último critério: o Gerente Técnico que não disponha da diplomação superior estabelecida deverá comprovar no mínimo 6 (seis) anos de experiência.
- 3.2.4.10. Os requisitos de qualificação descritos são requeridos dos profissionais atuantes a serviço da contratante a qualquer momento da atuação, ou no conjunto da equipe presencial da CONTRATADA;
- 3.2.4.11. Em qualquer um dos casos, poderão ser aceitas certificações ou experiências bem documentadas, avaliadas como equivalentes pela equipe técnica da contratante, por serem em produto assemelhado OU por evidenciarem longa experiência, ou qualquer outro motivo considerado aceitável, a exclusivo e discricionário critério da contratante.
- 3.2.4.12. Neste documento estão listadas as qualificações mínimas exigidas da equipe presencial da CONTRATADA. Entretanto, reitera-se que a responsabilidade da CONTRATADA é sobre o serviço de proteção de dados;
- 3.2.4.13. Sendo assim, a CONTRATADA deve se certificar de que, dado o conjunto de seus profissionais, está apta, a garantir os serviços que a ela sejam delegados e que são suportados por todo o ambiente de software e hardware descritos ou que resultem de uma evolução tecnológica natural nos termos desse documento, durante o prazo de validade do contrato.

- 3.2.4.14. Os limites de isenção de responsabilidade da CONTRATADA pela disponibilidade dos serviços que serão aceitos como justificativas para desconsideração de descontos daquilo que a CONTRATADA demonstrar, tecnicamente, devem ser resultado de:
- 3.2.4.15. Ação ativa da contratante na Infraestrutura ou do desenvolvimento de suas aplicações;
- 3.2.4.16. Problemas em outros Serviços de Infraestrutura que não estejam sob a responsabilidade da CONTRATADA, mas que afetem aqueles sob sua responsabilidade;
- 3.2.4.17. Bug de software de fabricante para o qual não exista correção, ou solução de contorno já documentada, desde que demonstrada a diligência da CONTRATADA para obter a resolução tempestivamente;
- 3.2.4.18. Problema de hardware de qualquer espécie que não tenha sido causado pelo mau uso pela CONTRATADA;
- 3.2.4.19. Motivo fortuito ou de força maior, classificados a critério exclusivo da CONTRATANTE.
- 3.2.4.20. **Quanto aos perfis e papéis desempenhados:**
- 3.2.4.21. Os Analistas de Suporte serão os Técnicos da CONTRATADA, devidamente qualificados e credenciados junto a contratante, que executarão os serviços contratados;
- 3.2.4.22. O(s) Gerente(s) Técnico(s) será(ão) o(s) profissional(is) designado pela CONTRATADA para representar a mesma perante o órgão, durante a execução dos serviços, recebendo as demandas, administrando a equipe da CONTRATADA e zelando pelo eficaz atendimento aos requisitos contratuais;
- 3.2.4.23. Deverá haver sempre um profissional designado como Gerente Técnico da CONTRATADA, a qualquer hora, no período comercial. No caso de haver profissional da CONTRATADA prestando serviço para a contratante em horários não úteis, também deverá ser designado Gerente Técnico, que poderá ser acionado, ainda que remotamente, para receber determinações ou tratar questões, INCIDENTES e problemas que sejam inadiáveis, a critério do contratante;

- 3.2.4.24. Para atividades realizadas fora do horário de expediente do contratante, a CONTRATADA deverá disponibilizar números de celular e escala do(s) profissional(ais) que responderão pelo papel de Gerente(s) Técnico(s);
- 3.2.4.25. Na assinatura do contrato, a CONTRATADA designará um ou mais profissionais para ser o seu Gerente Técnico como também seus substitutos eventuais. Sempre que houver mudanças, esses representantes administrativos deverão ter as suas indicações formalizadas junto à contratante. O substituto eventual atuará somente na ausência do Gerente Técnico titular;
- 3.2.4.26. O(s) Gerente(s) Técnico(s) será(ão) designados pela CONTRATADA para gerenciar as atividades técnicas dos Profissionais de Suporte sob sua responsabilidade, recebendo as demandas, administrando a qualidade da execução dos serviços sob sua responsabilidade e zelando pelo eficaz atendimento aos requisitos contratuais;
- 3.2.4.27. **Caberá ao Gerente Técnico formalmente indicado:**
- 3.2.4.28. Informar o contratante problemas de quaisquer naturezas que possam impedir o bom andamento dos serviços;
- 3.2.4.29. Executar os procedimentos administrativos referentes aos recursos alocados para execução dos serviços contratados;
- 3.2.4.30. Assegurar que as determinações da contratante sejam disseminadas junto aos profissionais alocados à execução dos serviços;
- 3.2.4.31. Proceder ao registro de atas de reunião, as quais deverão ser disponibilizadas para o contratante sempre que solicitadas;
- 3.2.4.32. Zelar pelo cumprimento eficaz e eficiente dos requisitos contratuais segundo as melhores práticas;
- 3.2.4.33. Participar, quando convocado pela contratante, de reuniões de alinhamento de expectativas contratuais ou de planejamento de atividades;
- 3.2.4.34. Elaborar, quando solicitado, minuta de OS, para discussão, aprovação e autorização pelos demandantes, Fiscais Técnicos e Gestor do Contrato;

- 3.2.4.35. Responsabilizar-se pelo planejamento, acompanhamento e cumprimento integral de todas as tarefas nos prazos e qualidade exigidos;
- 3.2.4.36. O prazo requerido e alocar os profissionais necessários para a execução das ORDENS DE SERVIÇO;
- 3.2.4.37. Informar os profissionais da CONTRATADA que serão os responsáveis pelo atendimento da ORDEM DE SERVIÇO ou atividade;
- 3.2.4.38. Acompanhar a execução de todas as ORDENS DE SERVIÇO, garantindo o cumprimento dos Níveis Mínimos de Serviço;
- 3.2.4.39. Informar à contratante sobre problemas de qualquer natureza que possam impedir o adequado atendimento das ORDENS DE SERVIÇO;
- 3.2.4.40. Realizar a entrega dos serviços e produtos previstos nas ORDENS DE SERVIÇO e nas demais obrigações deste edital;
- 3.2.4.41. Obter do Gestor do Contrato ou dos servidores por ele indicados, as assinaturas de autorização e ateste das ORDENS DE SERVIÇO a serem executadas ou concluídas, previamente a execução ou posterior a conclusão, respectivamente;
- 3.2.4.42. Atuar como representante da CONTRATADA para solução de qualquer dúvida, conflito ou desvio, em relação a questões técnicas envolvendo a prestação de serviço;
- 3.2.4.43. Deve possuir interlocução direta com o fabricante do software de proteção utilizado pela CONTRATADA;
- 3.2.4.44. Deve possuir autorização para abrir chamado diretamente com o fabricante;
- 3.2.4.45. **Suporte Técnico Especializado:**
 - 3.2.4.45.1. A CONTRATADA deverá assegurar junto ao fabricante da solução um suporte técnico especializado de alto nível, através de um recurso humano, para atuar como ponto único de contato, para fornecer assistência avançada em horário comercial através de telefone fixo, telefone móvel e e-mail. Caso este recurso humano esteja temporariamente indisponível, deve ser dado a opção de deixar uma mensagem

ou ser redirecionado para um engenheiro de suporte de nível avançado;

- 3.2.4.45.2. Estes serviços deverão ser prestados exclusivamente na modalidade remota, utilizando-se de ferramentas de acesso remoto através da Internet e permitida pelo Órgão (tal como Microsoft Teams), com total segurança e criptografia de dados, de forma que os recursos técnicos consigam acessar remotamente os servidores e dispositivos de rede para rápida resolução de problemas;
- 3.2.4.45.3. Fornecer detalhes técnicos e participar ativamente do processo de planejamento das contas e nas revisões de negócios para avaliar o estado do programa e na orientação estratégica em relação aos objetivos de negócio do Cliente;
- 3.2.4.45.4. Coordenar com o suporte técnico do fornecedor para a resolução de escalações de problema do produto para auxiliar na resolução mais rápida e reduzir o tempo de inatividade não planejado;
- 3.2.4.45.5. O fabricante emitirá relatório sempre que solicitado pelo CONTRATANTE, em papel e em arquivo eletrônico, preferencialmente em arquivo texto, com informações analíticas e sintéticas dos chamados da garantia abertos e fechados no período, incluindo:
 - 3.2.4.45.5.1. Quantidade de ocorrências (chamados) registradas no período;
 - 3.2.4.45.5.2. Número do chamado registrado e nível de severidade, inclusive aqueles com reabertura;
 - 3.2.4.45.5.3. Data e hora de abertura;
 - 3.2.4.45.5.4. Data e hora de início e conclusão do atendimento;
 - 3.2.4.45.5.5. Identificação do técnico do CONTRATANTE que registrou o chamado;
 - 3.2.4.45.5.6. Identificação do técnico do CONTRATANTE que atendeu ao chamado da garantia;
 - 3.2.4.45.5.7. Descrição do problema;

3.2.4.45.5.8. Descrição da solução;

3.2.4.45.5.9. Informações sobre eventuais escalações;

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

3.2.4.45.6. Deve possuir acesso direto ao sistema de chamados do fabricante para acompanhamento e escalonamento de prioridade;

3.2.4.45.7. Deve possuir acesso ao sistema do fabricante para informar possíveis bugs e solicitação de novas funcionalidades;

3.2.4.45.8. Deve possuir interlocução direta com os engenheiros de backoffice do fabricante, para escalonamento de chamados.

3.2.5. **SLA**

3.2.5.1. A CONTRATADA deve registrar no sistema de registro de chamados, seguindo os padrões definidos pela CONTRATANTE, todos os chamados registrados em seu sistema de forma a permitir à CONTRATANTE aferir o NMS e os atendimentos realizados;

3.2.5.2. São classificados 2 tipos de registro de chamados: INCIDENTE ou SOLICITAÇÃO.

3.2.5.3. Os chamados do tipo INCIDENTE são voltados para situações não previstas e que podem interferir diretamente na disponibilidade e/ou funcionamento da solução.

3.2.5.4. Os chamados do tipo SOLICITAÇÃO são voltados para atividades de melhoria, mudanças e/ou ajustes que não interferem na disponibilidade e/ou funcionamento da solução

3.2.5.5. Para cada tipo de registro de chamado há um NMS atribuído, considerando suas especificidades.

3.2.5.6. Chamados do tipo INCIDENTE

3.2.5.7. A hierarquia de severidade vai de 1 a 5, sendo a severidade 1 a de maior urgência, superior a todas as demais;

3.2.5.8. Os chamados técnicos devem ser categorizados nos seguintes níveis de severidade (rol exemplificativo):

CRITICIDADE	DESCRIÇÃO	PRAZO MÁXIMO DE ATENDIMENTO
Severidade 1 (Alta)	Sistema parado ou produto inoperante com impacto na	Atendimento dos chamados técnicos de nível de severidade 1 deve ser iniciado em

	operações críticas de negócio. Exemplos: Servidor de produção ou outro sistema inicial está inativo. Parte substancial dos dados essenciais corre risco de perda ou corrupção. Operações relacionadas ao negócio foram afetadas, falha que compromete a integridade geral do sistema ou dados	até 30 minutos e o chamado solucionado em até 12 horas corridas
Severidade 2 (Média/Alta)	Alto impacto no ambiente de produção ou grande restrição de funcionalidade. Exemplo: Ocorreu um problema no qual um recurso importante foi gravemente danificado. As operações podem continuar de forma limitada, embora a produtividade em longo prazo possa ser afetada negativamente.	O atendimento dos chamados técnicos de nível de severidade 2 deve ser iniciado em até 2 hora corrida e solucionado em até 24 horas corridas;
Severidade 3 (Média/Baixa)	O defeito não gera impacto ao negócio. Exemplo: Ocorreu um erro que causou impacto negativo limitado na operações.	O atendimento dos chamados técnicos de nível de severidade 3 deve ser iniciado em até 4 horas comerciais e solucionados em até 36 horas comerciais;
Severidade 4 (Baixa)	O problema é pequeno, ou de documentação. Exemplos: O problema não afetou as operações da contratante negativamente; Encaminhamento de solicitações e ou sugestões para novos recursos ou aprimoramento do software licenciado.	O atendimento dos chamados técnicos de nível de severidade 4 deve ser iniciado em até 4 horas comerciais e solucionados em até 36 horas comerciais;
Severidade 5	Investigação de solução definitiva	O atendimento dos chamados técnicos de nível de severidade 5, iniciados em até 12 (doze) horas comerciais e solucionados em até 360 (trezentas e sessenta) horas comerciais.

3.2.5.9. O nível de severidade dos chamados deve ser definido pela CONTRATANTE no momento de sua abertura;

3.2.5.10. O nível de severidade de um chamado pode ser reclassificado;

3.2.5.11. Os tempos de atendimento e resolução tem sua contagem iniciada a partir da abertura do chamado;

3.2.5.12. Caso a CONTRATADA apresente solução de contorno, a contagem do NMS do chamado original será suspensa até a apresentação da solução definitiva e será aberto chamado de investigação de solução definitiva em severidade 5;

3.2.5.12.1. É vedado o agendamento do chamado pela CONTRATADA sem a prévia aplicação de solução de contorno, exceto se autorizado pelo Órgão.

3.2.5.13. **Nível Mínimo de Serviço:**

3.2.5.13.1. Atendimento dos chamados técnicos de nível de severidade 1 deve ser iniciado em até 1 hora e o chamado solucionado em até 12 horas corridas;

- 3.2.5.13.2. O atendimento dos chamados técnicos de nível de severidade 2 deve ser iniciado em até 2 horas corridas e solucionado em até 24 horas corridas;
- 3.2.5.13.3. O atendimento dos chamados técnicos de nível de severidade 3 e 4 deve ser iniciado em até 4 horas comerciais e solucionados em até 36 horas comerciais;
- 3.2.5.13.4. O atendimento dos chamados técnicos de nível de severidade 5, iniciados em até 12 (doze) horas comerciais e solucionados em até 360 (trezentas e sessenta) horas comerciais.
- 3.2.5.14. Horas comerciais, para fins de cálculo do NMS, são as compreendidas entre 8 h e 18 h, horário de Brasília-DF, em dias úteis;
- 3.2.5.15. Por início de atendimento entende-se a alocação de técnico devidamente qualificado para efetuar a correção do problema ou o troubleshooting preciso, com interlocução direta com a equipe do Órgão.
- 3.2.5.16. Todos os profissionais que irão trabalhar de alguma maneira no projeto, inclusive técnicos, gerentes e procuradores da empresa, devem assinar termo de confidencialidade, sigilo e uso (Órgão);
- 3.2.5.17. Todos os profissionais que irão trabalhar de alguma maneira no projeto, inclusive analistas, gerentes e procuradores da empresa, devem ser previamente cadastrados para acesso remoto;
 - 3.2.5.17.1. A prestação de qualquer serviço somente será considerada iniciada após a assinatura do documento de confidencialidade, o devido credenciamento e a entrega, quando aplicável, dos certificados requeridos no Edital.
- 3.2.5.18. Em caso de necessidade de coleta de logs e demais informações que permitam o adequado troubleshooting, a CONTRATADA deve fazê-lo remota ou localmente, não devendo esperar que a equipe do Órgão se mobilize para esta ação;
- 3.2.5.19. A CONTRATADA deverá apresentar, mensalmente, até o quinto dia útil após o fechamento do ciclo de faturamento, relatório contendo as informações de data e hora de abertura e fechamento do chamado, nome do responsável pela abertura, nome do responsável pelo

atendimento, número de controle (protocolo), nível de severidade, descrição sucinta do chamado, NMS alvo e NMS atingido, justificativa para eventual violação de NMS, resumo executivo e oportunidades de melhoria;

3.2.5.20. A CONTRATANTE possui modelos de relatórios e informações desejadas consolidados ao longo do tempo por diferentes contratos. São relatórios em constante evolução e adaptação de acordo com o serviço prestado;

3.2.5.20.1. Estes modelos serão apresentados à licitante no momento da vistoria, caso seja realizada;

3.2.5.20.2. Na ausência da vistoria, os modelos serão apresentados à CONTRATADA durante a reunião de início de projeto;

3.2.5.20.3. É responsabilidade da CONTRATADA tomar estes modelos como parâmetro mínimo, propondo melhorias ao longo da prestação dos serviços.

3.2.5.21. O relatório deve permitir a mensuração dos tempos de NMS atingidos, detalhados por cada evento registrado no chamado;

3.2.5.22. O registro dos eventos nos chamados deve ser realizado de forma precisa, com “status” que permita identificar claramente se o evento deve ou não ser considerado no cálculo do NMS;

3.2.5.23. Chamados do tipo SOLICITAÇÃO:

3.2.5.23.1. Os Serviço de operação e suporte técnico especializado fazem parte desse escopo desse tipo de registro de chamado, serão demandados em situações de contingência, em rotinas operacionais, no esclarecimento de dúvidas ou em períodos de mudanças complexas no ambiente que ensejem a incorporação temporária de expertise, para realizar tarefas pré-determinadas;

3.2.5.23.2. A pedido do contratante, a CONTRATADA deve realizar, dentre outras atividades:

3.2.5.23.2.1. Download das versões/atualizações;

3.2.5.23.2.2. Aplicação das versões/atualizações.

3.2.5.23.2.3. Implementação de novas funcionalidades;

3.2.5.24. A hierarquia de prioridade vai de 1 a 4, sendo a prioridade 1 a de maior urgência, superior a todas as demais;

3.2.5.25. Os chamados técnicos devem ser categorizados nos seguintes níveis de severidade (rol exemplificativo):

3.2.5.26. **PRIORIDADE DESCRIÇÃO PRAZO MÁXIMO DE ATENDIMENTO**

PRIORIDADE	DESCRIÇÃO	PRAZO MÁXIMO DE ATENDIMENTO
Prioridade 1 (Alta)	Demanda que requer máxima atenção pois pode já estar interferindo na operação da solução e/ou alguma funcionalidade.	Até 2 horas comerciais
Prioridade 2 (Média/Alta)	Demanda que precisa ser realizada pois pode gerar impacto à solução em curto prazo.	Até 08 horas comerciais
Prioridade 3 (Média/Baixa)	Demanda que pode ser realizada de forma planejada.	Até 16 horas comerciais
Prioridade 4 (Baixa)	Demanda que precisa ser estudada e alinhada com outras equipes ou que não tenham os requisitos planejados.	Até 24 horas comerciais

3.2.5.27. O nível de prioridade dos chamados deve ser definido pela CONTRATANTE no momento de sua abertura;

3.2.5.28. O nível de severidade de um chamado pode ser reclassificado;

3.2.5.29. Os tempos de atendimento e resolução tem sua contagem iniciada a partir da abertura do chamado;

3.2.5.30. Nível Mínimo de Serviço:

3.2.5.30.1. Para chamados do tipo SOLICITAÇÃO não há prazo específico para execução, visto que a complexidade e esforço das demandas podem ser diferentes.

3.2.5.30.2. O prazo de execução será acordado entre as partes no momento do atendimento do chamado.

3.2.5.31. Horas comerciais, para fins de cálculo do NMS, são as compreendidas entre 8 h e 18 h, horário de Brasília-DF, em dias úteis;

3.2.5.32. Por início de atendimento entende-se a alocação de técnico devidamente qualificado para efetuar a correção do problema ou o troubleshooting preciso, com interlocução direta com a equipe do Órgão.

- 3.2.5.33. Todos os profissionais que irão trabalhar de alguma maneira no projeto, inclusive técnicos, gerentes e procuradores da empresa, devem assinar termo de confidencialidade, sigilo e uso (Órgão) ;
- 3.2.5.34. Todos os profissionais que irão trabalhar de alguma maneira no projeto, inclusive técnicos, gerentes e procuradores da empresa, devem ser previamente cadastrados para acesso remoto;
 - 3.2.5.34.1. A prestação de qualquer serviço somente será considerada iniciada após a assinatura do documento de confidencialidade, o devido credenciamento e a entrega, quando aplicável, dos certificados requeridos no Edital.
- 3.2.5.35. Em caso de necessidade de coleta de logs e demais informações que permitam o adequado troubleshooting, a CONTRATADA deve fazê-lo remota ou localmente, não devendo esperar que a equipe do Órgão se mobilize para esta ação;
- 3.2.5.36. A CONTRATADA deverá apresentar, mensalmente, até o quinto dia útil após o fechamento do ciclo de faturamento, relatório contendo as informações de data e hora de abertura e fechamento do chamado, nome do responsável pela abertura, nome do responsável pelo atendimento, número de controle (protocolo), nível de severidade, descrição sucinta do chamado, NMS alvo e NMS atingido, justificativa para eventual violação de NMS, resumo executivo e oportunidades de melhoria;
- 3.2.5.37. A CONTRATANTE possui modelos de relatórios e informações desejadas consolidados ao longo do tempo por diferentes contratos. São relatórios em constante evolução e adaptação de acordo com o serviço prestado;
- 3.2.5.38. Estes modelos serão apresentados à licitante no momento da vistoria, caso seja realizada;
- 3.2.5.39. Na ausência da vistoria, os modelos serão apresentados à CONTRATADA durante a reunião de início de projeto;
- 3.2.5.40. É responsabilidade da CONTRATADA tomar estes modelos como parâmetro mínimo, propondo melhorias ao longo da prestação dos serviços.

- 3.2.5.41. O relatório deve permitir a mensuração dos tempos de NMS atingidos, detalhados por cada evento registrado no chamado;
- 3.2.5.42. O registro dos eventos nos chamados deve ser realizado de forma precisa, com “status” que permita identificar claramente se o evento deve ou não ser considerado no cálculo do NMS;

3.3. REQUISITOS DE SEGURANÇA DA INFORMAÇÃO

- 3.3.1. A prestação de serviço deverá ser realizada no ambiente tecnológico da CONTRATANTE de maneira a garantir o rastreo e o controle ao acesso às informações de caráter sigiloso, quando ocorrer. Quando essa prestação ocorrer na modalidade não-presencial, deverá ser solicitado o acesso via VPN (Virtual Private Network) à COTIN, que deliberará sobre o pedido.
- 3.3.2. A CONTRATADA deverá observar as políticas, os padrões, as arquiteturas, os métodos e as técnicas previamente estabelecidas pela CONTRATANTE.
- 3.3.3. A CONTRATADA obriga-se, durante o curso do contrato e após o seu término, ao mais completo e absoluto sigilo com relação a toda informação de qualquer natureza referente às atividades da CONTRATANTE, das quais venha a ter conhecimento ou venha a ter acesso por força do cumprimento do presente contrato, não podendo sob qualquer pretexto, utilizá-las para si, invocar, revelar, reproduzir ou delas dar conhecimento a terceiros, responsabilizando-se e sujeitando-se às legislações vigentes.
- 3.3.4. Desta forma, para garantir a confidencialidade e segurança das informações será celebrado entre a CONTRATADA e a CONTRATANTE o Termo de Compromisso de Manutenção de Sigilo (**ANEXO C**).
 - 3.3.4.1. Após a assinatura do contrato, a CONTRATADA por meio de seu representante, assinará o Termo de Compromisso de Manutenção de Sigilo.
 - 3.3.4.2. A CONTRATADA deverá disponibilizar Termo de Ciência (**ANEXO B**) em que seus profissionais declarem estar cientes das responsabilidades pela manutenção de sigilo e confidencialidade. O Termo de ciência deverá ser assinado somente pelos funcionários que vier a executar as atividades referente a solução contratada.

- 3.3.5. Informações Confidenciais, significam os dados ou informações confidenciais desenvolvidas ou adquiridas pela CONTRATANTE ou cuja divulgação ou utilização não autorizada, por qualquer das partes, poderá ser prejudicial a um ou a outro.
- 3.3.6. A CONTRATADA deverá submeter-se às políticas de segurança da informação e assumir todos os possíveis danos físicos e/ou materiais causados a CONTRATANTE ou a terceiros, advindos de imperícia, negligência, imprudência ou desrespeito às normas de segurança, quando da execução dos serviços, sempre atentando aos princípios de:
- 3.3.6.1. Disponibilidade – garantir aos usuários, autorizados pelo gestor do contrato, acesso às informações e aos locais de instalação dos ativos de rede, quando necessário, disponibilizando, ainda, todas as informações solicitadas pelo gestor ou fiscais quanto aos serviços executados e as condições atuais da estrutura da rede (fragilidade, oportunidades de implementações e melhorias, etc.);
 - 3.3.6.2. Integridade - guardar a exatidão e inteireza das informações e, ainda, documentar as atividades realizadas, objetivando manter a consistência das informações contidas nos arquivos com as condições reais das instalações;
 - 3.3.6.3. Confidencialidade - garantir que as informações sejam acessíveis somente ao pessoal autorizado, não fornecendo arquivos digitalizados ou mesmo impressos a pessoas que não foram autorizadas pelo gestor do contrato;
 - 3.3.6.4. Autenticidade - todas as comunicações entre a contratada e a CONTRATANTE deverão ser formalizadas e todos os documentos devidamente identificados com os dados pessoais dos responsáveis, garantindo a autenticidade dos documentos e a possibilidade de auditoria das atuações das partes envolvidas;
- 3.3.7. A CONTRATANTE e a CONTRATADA tratarão sigilosamente todas as informações confidenciais, produtos e materiais que as contenham, não podendo ser copiados ou reproduzidos, publicados, divulgados ou de outra forma colocados à disposição, direta ou indiretamente, de qualquer pessoa, a não ser empregados e agentes da CONTRATANTE e/ou da Licitante vencedora que deles necessitem para desempenhar

as suas funções no CONTRATANTE, sem que para tanto seja devido o consentimento prévio da CONTRATANTE.

- 3.3.8. As partes se obrigam a instruir sua equipe e prepostos a respeito das presentes disposições, as quais deverão ser observadas mesmo após o término ou cancelamento futuro do contrato.
- 3.3.9. A CONTRATADA responderá pelo não cumprimento, por quaisquer de seus funcionários, das normas e procedimentos de segurança da informação da CONTRATANTE.
- 3.3.10. É de responsabilidade da CONTRATADA garantir o tratamento de dados pessoais de acordo com a Lei Geral de Proteção de Dados Pessoais (LGPD), Lei nº 13.709 de 2018, com o objetivo específico de assegurar a proteção, privacidade e transparência de dados de pessoas físicas.

4. ESTIMATIVA DAS QUANTIDADES PARA A CONTRATAÇÃO

- 4.1. O dimensionamento da solução pretendida foi realizado com base no cenário levando em consideração as necessidades atuais da infraestrutura e com provisionamento para futuras ampliações no ambiente da COTIN/SAT/SEFAZ-MS.
- 4.2. As quantidades a serem contratadas foram definidas da seguinte forma:
 - 4.2.1. Licenças de Software de Backup/Restore com licenciamento de 36 meses;
 - 4.2.2. 1 (um) Repositório de Backup de curta retenção, em alta disponibilidade, composto de no mínimo 2 (dois) nós configurados como cluster ativo/ativo
 - 4.2.3. 1 (um) Repositório de Backup de longa retenção, em alta disponibilidade, composto de no mínimo 2 (dois) nós configurados como cluster ativo/passivo.
 - 4.2.4. Serviços de Operação e Suporte Técnico Especializado.

5. LEVANTAMENTO DE MERCADO

- 5.1. Dentro do presente estudo, foram analisados processos de contratações semelhantes feitas por outros órgãos e entidades, por meio de consultas a outros editais, com a finalidade de identificar a existência de novas metodologias, tecnologias ou inovações que melhor atendessem às necessidades, e as que foram identificadas foram incorporadas nesta contratação em análise.
- 5.2. Foram analisadas as seguintes alternativas para atendimento às necessidades elencadas:

5.2.1. **Cenário (1):** Outsourcing da solução de proteção de dados: incluindo o fornecimento de solução como serviço, envolvendo hardware, software, instalação, treinamento, customização, suporte técnico e manutenção.

5.2.2. **Cenário (2):** Aquisição da solução de proteção de dados: inclui a aquisição de todos os equipamentos e dos softwares, sem a instalação, treinamento, customização, suporte técnico e manutenção, estes ficando a cargo da Administração.

5.3. A análise comparativa das soluções observou as seguintes diretrizes:

Diretriz	Cenário (1)	Cenário (2)
Aderência aos padrões tecnológicos adotados pelo Estado	A solução atende aos padrões tecnológicos adotados pelo Estado.	A solução não atende aos padrões tecnológicos adotados pelo Estado.
Disponibilidade de solução de TIC similar em outro órgão ou entidade da Administração Pública	Encontramos a utilização deste modelo de solução de TIC em diversos outros editais e contratos da Administração Pública.	Encontramos a utilização deste modelo de solução de TIC em diversos outros editais e contratos da Administração Pública.
Alternativas do mercado, inclusive quanto a existência de software livre ou gratuito	Não se aplica.	Não se aplica.
Aderência às regulamentações da ICP-Brasil e modelo eARQ	Não se aplica.	Não se aplica.
Necessidades de adequação do ambiente	Não é necessário adequar o ambiente do órgão ou entidade para implantar a solução.	Não é necessário adequar o ambiente do órgão ou entidade para implantar a solução.
Diferentes modelos de prestação dos serviços	Este modelo preconiza a contratação de solução através dos conceitos atuais de IAAS (infraestrutura como serviço). Tem sido amplamente utilizada, é estabelece a terceirização integral dos serviços.	Este modelo estabelece a aquisição de toda a solução, agregando os equipamentos e softwares ao patrimônio, e mantém o encargo de gestão e controle da solução para o Estado.
Diferentes tipos de soluções em termos de especificação, composição ou características	Independente da solução a ser adotada, todas deverão possuir especificação e características semelhantes.	Independente da solução a ser adotada, todas deverão possuir especificação e características semelhantes.
Possibilidade de aquisição na forma de bens ou contratação como serviço	A solução prevê a contratação integralmente como serviço.	A solução prevê a aquisição (fornecimento) de bens.
Ampliação ou substituição da solução implantada	Ampliação e substituição viável, através de nova contratação ou aditivo ao contrato de prestação de serviços	Ampliação viável, através de aquisição de novos bens. A substituição irá demandar nova

		aquisição e substituição de todo o patrimônio adquirido. Necessário a aquisição de licenças a cada 12 ou 36 meses para manutenção do ambiente em funcionamento.
--	--	--

6. ESTIMATIVA DO VALOR DA CONTRATAÇÃO

6.1. A definição e documentação da estimativa de preços referenciais foram baseadas nas seguintes premissas:

6.1.1. Orçamentos obtidos mediante proposta comercial no mês de março de 2024, conforme valores e referências abaixo:

Item	EMPRESA	CNPJ	DESCRIÇÃO	QTD	Unid.	Prazo	VALOR UNITÁRIO	TOTAL
01	Norden Tecnologia Ltda	20.022.974/0001-83	Solução de Serviços gerenciados de proteção de dados, incluindo a disponibilização de appliance de backup/restore (on-premise), instalação, configuração e suporte, pelo período de 36 meses.	400	TB	36 meses	R\$ 2.385,00	R\$ 34.344.000,00
01	Arvvo Tecnologia Consultoria e Serviços	25.359.140/0001-81	Solução de Serviços gerenciados de proteção de dados, incluindo a disponibilização de appliance de backup/restore (on-premise), instalação, configuração e suporte, pelo período de 36 meses.	400	TB	36 meses	R\$ 2.408,50	R\$ 34.682.400,00

01	Vönk Tecnologi a da Informaçã o Ltda-ME	28.840 .741/0 001-08	Solução de Serviços gerenciados de proteção de dados, incluindo a disponibilizaçã o de appliance de backup/restore (on-premisse), instalação, configuração e suporte, pelo período de 36 meses.	400	TB	36 meses	R\$ 2.300,00	R\$ 33.120.000,00
----	---	----------------------------	--	-----	----	-------------	--------------	----------------------

6.2. A concretização da pesquisa de preços e memórias de cálculo resultou nos seguintes valores:

6.2.1. O valor estimado *global* (36 meses) da presente contratação é de R\$ 34.048.800,00 (Trinta e quatro milhões e quarenta e oito mil e oitocentos reais).

6.2.2. O valor estimado *mensal* da presente contratação é de R\$ 945.800,00 (Novecentos e quarenta e cinco mil e oitocentos reais).

6.2.3. As propostas estão anexa a este Estudo Técnico Preliminar.

6.3. Nos valores descritos já estão incluídos impostos, tributações e taxas necessárias para execução dos serviços propostos, conforme a legislação tributária vigente, cujo recolhimento é de total responsabilidade da CONTRATADA.

6.4. A planilha de composição de custos unitários da Solução de Tecnologia da Informação e Comunicação constará como anexo ao Termo de Referência.

7. DESCRIÇÃO DA SOLUÇÃO COMO UM TODO

7.1. SOLUÇÃO ADOTADA:

7.1.1. Dentre as soluções passíveis de atendimento as necessidades levantadas, optamos pela constante no **Cenário (1)**: Outsourcing da solução de proteção de dados: incluindo o fornecimento de solução como serviço, envolvendo hardware, software, instalação, treinamento, customização, suporte técnico e manutenção.

7.2. JUSTIFICATIVA DA ESCOLHA DA SOLUÇÃO:

7.2.1. A solução escolhida é a proposta no cenário 1, que é o outsourcing da solução de proteção de dados, pois a alternativa observada no cenário 2, Aquisição da solução de proteção de dados, não se mostra vantajosa nos seguintes aspectos:

7.2.1.1. As tecnologias de informação, no caso as de proteção e segurança de dados são periodicamente atualizadas, com novas features de

retenção específica, disponibilização de novos recursos, atualização dos recursos tecnológicos, dentre outros aspectos. Adquirir os equipamentos não garante essa atualização constante, o que em curto período de tempo tornariam os ativos adquiridos obsoletos e inservíveis, obrigando o Estado a substituir constantemente a tecnologia já implantada, sob o risco de não garantir a proteção e continuidade de serviços necessária;

- 7.2.1.2. Todos os valores envolvidos na aquisição dos equipamentos e licenças deverão ser pagos em parcela única, o que dispenderia um grande desembolso por parte da administração;
- 7.2.1.3. O órgão não dispõe de equipe capacitada e em quantidade suficiente para a instalação, manutenção e operação dos equipamentos e serviços necessários para esta contratação.
- 7.2.1.4. A COTIN/SAT/SEFAZ-MS não dispõe de servidores com função de analistas especialistas em retenção e segurança de dados, que cubram as funções de gerenciamento e proteção de dados sensíveis, o que justifica buscar empresa especializada no mercado para esta finalidade;
- 7.2.1.5. Os licenciamentos dos equipamentos que compõem a solução possuem validade de 12 (doze) até 36 (trinta e seis) meses, o que demandaria após essa janela de período, uma nova licitação para aquisição de novas licenças, garantindo desta forma o pleno funcionamento da solução de segurança da informação.
- 7.2.1.6. Caso os dados permaneçam sem a devida retenção segura durante um determinado período, poderia comprometer todo o ambiente de TIC desta Coordenadoria e de negócios da SAT/SEFAZ, tornando o ambiente vulnerável perante aos diversos tipos de sinistros possíveis, dentre eles ataques cibernéticos com sequestro dos dados, que se não estiverem mantidos backupeados e seguros para restauração, compromete toda estrutura fazendária do estado.

- 7.2.2. Por outro lado, a contratação da solução por meio de outsourcing, garantirá inúmeros benefícios, podendo citar alguns:

- 7.2.2.1. Eliminação de investimentos iniciais com a aquisição de equipamentos e licenças;
- 7.2.2.2. Proporcionar a gestão efetiva do serviço de locação de acordo com a demanda, que, em consequência, possibilita a obtenção de indicadores de qualidade, desempenho, disponibilidade, utilização de recursos e custos de forma mais ágil e exata, permitindo melhor planejamento, tomadas de decisão e ações rápidas, cada vez mais demandadas pelas Unidades, especialmente aquelas finalísticas;
- 7.2.2.3. Reduzir de forma drástica as interrupções do serviço devido as manutenções corretivas, através da implantação e aplicação de acordos de níveis de serviço (Service Level Agreement - SLA);
- 7.2.2.4. Proporcionar o licenciamento de todos os equipamentos e softwares durante toda a vigência contratual, sendo de responsabilidade da empresa contratada efetuar a aplicação das licenças necessárias durante esse período;
- 7.2.2.5. O serviço de operação, manutenção e monitoramento da solução ofertada ficará a cargo da contratada, que deverá alocar os técnicos especializados e treinados na solução para realizar as atividades de instalação, manutenção, operação e troubleshooting. Ficar a cargo da COTIN/SAT/SEFAZ-MS, a fiscalização dos serviços prestados e gestão do contrato.

7.3. BENEFÍCIOS A SEREM ALCANÇADOS:

- 7.3.1. Poder estabelecer políticas de segurança de dados baseada em soluções de tecnologia modernas, capaz de suportar todo tipo de sinistro previsível;
- 7.3.2. Prover a Coordenadoria de Tecnologia da Informação, COTIN/SAT/SEFAZ-MS, de uma infraestrutura de segurança de dados robusta;
- 7.3.3. Garantir que a infraestrutura de retenção e recuperação de dados do Data Center da COTIN/SAT/SEFAZ-MS possua os requisitos necessários para atender as demandas de itens constantes no PETI-GOV.MS, bem como tenha a possibilidade de permitir, de forma segura, a ampliação da capacidade tecnológica em demandas futuras;
- 7.3.4. Assegurar que a recuperação e disponibilização dos dados após evento de sinistro, ocorra de forma rápida e sem corrupção dos dados, ou seja, de forma íntegra;
- 7.3.5. Visualização dos ambientes de backup em plataforma única, maximizando sua rotina;

- 7.3.6. Adequação às legislações vigentes, tais como LGPD – Lei Geral de Proteção de Dados (Lei nº 13.709/2018) e Marco Civil da Internet Lei nº 12.965/2014);
 - 7.3.7. Mitigação de riscos de paralização dos serviços de TI por perda de dados e/ou incapacidade de recuperação;
 - 7.3.8. Manter a qualidade na prestação de serviços frente aos desafios que a COTIN/SAT/SEFAZ-MS fatalmente deve enfrentar diante do advento de novas tecnologias e do crescimento da demanda pelos serviços digitais, dando segurança ao processo de Transformação Digital e automação de processos de negócio, garantindo a permanente integridade dos dados;
- 7.4. DESCRIÇÃO DA SOLUÇÃO COMO UM TODO:
- 7.4.1. Contratação de empresa especializada para fornecimento de solução de proteção de dados sob a modalidade de Serviços Gerenciados, envolvendo hardware, software, instalação, treinamento, customização e suporte, conforme especificações técnicas discurridas no subitem 3 - REQUISITOS DO NEGÓCIO, incluindo appliances (Repositórios de Backup de curta e longa retenção), Softwares (Licenças) e Operacionalização, necessários e suficientes para a prestação desses serviços, para atender a demanda da Coordenadoria de Tecnologia da Informação, COTIN/SAT/SEFAZ-MS pelo período de 36 (trinta e seis) meses.
 - 7.4.2. A solução deverá ser composta de, no mínimo:
 - 7.4.2.1. Licenças de Software de Backup/Restore com licenciamento de 36 meses;
 - 7.4.2.2. 1 (um) Repositório de Backup de curta retenção, em alta disponibilidade, composto de no mínimo 2 (dois) nós configurados como cluster ativo/ativo;
 - 7.4.2.3. 1 (um) Repositório de Backup de longa retenção, em alta disponibilidade, composto de no mínimo 2 (dois) nós configurados como cluster ativo/passivo;
 - 7.4.2.4. Serviços de Operação e Suporte Técnico Especializado;
 - 7.4.2.5. Software de gerenciamento e geração de relatórios de toda a solução;
 - 7.4.2.6. Todos os softwares, firmwares e drivers de controle necessários ao perfeito funcionamento da solução, na última versão disponível;

- 7.4.2.7. Todas as licenças de utilização definitivas para os softwares, firmwares e drivers necessários ao perfeito funcionamento da solução;
- 7.4.2.8. Todos os cabos e acessórios necessários para a perfeita instalação, configuração e uso da solução;
- 7.4.2.9. Serviço especializado de instalação e customização de equipamentos, a montagem física dos equipamentos e seus respectivos acessórios;
- 7.4.2.10. Serviços de Suporte Técnico Especializado, Manutenção e Apoio deverão ser prestados pela empresa contratada na forma on-site ou remoto, no regime 24X7;
- 7.4.2.11. Treinamento da solução;

7.5. CLASSIFICAÇÃO DOS BENS COMUNS:

- 7.5.1. O serviço objeto desta contratação é caracterizado como serviço comum, pois possui especificação usual de mercado e padrão de qualidade definidas em Edital, para os fins do disposto no inciso XIII do art.6º da Lei Federal nº 14.133/2021.

7.6. CARÁTER CONTINUADO DO OBJETO

- 7.6.1. A Solução a ser contratada, constante nesse estudo, tem caráter continuado, tendo em vista que se trata de objeto com características intrínsecas de essencialidade e habitualidade, cuja eventual paralisação da atividade contratada implica em prejuízo ao exercício das atividades da Contratante. Neste aspecto, o objeto contratado é configurado pela necessidade de prestação de modo permanente, e a necessidade desta estende-se continuamente, por mais de um exercício financeiro.

8. JUSTIFICATIVA PARA O PARCELAMENTO OU NÃO DO OBJETO

- 8.1. É sabido que o parcelamento da solução é a regra, devendo a licitação ser realizada por item sempre que o objeto for divisível, desde que se verifique não haver prejuízo para o conjunto da solução ou perda de economia de escala, visando propiciar a ampla participação de licitantes, que embora não disponham de capacidade para execução da totalidade do objeto, possam fazê-lo com relação a itens ou unidades autônomas.
- 8.2. Contudo, a contratação dos serviços em apreço em item único sem parcelamento é a que melhor atende às necessidades da SEFAZ/MS, pelas razões seguintes:
 - 8.2.1. A solução deve ser contratada de maneira completa, pois perfazem uma única solução, uma vez que os equipamentos devem ser compatíveis entre si e com os

softwares de gerenciamento. Ao fragmentar as contratações, não será possível garantir a compatibilidade dos itens de hardware e dos softwares a serem instalados;

- 8.2.2. Por se tratar de uma solução integrada, constituída por funcionalidades e serviços intrinsecamente ligados entre si, e considerando que todos os componentes devem ser de um mesmo fabricante, bem, como o serviço de suporte que devem ser realizados por profissional especializado na solução, não há viabilidade técnica para o parcelamento da solução por itens;
- 8.2.3. Não avaliamos restrição de mercado ao adquirir a solução de maneira global, visto que individualmente tratam-se de bens e materiais de uso comum e de requisitos padronizados, não havendo dificuldade das empresas em providenciar os bens e prestar os serviços requisitados;
- 8.2.4. No caso em análise, os serviços citados são indivisíveis, não havendo possibilidade de contratar o suporte técnico e a manutenção de fornecedores diferentes, tendo em vista que são serviços caracterizados pela interoperabilidade e interdependência, pois corriqueiramente as manutenções realizadas derivam de suporte técnico demandado, ou que demandam suporte técnico para sua correta implantação.
- 8.3. Não há viabilidade para formação de consórcios, visto que a estrutura da solução é única, não cabendo tal formação para fornecimento de objeto uno e indivisível.

9. RESULTADOS PRETENDIDOS

- 9.1. Ser o mais responsável possível na atribuição de gestão e zelo da infraestrutura tecnológica da SEFAZ-MS, mais especificamente no que tange aos dados e informações relativas ao trinômio Tributação, Arrecadação e Fiscalização, base fundamental da Superintendência de Administração Tributária do Estado de MS.
- 9.2. Ter maior capacidade, diversidade, garantia e confiabilidade de armazenamento, gravação, recuperação, segura e íntegra dos dados e informações, visando atender as demandas atuais e futuras.

10. PROVIDÊNCIAS A SEREM ADOTADAS PELA ADMINISTRAÇÃO PREVIAMENTE À CELEBRAÇÃO DO CONTRATO

- 10.1. Não foram identificadas necessidades de adequação do ambiente para execução contratual, em relação ao modelo que já é adotado.

11. CONTRATAÇÕES CORRELATAS E/OU INTERDEPENDENTES

11.1. Não se aplica.

12. POSSÍVEIS IMPACTOS AMBIENTAIS E RESPECTIVAS MEDIDAS DE TRATAMENTO

12.1. Não se aplica.

13. VIABILIDADE E ADEQUAÇÃO DA CONTRATAÇÃO

13.1. Conforme fundamentação acima, esta Equipe de Planejamento da Contratação considera que a Solução de Tecnologia da Informação e Comunicação escolhida é viável, com base nos elementos anteriormente apresentados neste Estudo Técnico Preliminar, além de ser necessária para o atendimento das necessidades e interesses da COTIN/SAT/SEFAZ/MS.

13.2. A contratação obedece às disposições do Decreto Estadual n. 15.606 de 12 de fevereiro de 2021 e está em harmonia com o Objetivo Estratégico (OE8 – Estabelecer os procedimentos de segurança da informação e de proteção de dados) presente no Plano Estratégico de Tecnologia da Informação (PETI-GOV.MS 2021-2023) aprovado conforme Deliberação CETI n. 03 de 23 de abril de 2021, publicado no Diário Oficial do Estado de MS em 30 de abril de 2021

14. ASSINATURA

Campo Grande, 29 de janeiro de 2025.

Nome: **Vicente da Fonseca Bezerra Júnior**

Cargo: Auditor Fiscal da Receita Estadual

Nome: **Cláudio Norikazu Uemura**

Cargo: Analista de Tecnologia da Informação

Aprovado em: ____ / ____ / ____

Nome: **Flávio César Mendes de Oliveira**

Cargo: Secretário de Estado de Fazenda

15. RELAÇÃO DE ANEXOS

- ANEXO A – PROPOSTAS: NORDEN IT; ARVVO TECNOLOGIA; VONK TECNOLOGIA.
- ANEXO B – TERMO DE CIÊNCIA.
- ANEXO C – TERMO DE COMPROMISSO.