

INSTITUTO NACIONAL DE CARDIOLOGIA

Termo de Referência 86/2026

Informações Básicas

Número do artefato	UASG	Editado por	Atualizado em
86/2026	250059-INSTITUTO NACIONAL DE CARDIOLOGIA	NATASHA DE SOUZA ARRUDA	12/06/2026 16:25 (v 0.8)
Status			
ASSINADO			

Outras informações

Categoria	Número da Contratação	Processo Administrativo
VII - contratações de tecnologia da informação e de comunicação/Bens de TIC		33409.007123/2025-02

1. CONDIÇÕES GERAIS DA CONTRATAÇÃO

- 1.1. O presente Termo refere-se à aquisição de solução integrada de Tecnologia da Informação e Comunicação (TIC) para implantação e sustentação de infraestrutura de Datacenter On-Premise, contemplando o fornecimento de bens e a prestação de serviços associados ao seu ciclo de vida, incluindo: entrega, instalação física e lógica, configuração, integração, testes, operação assistida e transferência de conhecimento.
- 1.2. A solução abrange, no mínimo: (i) servidores de processamento de uso geral; (ii) servidores com aceleração por unidades de processamento gráfico (GPUs), destinados a cargas computacionais especializadas; (iii) sistemas de armazenamento de dados de alto desempenho, com mecanismos de redundância, proteção e alta disponibilidade; (iv) sistema de backup e (iv) equipamentos de rede necessários à conectividade, segmentação e segurança do ambiente.
- 1.4. A solução deverá ser entregue em pleno funcionamento, integrada ao ambiente tecnológico existente, com todos os seus componentes devidamente licenciados, documentados e operacionais, conforme condições, especificações técnicas, métricas de desempenho e critérios de aceitação definidos neste Termo de Referência, visando atender às demandas institucionais do Instituto Nacional de Cardiologia (INC).
- 1.5 Dos preços, especificações e quantitativos, as especificações do objeto, as quantidades de cada item são as que seguem:

Lote	Item	Especificação	CATMAT CATSER	Métrica ou Unidade de Medida	Quantidade	Valor Unitário	Valor Total
	1	Servidor Rack Tipo 1U – 2 Procs. / 256 GB RAM	476881	Unidade	5		
	2	Servidor Rack Tipo 1U – 2 Procs. / 1.536 GB RAM	481693	Unidade	2		
	3	Switch L3 com 48 Portas Fixas 1/10/25GbE e 6 Portas 100GbE	481771	Unidade	2		

Único	4	Infraestrutura de Armazenamento de Dados	622412	Unidade	1		
	5	Servidor Rack Tipo 1U – 1 Proc / 128 GB RAM	622412	Unidade	1		
	6	Appliance Scale-Out NAS para Armazenamento de Dados	476654	Unidade	1		
	7	Servidor Rack Tipo 1U – 2 Procs / 256 GB RAM	476881	Unidade	1		
	8	Software de Proteção e Recuperação de Dados	27464	Unidade	1		
	9	Appliance de Proteção e Recuperação de Dados	476654	Unidade	1		

1.6 Utilização do Sistema de Registro de Preço

1.6.1 A contratação utilizará o Sistema de Registro de Preços (SRP), estando a administração ciente do previsto no Inciso I do Art. 2º do Decreto Nº 11.462, de 31 de março de 2023, onde é definido o Sistema de Registro de Preços (SRP) como conjunto de procedimentos para a realização, mediante contratação direta ou licitação nas modalidades pregão ou concorrência, de registro formal de preços relativos à prestação de serviços, às obras e à aquisição e à locação de bens para contratações futuras, assim como a jurisprudência do TCU, a exemplo dos Acórdãos 113/2014, 757/2015 e 119/2016, todos do Plenário, não sendo o objetivo dessa contratação a elaboração de contrato único abarcando a totalidade do seu objeto, de forma a empenhar todos os itens constantes na Ata de Registro de Preços de uma única vez, e sim a realização de empenhos parcelados.

1.6.2 A utilização do Sistema de Registro de Preços (SRP) se apresenta como opção mais adequada à conveniência administrativa, de acordo com a realidade orçamentária anual dessa unidade, visto que o recurso orçamentário depende de descentralização fragmentada ao longo do ano, e o SRP permite a execução parcelada da despesa, conforme liberação do fluxo orçamentário ao longo do exercício financeiro.

De acordo com o **Decreto 11.462/2023** que regulamenta os **artigos 82 a 86 da Lei 14.133/2021**:

Art 3º O SRP poderá ser adotado quando a Administração julgar pertinente, em especial:

(...)

II - quando for conveniente a aquisição de bens com previsão de entregas parceladas (...).

1.6.3 Em relação ao Inciso II do Art. 3º do Decreto Nº 11.462, de 31 de março de 2023, a contratação contemplará a instalação de equipamentos se dará conforme o cronograma de implantação constante nesse Termo de Referência, que deverá ser executado de forma coordenada e parcelada, podendo inclusive fazer uso de recursos orçamentários de mais de um exercício financeiro e de mais de uma ação orçamentária. Adicionalmente, os equipamentos e softwares contam com período de garantia e suporte que devem iniciar o período de cobertura quando da efetiva instalação dos equipamentos. Dessa forma, devido aos pontos elencados, justifica-se o uso do SRP.

1.7. Classificação do objeto quanto à heterogeneidade ou complexidade

1.7.1 O objeto desta contratação não se enquadra como sendo de bem de luxo, conforme Decreto nº 10.818, de 27 de setembro de 2021.

1.7.2 O objeto desta aquisição, assim como seus componentes são caracterizados como comum, uma vez que se trata de renovação dos ativos de infraestrutura de TI do Datacenter do Instituto Nacional de Cardiologia.

1.7.3 O presente objeto caracteriza-se por se enquadrar como Fornecimento Não-Contínuo, na forma do artigo 105 da Lei nº 14.133 de 2021, bem como preconiza o Estudo Técnico Preliminar.

1.7.4 A Solução objeto da presente contratação é classificada predominantemente como aquisição de material permanente.

1.7.5 A classificação do objeto como predominantemente uma aquisição de material é fundamentada em uma análise criteriosa das características do projeto, bem como nas diretrizes estabelecidas na Instrução Normativa SGD/ME nº 94, de 23 de dezembro de 2022, regida pela Lei nº 14.133.

1.7.6 A referida instrução normativa define uma "Solução de TIC" como um "conjunto de bens e/ou serviços que apoiam processos de negócio mediante a conjugação de recursos de TIC". Esta definição reconhece que uma solução de TIC pode ser composta tanto por bens materiais quanto por serviços, o que proporciona flexibilidade na interpretação da natureza da aquisição em questão.

1.7.7 Dentre os argumentos que justificam a classificação do objeto como aquisições de material se destacam:

1.7.7.1 Natureza dos Componentes: Os componentes envolvidos neste projeto, como servidores, de dados e switches, são bens físicos ou materiais. Eles são objetos tangíveis que compõem a infraestrutura física do Datacenter.

1.7.7.2 Renovação de Hardware: O foco principal da renovação é a modernização da infraestrutura de TI por meio da substituição de equipamentos existentes. Isso implica a atualização de hardware, que se enquadra na categoria de aquisição de material.

1.7.7.3 Investimento de Capital: A aquisição desses bens materiais de TI geralmente envolve um investimento substancial de capital, alinhando-se mais com a natureza da aquisição de material do que com a contratação de serviços.

1.7.7.4 Especificações Técnicas: A seleção dos equipamentos é fortemente baseada em especificações técnicas, como capacidade de processamento, capacidade de armazenamento e velocidade de rede. Esses critérios estão relacionados diretamente aos aspectos materiais dos bens adquiridos.

1.7.7.5 Ciclo de Vida e Depreciação: Bens materiais de TI têm um ciclo de vida útil mensurável e estão sujeitos à depreciação. Isso é característico de aquisições de material, enquanto os serviços têm uma natureza diferente nesse aspecto.

1.7.8 Os itens que compõem do Objeto devem ser adquiridos e fornecidos com suas respectivas Garantias de implementação e funcionamento, desta forma, cabendo estar atrelado o serviço referente ao perfeito e completo funcionamento enquanto estiver vigente a garantia do equipamento fornecido.

1.7.9 O contrato, referente ao fornecimento e entrega do Objeto, deve oferecer maior detalhamento das regras que serão aplicadas em relação à vigência da contratação.

1.7.9.1 A natureza integrada da solução (hardware + software + garantia técnica) impõe um ciclo de vida tecnológico típico entre 5 e 7 anos, período no qual os ativos permanecem adequados em termos de desempenho e suporte do fabricante. Assim, o prazo inicial de 5 anos se mostra tecnicamente adequado para: amortização dos investimentos realizados, maturação da operação e estabilização do ambiente, obtenção de ganhos de eficiência operacional.

1.7.9.2 Sob o enfoque da economicidade, a contratação plurianual: reduz custos administrativos com sucessivas licitações, permite melhores condições comerciais (ganhos de escala e diluição de custos), evita substituições prematuras de infraestrutura ainda operacional e reduz o risco de descontinuidade contratual, que poderia implicar custos indiretos elevados.

Prazo de vigência

1.7.9.3 Dessa forma, o prazo de vigência proposto mostra-se tecnicamente justificado, economicamente vantajoso e juridicamente adequado, em conformidade com a Lei nº 14.133/2021 e com a IN SGD/ME nº 94/2022.

2. FUNDAMENTAÇÃO E DESCRIÇÃO DA NECESSIDADE DA CONTRATAÇÃO

2.1 A Tecnologia da Informação (TI) é essencial para o funcionamento eficiente de qualquer instituição, incluindo o Instituto Nacional de Cardiologia. No entanto, quando a infraestrutura de dados atual se torna obsoleta e não é mais possível contratar serviços de manutenção, que é o caso atual, é fundamental buscar uma solução que possa atender às demandas da instituição e garantir a segurança dos dados. Nesse contexto, a aquisição de infraestrutura de um novo Datacenter se apresenta como uma solução capaz de suprir as necessidades do Instituto.

2.2 Essa solução inclui servidores de processamento, armazenamento de dados de alto desempenho, sistemas de backup e alta disponibilidade e equipamentos de rede, bem como serviços de garantia e manutenção, a fim de atender às necessidades do Instituto Nacional de Cardiologia (INC).

2.3 Com a aquisição desta solução o Instituto Nacional de Cardiologia poderá modernizar sua infraestrutura de TI e contar com um ambiente de dados seguro e disponível a qualquer momento. A solução permitirá ao INC manter seus dados sensíveis de pacientes protegidos e disponíveis para acesso rápido pelos profissionais de saúde, garantindo a continuidade dos serviços de saúde e a segurança do paciente. Além disso, a solução é escalável, permitindo que o INC expanda sua infraestrutura de TI de acordo com as necessidades e demandas. Por essas razões, a aquisição de infraestrutura de um Datacenter on-premise é uma opção vantajosa e justificável para o Instituto Nacional de Cardiologia.

2.4 Essa solução permitirá que a instituição de saúde mantenha uma infraestrutura de TI moderna, escalável e gerenciável, atendendo às necessidades do setor de saúde e garantindo a continuidade dos serviços de saúde para seus pacientes. Justifica-se a composição do objeto em Lote, devido aos itens comporem uma Solução de Tecnologia de Informação Integrada, interligadas, convergentes e de dependência mútua, culminando no objeto de renovação dos ativos de infraestrutura Tecnológica do atual Datacenter, bem como mitigando eventuais incompatibilidades até mesmo despesas futuras no que se refere a versões ou impactos na comunicação de itens distintos.

2.5 A presente contratação está alinhada com o planejamento estratégico de TI do INC e foi prevista no Plano Anual de Contratações de 2025 do setor de Tecnologia da Informação. A modernização do Datacenter constitui uma demanda prioritária identificada no planejamento de TIC, em virtude do encerramento do suporte dos equipamentos atuais e da necessidade de adequar a infraestrutura às demandas crescentes. Houve a previsão orçamentária para esta finalidade, e os estudos técnicos foram iniciados em 2024, com execução programada para 2025, em consonância com as diretrizes da nova Lei de Licitações (Lei 14.133/2021). Assim, a contratação alinha-se ao planejamento institucional, garantindo que os investimentos em TI estejam coordenados com as metas de melhoria da infraestrutura e continuidade dos serviços legislativos.

2.6. A presente contratação está alinhada com o planejamento estratégico de TI do INC e foi prevista no Plano Anual de Contratações de 2026 do setor de Tecnologia da Informação. A modernização do Datacenter constitui uma demanda prioritária identificada no planejamento de TIC, em virtude do encerramento do suporte dos equipamentos atuais e da necessidade de adequar a infraestrutura às demandas crescentes. Houve a previsão orçamentária para esta finalidade, e os estudos técnicos foram iniciados em 2024, com execução programada para 2026, em consonância com as diretrizes da nova Lei de Licitações (Lei 14.133/2021). Assim, a contratação alinha-se ao planejamento institucional, garantindo que os investimentos em TI estejam coordenados com as metas de melhoria da infraestrutura e continuidade dos serviços legislativos.

2.7. Com base na necessidade de apresentar as justificativas da contratação previstas no art. 15 da IN SGD/ME nº 94 /2022, descreve-se:

2.7.1 Contextualização e Problema a Ser Resolvido

2.7.1.1 A presente contratação decorre da necessidade de substituição e modernização da infraestrutura de Datacenter do Instituto Nacional de Cardiologia (INC), atualmente caracterizada por elevado grau de obsolescência tecnológica, indisponibilidade de suporte do fabricante e limitações de capacidade operacional.

2.7.1.2 O ambiente atual apresenta riscos concretos à continuidade dos serviços institucionais, especialmente aqueles relacionados ao processamento e armazenamento de dados sensíveis de saúde, em razão de: indisponibilidade de peças e suporte técnico, aumento de falhas operacionais, limitação de desempenho e escalabilidade e exposição a vulnerabilidades de segurança.

2.7.2 Necessidade de Negócio

2.7.2.1 A contratação visa atender à necessidade institucional de: garantir a continuidade dos serviços assistenciais suportados por sistemas de informação, assegurar a disponibilidade, integridade e confidencialidade dos dados, suportar o crescimento da demanda computacional e viabilizar evolução tecnológica compatível com as necessidades do INC.

2.7.3 Alinhamento Estratégico

2.7.3.1 A contratação encontra-se alinhada ao Planejamento Estratégico de TIC do INC, ao Plano Anual de Contratações (PAC) e às diretrizes de governança e transformação digital da Administração Pública Federal.

2.7.3.2 Trata-se de iniciativa prioritária, vinculada à sustentação de serviços essenciais à atividade-fim da instituição.

2.7.4 Adequação da Solução de TIC

2.7.4.1 A solução proposta — infraestrutura de Datacenter On-Premise integrada — é tecnicamente adequada por: garantir controle direto sobre dados sensíveis, assegurar baixa latência e alto desempenho, permitir integração com sistemas legados, oferecer alta disponibilidade e resiliência e suportar cargas computacionais avançadas (incluindo uso de GPUs).

2.7.4.2 A solução contempla o ciclo completo de vida (fornecimento, implantação, garantia e manutenção), reduzindo riscos de descontinuidade e falhas de integração.

2.7.5 Justificativa da Modelagem da Contratação

2.7.5.1 Não Parcelamento da Solução:

2.7.5.1.1 A contratação em lote único é tecnicamente justificada pela natureza integrada e interdependente dos componentes da solução, considerando que: os elementos (servidores, armazenamento, backup, rede e serviços) operam de forma convergente, há necessidade de compatibilidade tecnológica plena e gerenciamento que deve ser unificado.

2.7.5.1.2 O parcelamento implicaria riscos relevantes, tais como: incompatibilidade entre componentes, aumento da complexidade de integração, dificuldade de responsabilização contratual e elevação do custo total da solução.

2.7.5.1.3 A solução combina bens e serviços de TIC, sendo os serviços essenciais para garantir operação contínua, assegurar níveis de serviço (SLA), viabilizar suporte técnico especializado, reduzir riscos operacionais.

2.7.5.1.4 Todos os itens que compõem a solução deverão ser adquiridos de um único fornecedor em atendimento ao inciso VIII do § 1º do Art. 18 da Lei nº 14.133, de 2021, motivo pelo qual deverão se elencados, em grupo único.

2.7.5.2 Dessa forma, a Equipe de Planejamento da Contratação considera inviável o parcelamento da solução, porém os itens que compõem a solução poderão ser adquiridos de forma parcelada, de acordo com a demanda da contratante para tornar a aquisição, técnica e economicamente viável.

2.7.6 Benefícios Esperados

2.7.6.1 A contratação proporcionará:

2.7.6.1.1 Aumento da disponibilidade dos sistemas críticos;

2.7.6.1.2 Melhoria de desempenho e capacidade de processamento;

2.7.6.1.3 Maior segurança da informação;

2.7.6.1.4. Escalabilidade da infraestrutura;

2.7.6.1.5. Redução de falhas e incidentes;

2.7.7 Riscos da Não Contratação

2.7.7.1 A não realização da contratação poderá resultar em: interrupção de sistemas essenciais, perda ou indisponibilidade de dados, comprometimento de serviços assistenciais, aumento de vulnerabilidades de segurança, impossibilidade de expansão tecnológica.

Diante do exposto, a contratação é necessária, adequada e vantajosa, atendendo plenamente aos objetivos institucionais e aos requisitos legais aplicáveis.

2.8. A oferta não se trata de serviços públicos digitais.

3. DESCRIÇÃO DA SOLUÇÃO COMO UM TODO CONSIDERADO O CICLO DE VIDA DO OBJETO E ESPECIFICAÇÃO DO PRODUTO

3.1 A modernização da infraestrutura de datacenter do Instituto Nacional de Cardiologia (INC) demanda não apenas a substituição de ativos obsoletos, mas a implementação de uma arquitetura tecnológica integrada, coesa e plenamente suportada, capaz de sustentar operações de missão crítica com elevados requisitos de desempenho, disponibilidade e segurança da informação.

3.2 Nesse contexto, a contratação de infraestrutura de Datacenter On-Premise observa o princípio da integração sistêmica dos componentes de TIC, conforme preconizado pela Instrução Normativa SGD/ME nº 94/2022, garantindo que os elementos de computação, armazenamento, rede e software atuem de forma coordenada, interoperável e sob governança unificada, sendo os elementos contidos na Solução escolhida plenamente apta para produzir os resultados pretendidos pela Administração.

4. REQUISITOS DA CONTRATAÇÃO

4.1 REQUISITOS TÉCNICOS DOS PRODUTOS E SERVIÇOS DE INSTALAÇÃO

4.1.1 SERVIDOR RACK TIPO 1U – 2 PROCS. / 256 GB RAM

Gabinete

4.1.1.1 Gabinete para instalação em rack de 19" através de sistema de trilhos deslizantes; 4.1.1.2 Altura máxima de 1U;

4.1.1.3 Deve possuir botão liga/desliga na parte frontal do equipamento;

4.1.1.4 Deve possuir suporte de no mínimo 10 (dez) baias para instalação de drives do tipo SAS/SATA;

4.1.1.5 Deverá ser entregue junto com o servidor, um kit de fixação para rack, do tipo retrátil, permitindo o deslizamento do servidor a fim de facilitar sua manutenção;

4.1.1.6 Possuir projeto tool-less, ou seja, não necessita de ferramentas para instalação/desinstalação de placas de expansão;

4.1.1.7 Deve possuir sistema de ventilação redundante e hot-pluggable para que a CPU suporte a configuração máxima e dentro dos limites de temperatura adequados para o perfeito funcionamento do equipamento, e que permita a substituição do mesmo com o equipamento em funcionamento.

4.1.1.8 Deverá ser fornecido com Módulo TPM 2.0 FIPS ou superior;

Fonte de alimentação

4.1.1.9 Mínimo de 2 (duas) fontes, suportando o funcionamento do equipamento na configuração ofertada mesmo em caso de falha de uma das fontes;

4.1.1.10 Deverá ser fornecido com sua quantidade máxima de fontes;

4.1.1.11 As fontes deverão ser totalmente redundantes e hot-pluggable permitindo a substituição de qualquer uma das fontes em caso de falha sem parada ou comprometimento do funcionamento do equipamento;

4.1.1.12 As fontes de alimentação devem possuir certificação 80Plus, no mínimo na categoria TITANIUM.

4.1.1.13 A fonte deve ter potência mínima de 1.500 watts;

4.1.1.14 As fontes devem possuir tensão de entrada de 100VAC a 240VAC a 60Hz, com ajuste automático de tensão; 4.1.1.15 Deverá acompanhar cabo de alimentação C13/C14 para cada fonte de alimentação fornecida.

Processador

4.1.1.16 O servidor deverá suportar processadores do tipo single-threaded, com até 144 núcleos, ou multi-threaded, com até 86 núcleos, por processador;

4.1.1.17 Equipado com 2 (dois) processadores de 32 núcleos do tipo multi-threaded, com arquitetura x86;

4.1.1.18 Deverá implementar mecanismos de gerenciamento do consumo de energia compatível com o padrão ACPI;

4.1.1.19 Deve suportar conjunto de instruções estendido compatível com padrão AVX-512;

4.1.1.20 Consumir no máximo 250W;

4.1.1.21 Frequência de clock interno de no mínimo 2.5 GHz;

4.1.1.22 Controladora de memória com suporte a DDR5 de no mínimo 6400 MT/s para 1 DIMM por canal, ou 5200 MT/s para 2 DIMMs por canal;

4.1.1.23 Link de comunicação do processador com o restante do sistema de 24 GT/s;

4.1.1.24 Memória cache de 288 MB – L3.

Desempenho

4.1.1.25 O processador ofertado deverá ter índice SPEC CPU2017 Integer Rate Results (Baseline) auditado de no mínimo 721 para 2 processadores. Os índices SPEC CPU2017 Integer Rate Results (Baseline) utilizados como referência serão validados junto ao site da Internet <https://www.spec.org/> Standard Performance Evaluation Corporation. Não serão aceitas estimativas para modelos / famílias de processadores não auditados pelo SPEC, resultados obtidos com a utilização de servidores em cluster, bem como estimativas em resultados inferiores ao mínimo especificado;

4.1.1.26 Não será aceito modelo de servidor não auditada pelo Standard Performance Evaluation Corporation ou auditada antes de 2017.

Memória RAM

4.1.1.27 Módulos de memória RAM tipo DDR5 RDIMM (Registered DIMM) com tecnologia de correção ECC (Error Correcting Code) e velocidade de, no mínimo, 6400 MT/s;

4.1.1.28 Deve possuir no mínimo 32 slots de memória DIMM;

4.1.1.29 Deve possuir 256 GB de memória instalada;

Circuitos integrados (chipset) e placa mãe

4.1.1.30 O chipset deve ser da mesma marca do fabricante do processador;

4.1.1.31 Possuir, no mínimo, 2 slots OCP 3.0 e 2 slots PCI Express 5.0;

4.1.1.32 Placa mãe da mesma marca do fabricante do equipamento, desenvolvida especificamente para o modelo ofertado. Não serão aceitas placas de livre comercialização no mercado;

Controladora de vídeo

4.1.1.33 Deve ser do tipo on board (integrado na placa mãe) ou placa de vídeo PCIe;

4.1.1.34 Resolução gráfica de 1024 x 768 pixels ou superior.

BIOS ou UEFI

4.1.1.35 Possuir UEFI (Unified Extensible Firmware Interface) ou BIOS (Basic Input Output System) totalmente compatível e desenvolvida para o servidor fornecido;

4.1.1.36 A BIOS/UEFI deve ser atualizável por software;

4.1.1.37 O servidor deve implementar mecanismos de garantia de integridade e autenticidade do código da BIOS /UEFI, antes de sua execução, por meio de assinatura digital que poderá ser validada usando chave criptográfica imutável armazenada em hardware;

4.1.1.38 O servidor deve prover mecanismos preliminares às atualizações de firmware da BIOS/UEFI e de firmware da controladora de gerenciamento remoto que assegurem que os pacotes de atualização de firmware possuam assinatura digital cuja autenticidade poderá ser verificada usando chave criptográfica imutável armazenada em hardware;

4.1.1.39 O servidor deverá ser capaz de restaurar, automaticamente, o estado da BIOS/UEFI para uma versão íntegra anterior, armazenada em área de memória oculta e protegida contra gravação, em casos de corrupção identificados durante a inicialização da BIOS/UEFI;

4.1.1.40 Deverá suportar escaneamento de BIOS Firmware em tempo real para detecção de código malicioso;

4.1.1.41 Deve possuir funcionalidade que permita que os discos locais do servidor sejam apagados de forma definitiva através de tecnologia de regravação de dados ou similar. Esta funcionalidade deve possibilitar que sejam definitivamente apagados quaisquer discos dentro do servidor, suportando discos físicos (HDDs), discos criptografados (SEDs) e dispositivos de flash SSDs e NVMe;

4.1.1.42 A console de gerenciamento local deverá implementar modo "System Lockdown", o qual deve impedir que usuários com menos privilégios façam alterações nas configurações do servidor;

4.1.1.43 A console de gerenciamento local deve possuir uma área de armazenamento oculta para a rápida recuperação da BIOS e do Sistema Operacional quando comprometidos;

4.1.1.44 Deverá permitir que as portas USB possam ser desativadas de maneira programada;

Portas de Comunicação

4.1.1.45 Todos os conectores das portas de entrada/saída devem ser identificados pelos nomes ou símbolos;

4.1.1.46 Possuir 3 (três) interfaces USB sendo, no mínimo duas destas interfaces no padrão 3.0;

4.1.1.47 Possuir, no mínimo, 1 (uma) porta de vídeo padrão VGA (DB-15);

Interface de Rede

4.1.1.48 Possuir 06 (seis) interfaces de rede de 10/25Gb DA/SFP28 em 2 ou 3 adaptadores distintos suportando taxas de transferência de 10Gbps e 25Gbps;

4.1.1.49 Suporte ao protocolo de virtualização VMQ

4.1.1.50 Suporte ao protocolo VXLAN

4.1.1.51 Possuir tecnologia de processamento TCP/IP offload LSO, RSS e TSS

Controladora RAID

4.1.1.52 Controladora RAID, compatível com discos padrão SAS 22.5 Gbps, SAS 12 Gbps, SATA/SAS 6 Gbps e drives NVMe;

4.1.1.53 Suportar e implementar RAID 0, 1 e 10;

4.1.1.54 Suportar expansão de capacidade de formatação on-line;

4.1.1.55 Permita detecção e recuperação automática de falhas e reconstrução, também de forma automática, dos volumes de RAID sem necessidade de reiniciar o equipamento;

4.1.1.56 Deverá permitir a operação em modo RAID e pass-through em discos distintos. Ou fornecer controladora RAID e controladora pass-through.

4.1.1.57 Suporte a recursos de hot swap para as unidades de disco;

4.1.1.58 Suportar implementação de disco Global Hot-spare;

4.1.1.59 Suportar Self-Monitoring Analysis and Reporting Technology (SMART).

Dispositivos de armazenamento padrão SSD com as seguintes características

4.1.1.60 Para a instalação do Sistema Operacional devem ser fornecidos 2 (dois) drives do tipo SSD (Solid State Drive) no

formato de 2,5 polegadas de, no mínimo, 480GB cada um, ligados em RAID1 através da controladora de discos especificada acima;

4.1.1.61 Devem ser do tipo hot plug e hot swap, que permita sua substituição sem a necessidade de desligar o equipamento, garantindo a continuidade das operações sem impacto para as aplicações;

4.1.1.62 Devem possuir DWPD igual a 1 medido pelo período de 5 anos;

4.1.1.63 Devem possuir taxa de transferência de, no mínimo, 6Gb/s;

4.1.1.64 Devem ser do tipo SATA Read Intensive;

4.1.1.65 Não serão aceitos discos em gabinetes externos ao servidor;

4.1.1.66 Não serão aceitas soluções baseadas em cartão SD ou similar;

Sistema Operacional

4.1.1.67 O servidor deverá ser ofertado com o sistema operacional OEM Windows Server 2025 Datacenter licenciado para todos os núcleos de todos os processadores;

4.1.1.68 O fabricante deve disponibilizar no seu respectivo web site, download gratuito de todos os Drivers dos dispositivos, BIOS e

Firmwares para o equipamento ofertado;

4.1.1.69 Apresentar declaração do fabricante informando que todos os componentes do objeto são novos (sem uso, reforma ou recondicionamento) e que não estão fora de linha de fabricação;

4.1.1.70 O modelo do equipamento ofertado deverá suportar o sistema operacional Windows Server 2022 ou superior. Esse item deverá ser comprovado através do HCL (Hardware Compatibility List) da Microsoft no link: <https://www.windowsservercatalog.com>;

4.1.1.71 O modelo do equipamento ofertado deverá suportar o sistema operacional Red Hat Enterprise Linux 9.4 ou posterior. Esse item deverá ser comprovado através do HCL (Hardware Compatibility List) da Red Hat no link: <https://hardware.redhat.com/hwcert/index.cgi>;

4.1.1.72 O modelo do equipamento ofertado deverá suportar o sistema de virtualização VMware ESXi 8.0 ou posterior. Esse item deverá ser comprovado através do Compatibility Guide da Broadcom no link: <https://compatibilityguide.broadcom.com/searchprogram=server&persona=live&column=partnerName&order=asc>;

Gerenciamento e Inventário

4.1.1.73 O equipamento deve possuir solução de gerenciamento do próprio fabricante através de recursos de hardware e software com capacidade de prover as seguintes funcionalidades:

4.1.1.74 O software de gerenciamento deverá estar licenciado para todas as funcionalidades requisitadas nestas especificações e unificar as operações de administração, monitoramento e gestão de tarefas de gerenciamento de todos os servidores fornecidos em uma única console gráfica.

4.1.1.75 O equipamento deve possuir interface de rede dedicada para gerenciamento que suporte nativamente a atribuição de endereçamento IP dinâmico;

4.1.1.76 Permitir o monitoramento remoto, de todo o hardware das condições de funcionamento dos equipamentos e seus componentes, tais como: processadores, memória RAM, controladora RAID, discos, fontes de alimentação, NICs e ventiladores;

4.1.1.77 Permitir acessar a BIOS ou UEFI remotamente;

4.1.1.78 Suportar os protocolos de criptografia SSL para acesso Web e SSH para acesso CLI;

4.1.1.79 Emitir alertas de anormalidade de hardware através do software de gerência e suportar o encaminhamento via e-mail e trap

SNMP;

4.1.1.80 Suportar autenticação local e através de integração com MS Active Directory/LDAP;

4.1.1.81 Deverá suportar autenticação de 2 fatores.

4.1.1.82 Permitir o controle remoto da console do servidor do tipo virtual KVM out-of-band, ou seja, independente de sistema operacional ou software agente;

4.1.1.83 Permitir a captura de vídeo ou tela de situações de falhas críticas de sistemas operacionais e inicialização do sistema (boot), possibilitando uma depuração mais aprimorada;

4.1.1.84 As funcionalidades de gerenciamento e monitoramento de hardware devem ser providas por recursos do próprio equipamento e independente de agentes ou sistema operacional;

4.1.1.85 A console virtual deverá ser acessível via interface HTML5 ou, caso necessite de algum tipo de plugin licenciado, por exemplo JAVA, deverá ser fornecido o licenciamento por pelo menos 5 anos;

4.1.1.86 Suportar os protocolos de gerenciamento, IPMI e SNMP v1/v2c/v3, WMI, SSH, WS MAN e REDFISH;

4.1.1.87 Permitir customizar alertas e automatizar a execução de tarefas baseadas em script;

4.1.1.88 O software de gerenciamento deverá permitir instalação remota de sistemas operacionais como Windows, Linux e VMware vSphere.

4.1.1.89 Permitir integração com o VMware vCenter de modo que o gerenciamento e inventário também possa ser realizado através do vSphere Web Client com informações referentes aos hosts (nome do host, endereço IP do host, configuração de CPU, memória, NIC, firmware), além de listar as versões de software e hardware em uso pelo host, controladoras de rede, RAID.

4.1.1.90 A integração com o VMware vCenter deverá permitir a redução nos tempos de resposta a eventos de hardware através de ações automáticas pré-estabelecidas pelo administrador, tais como, evacuação de máquinas virtuais em execução em host que venha emitir alertas de pré-falha de qualquer componente vital como CPU, memória e disco, e manter a estabilidade e a confiabilidade do ambiente através do gerenciamento de firmwares empregados no ambiente, garantindo conformidade entre todos os hosts ESXi;

4.1.1.91 Permitir configurar os seguintes parâmetros de hardware: WWN, BIOS, RAID, NIC, MAC, Virtual MAC Address, iSCSI Name, VLAN e perfil de QOS, através de templates pré-definidos;

4.1.1.92 Permitir a instalação, update e configuração remota de sistemas operacionais, drivers e firmwares, através de solução de deployment compatível com a solução ofertada;

4.1.1.93 Permitir estabelecer perfis de configuração com o inventário das versões de firmwares disponíveis para execução programada de verificações de conformidade das versões de firmware presentes nos demais equipamentos;

4.1.1.94 Possuir informações de garantia e apresentar, via relatório e/ou scorecard, listando o tipo de garantia e data limite, em caso de limite informar via email de forma automatizada para que seja possível ação da contratante;

4.1.1.95 Permitir a detecção de pré-falhas dos componentes de hardware.

4.1.1.96 Realizar a abertura automática de chamados sem intervenção humana, diretamente ao fabricante dos equipamentos em caso de falha de componentes de hardware;

4.1.1.97 Permitir ligar, desligar e reiniciar os servidores remotamente e independente de sistema operacional;

4.1.1.98 O software de gerenciamento deverá permitir a medição do consumo elétrico de grupos de servidores instalados em um rack, distribuídos em vários racks em um corredor e em todo o data center. Também deverá ser capaz de controlar o consumo elétrico dos servidores e implementar políticas de consumo, reduzindo o consumo individual ou de grupos de equipamentos caso ultrapassem os limites de consumo pré-estabelecidos;

4.1.1.99 Deve possuir recurso remoto que permita o completo desligamento e reinicialização (Hard-Reset) remoto do equipamento através da interface de gerência ou através de solução alternativa (Hardware/Software);

4.1.1.100 Permitir a emulação de mídias virtuais de inicialização (boot) através de CD/DVD remoto, compartilhamentos de rede NFS/CIFS e dispositivos de armazenamento USB remotos;

4.1.1.101 Permitir acesso do tipo Console Virtual, do mesmo fabricante dos servidores ofertados, que permita gerenciar, monitorar e configurar parâmetros físicos dos servidores de forma remota e centralizada;

4.1.1.102 O software de gerenciamento deve realizar descoberta automática dos servidores, permitindo inventariar os mesmos e seus componentes;

4.1.1.103 Suportar o monitoramento remoto (1:1 e 1:N) do consumo de energia elétrica e temperatura dos servidores, através de exibição gráfica, e permitir gerenciar parâmetros de consumo de CPU, memória, IO e Motherboard, com geração de alertas;

4.1.1.104 Possuir configuração de alerta de consumo de energia para grupos de dispositivos;

4.1.1.105 Possuir controles de energia baseados no tempo (diariamente, semanalmente e ou faixa de datas);

4.1.1.106 Permitir configurar dispositivos individuais, grupos físicos e grupos lógicos;

4.1.1.107 Permitir comparação de dispositivos relacionado ao seu consumo, criando reports com equipamentos ociosos em consumo e os de maior consumo;

4.1.1.108 Deve possuir funcionalidade que permita que os discos locais do servidor sejam apagados de forma definitiva através de tecnologia de gravação de dados ou similar. Esta funcionalidade deve possibilitar que sejam definitivamente apagados quaisquer discos dentro do servidor, suportando, no mínimo discos físicos (HDDs), discos criptografados (SEDs) e dispositivos de memória não volátil (SSDs e NVMe).

4.1.1.109 Deve possibilitar o download automático de atualizações de firmwares, BIOS e drivers diretamente do site do fabricante ou repositório local.

4.1.1.110 O servidor deve prover mecanismos preliminares às atualizações de firmware da controladora de gerenciamento remoto (BMC, por exemplo) que assegurem que as imagens de atualização possuam assinatura digital cuja autenticidade possa ser verificada usando chave criptográfica imutável armazenada em hardware;

4.1.1.111 Deverá fazer o gerenciamento e inventário para até 1500 dispositivos;

Acessórios

4.1.1.112 Devem ser fornecidos junto com o equipamento, todos os acessórios e cabos necessários para o pleno funcionamento do mesmo.

Documentação Técnica

4.1.1.113 Deverão ser fornecidos manuais técnicos do usuário e de referência contendo todas as informações sobre os produtos com as instruções para instalação, configuração, operação e administração

Certificados

4.1.1.114 Deverá ser entregue no dia do pregão a certificação comprovando que o equipamento está em conformidade com a norma IEC 60950, Energy Star, Rohs e Inmetro;

4.1.1.115 As atualizações de BIOS/UEFI devem possuir autenticação criptográfica (assinatura) segundo as especificações NIST SP800147B, NIST SP800-193 e NIST SP800-155;

4.1.1.116 O fabricante do servidor deve ser membro do DMTF (Desktop Management Task Force) na categoria "BOARD", comprovado através de acesso a página <http://www.dmtf.org/about/list/>;

4.1.1.117 O fabricante do servidor deve ser membro do TCG (Trusted Computing Group) na categoria "PROMOTER", comprovado através do link <https://trustedcomputinggroup.org/membership/member-companies/>;

4.1.1.118 O fabricante do servidor deverá constar na lista pública do TSANet no nível "Elite", de forma a garantir a cooperação entre suportes de fabricantes diferentes acelerando a resolução de problemas, comprovado através do link <https://www.tsanet.org/members/>;

Outros

4.1.1.119 Quando o Licitante não for o próprio fabricante dos equipamentos ofertados, deverá apresentar declaração do Fabricante específica para o edital, autorizando a empresa licitante a comercializar os itens envolvidos;

4.1.1.120 Os componentes do equipamento deverão ser homologados pelo fabricante. Não será aceita a adição ou subtração de qualquer componente não original de fábrica para adequação do equipamento;

4.1.1.121 Apresentação de no mínimo um atestado emitido por pessoa jurídica de direito público ou privado, comprovando que a proponente fornece/forneceu bens compatíveis com os objetos da licitação, emitidos em papel timbrado, com assinatura, identificação e telefone do emitente.

4.1.2 SERVIDOR RACK TIPO 1U – 2 PROCS. / 1.536 GB RAM

Gabinete

- 4.1.2.1 Gabinete para instalação em rack de 19" através de sistema de trilhos deslizantes; 4.1.2.2 Altura máxima de 1U;
- 4.1.2.3 Deve possuir botão liga/desliga na parte frontal do equipamento;
- 4.1.2.4 Deve possuir suporte de no mínimo 10 (dez) baias para instalação de drives do tipo SAS/SATA;
- 4.1.2.5 Deverá ser entregue junto com o servidor, um kit de fixação para rack, do tipo retrátil, permitindo o deslizamento do servidor a fim de facilitar sua manutenção;
- 4.1.2.6 Possuir projeto tool-less, ou seja, não necessita de ferramentas para instalação/desinstalação de placas de expansão;
- 4.1.2.7 Deve possuir sistema de ventilação redundante e hot-pluggable para que a CPU suporte a configuração máxima e dentro dos limites de temperatura adequados para o perfeito funcionamento do equipamento, e que permita a substituição do mesmo com o equipamento em funcionamento.
- 4.1.2.8 Deverá ser fornecido com Módulo TPM 2.0 FIPS ou superior;

Fonte de Alimentação

- 4.1.2.9 Mínimo de 2 (duas) fontes, suportando o funcionamento do equipamento na configuração ofertada mesmo em caso de falha de uma das fontes;
- 4.1.2.10 Deverá ser fornecido com sua quantidade máxima de fontes;
- 4.1.2.11 As fontes deverão ser totalmente redundantes e hot-pluggable permitindo a substituição de qualquer uma das fontes em caso de falha sem parada ou comprometimento do funcionamento do equipamento;
- 4.1.2.12 As fontes de alimentação devem possuir certificação 80Plus, no mínimo na categoria TITANIUM.
- 4.1.2.13 A fonte deve ter potência mínima de 1.500 watts;
- 4.1.2.14 As fontes devem possuir tensão de entrada de 100VAC a 240VAC a 60Hz, com ajuste automático de tensão;
- 4.1.2.15 Deverá acompanhar cabo de alimentação C13/C14 para cada fonte de alimentação fornecida.

Processador

- 4.1.2.16 O servidor deverá suportar processadores do tipo single-threaded, com até 144 núcleos, ou multi-threaded, com até 86 núcleos, por processador;
- 4.1.2.17 Equipado com 2 (dois) processadores de 32 núcleos do tipo multi-threaded, com arquitetura x86;
- 4.1.2.18 Deverá implementar mecanismos de gerenciamento do consumo de energia compatível com o padrão ACPI;
- 4.1.2.19 Deve suportar conjunto de instruções estendido compatível com padrão AVX-512;
- 4.1.2.20 Consumir no máximo 250W;
- 4.1.2.21 Frequência de clock interno de no mínimo 2.5 GHz;
- 4.1.2.22 Controladora de memória com suporte a DDR5 de no mínimo 6400 MT/s para 1 DIMM por canal, ou 5200 MT/s para 2 DIMMs por canal;
- 4.1.2.23 Link de comunicação do processador com o restante do sistema de 24 GT/s;
- 4.1.2.24 Memória cache de 288 MB – L3.

Desempenho

4.1.2.25 O processador ofertado deverá ter índice SPEC CPU2017 Integer Rate Results (Baseline) auditado de no mínimo 721 para 2 processadores. Os índices SPEC CPU2017 Integer Rate Results (Baseline) utilizados como referência serão validados junto ao site da Internet <https://www.spec.org/> Standard Performance Evaluation Corporation. Não serão aceitas estimativas para modelos / famílias de processadores não auditados pelo SPEC, resultados obtidos com a utilização de servidores em cluster, bem como estimativas em resultados inferiores ao mínimo especificado;

4.1.2.26 Não será aceito modelo de servidor não auditada pelo Standard Performance Evaluation Corporation ou auditada antes de 2017.

Memória RAM

4.1.2.27 Módulos de memória RAM tipo DDR5 RDIMM (Registered DIMM) com tecnologia de correção ECC (Error Correcting Code) e velocidade de, no mínimo, 6400 MT/s;

4.1.2.28 Deve possuir no mínimo 32 slots de memória DIMM;

4.1.2.29 Deve possuir 1.536 GB de memória instalada;

Circuitos Integrados (Chipset) e Placa Mãe

4.1.2.30 O chipset deve ser da mesma marca do fabricante do processador;

4.1.2.31 Possuir, no mínimo, 2 slots OCP 3.0 e 2 slots PCI Express 5.0;

4.1.2.32 Placa mãe da mesma marca do fabricante do equipamento, desenvolvida especificamente para o modelo ofertado. Não serão aceitas placas de livre comercialização no mercado;

Controladora de Vídeo

4.1.2.33 Deve ser do tipo on board (integrado na placa mãe) ou placa de vídeo PCIe;

4.1.2.34 Resolução gráfica de 1024 x 768 pixels ou superior.

BIOS ou UEFI

4.1.2.35 Possuir UEFI (Unified Extensible Firmware Interface) ou BIOS (Basic Input Output System) totalmente compatível e desenvolvida para o servidor fornecido;

4.1.2.36 A BIOS/UEFI deve ser atualizável por software;

4.1.2.37 O servidor deve implementar mecanismos de garantia de integridade e autenticidade do código da BIOS /UEFI, antes de sua execução, por meio de assinatura digital que poderá ser validada usando chave criptográfica imutável armazenada em hardware;

4.1.2.38 O servidor deve prover mecanismos preliminares às atualizações de firmware da BIOS/UEFI e de firmware da controladora de gerenciamento remoto que assegurem que os pacotes de atualização de firmware possuam assinatura digital cuja autenticidade poderá ser verificada usando chave criptográfica imutável armazenada em hardware;

4.1.2.39 O servidor deverá ser capaz de restaurar, automaticamente, o estado da BIOS/UEFI para uma versão íntegra anterior, armazenada em área de memória oculta e protegida contra gravação, em casos de corrupção identificados durante a inicialização da BIOS/UEFI;

4.1.2.40 Deverá suportar escaneamento de BIOS Firmware em tempo real para detecção de código malicioso;

4.1.2.41 Deve possuir funcionalidade que permita que os discos locais do servidor sejam apagados de forma definitiva através de tecnologia de regravação de dados ou similar. Esta funcionalidade deve possibilitar que sejam definitivamente apagados quaisquer discos dentro do servidor, suportando discos físicos (HDDs), discos criptografados (SEDs) e dispositivos de flash SSDs e NVMe;

4.1.2.42 A console de gerenciamento local deverá implementar modo "System Lockdown", o qual deve impedir que usuários com menos privilégios façam alterações nas configurações do servidor;

4.1.2.43 A console de gerenciamento local deve possuir uma área de armazenamento oculta para a rápida recuperação da BIOS e do Sistema Operacional quando comprometidos;

4.1.2.44 Deverá permitir que as portas USB possam ser desativadas de maneira programada;

Portas de Comunicação

4.1.2.45 Todos os conectores das portas de entrada/saída devem ser identificados pelos nomes ou símbolos;

4.1.2.46 Possuir 3 (três) interfaces USB sendo, no mínimo duas destas interfaces no padrão 3.0;

4.1.2.47 Possuir, no mínimo, 1 (uma) porta de vídeo padrão VGA (DB-15);

Interface de Rede

4.1.2.48 Possuir 06 (seis) interfaces de rede de 10/25Gb DA/SFP28 em 2 ou 3 adaptadores distintos suportando taxas de transferência de 10Gbps e 25Gbps;

4.1.2.49 Suporte ao protocolo de virtualização VMQ

4.1.2.50 Suporte ao protocolo VXLAN

4.1.2.51 Possuir tecnologia de processamento TCP/IP offload LSO, RSS e TSS

Controladora RAID

4.1.2.52 Controladora RAID, compatível com discos padrão SAS 22.5 Gbps, SAS 12 Gbps, SATA/SAS 6 Gbps e drives NVMe;

4.1.2.53 Suportar e implementar RAID 0, 1 e 10;

4.1.2.54 Suportar expansão de capacidade de formatação on-line;

4.1.2.55 Permita detecção e recuperação automática de falhas e reconstrução, também de forma automática, dos volumes de RAID sem necessidade de reiniciar o equipamento;

4.1.2.56 Deverá permitir a operação em modo RAID e pass-through em discos distintos. Ou fornecer controladora RAID e controladora pass-through.

4.1.2.57 Suporte a recursos de hot swap para as unidades de disco;

4.1.2.58 Suportar implementação de disco Global Hot-spare;

4.1.2.59 Suportar Self-Monitoring Analysis and Reporting Technology (SMART).

Dispositivos de armazenamento padrão SSD com as seguintes características

4.1.2.60 Para a instalação do Sistema Operacional devem ser fornecidos 2 (dois) drives do tipo SSD (Solid State Drive) no

formato de 2,5 polegadas de, no mínimo, 480GB cada um, ligados em RAID1 através da controladora de discos especificada acima;

4.1.2.61 Devem ser do tipo hot plug e hot swap, que permita sua substituição sem a necessidade de desligar o equipamento, garantindo a continuidade das operações sem impacto para as aplicações;

4.1.2.62 Devem possuir DWPD igual a 1 medido pelo período de 5 anos;

4.1.2.63 Devem possuir taxa de transferência de, no mínimo, 6Gb/s;

4.1.2.64 Devem ser do tipo SATA Read Intensive;

4.1.2.65 Não serão aceitos discos em gabinetes externos ao servidor;

4.1.2.66 Não serão aceitas soluções baseadas em cartão SD ou similar;]

Sistema Operacional

4.1.2.67 O servidor deverá ser ofertado com o sistema operacional OEM Windows Server 2025 Datacenter licenciado para todos os núcleos de todos os processadores;

4.1.2.68 O fabricante deve disponibilizar no seu respectivo web site, download gratuito de todos os Drivers dos dispositivos, BIOS e

Firmwares para o equipamento ofertado;

4.1.2.69 Apresentar declaração do fabricante informando que todos os componentes do objeto são novos (sem uso, reforma ou recondicionamento) e que não estão fora de linha de fabricação;

4.1.2.70 O modelo do equipamento ofertado deverá suportar o sistema operacional Windows Server 2022 ou superior. Esse item deverá ser comprovado através do HCL (Hardware Compatibility List) da Microsoft no link: <https://www.windowsservercatalog.com>;

4.1.2.71 O modelo do equipamento ofertado deverá suportar o sistema operacional Red Hat Enterprise Linux 9.4 ou posterior. Esse item deverá ser comprovado através do HCL (Hardware Compatibility List) da Red Hat no link: <https://hardware.redhat.com/hwcert/index.cgi>;

4.1.2.72 O modelo do equipamento ofertado deverá suportar o sistema de virtualização VMware ESXi 8.0 ou posterior. Esse item deverá ser comprovado através do Compatibility Guide da Broadcom no link: <https://compatibilityguide.broadcom.com/searchprogram=server&persona=live&column=partnerName&order=asc>;

Gerenciamento e Inventário

4.1.2.73 O equipamento deve possuir solução de gerenciamento do próprio fabricante através de recursos de hardware e software com capacidade de prover as seguintes funcionalidades:

4.1.2.74 O software de gerenciamento deverá estar licenciado para todas as funcionalidades requisitadas nestas especificações e unificar as operações de administração, monitoramento e gestão de tarefas de gerenciamento de todos os servidores fornecidos em uma única console gráfica.

4.1.2.75 O equipamento deve possuir interface de rede dedicada para gerenciamento que suporte nativamente a atribuição de endereçamento IP dinâmico;

4.1.2.76 Permitir o monitoramento remoto, de todo o hardware das condições de funcionamento dos equipamentos e seus componentes, tais como: processadores, memória RAM, controladora RAID, discos, fontes de alimentação, NICs e ventiladores;

4.1.2.77 Permitir acessar a BIOS ou UEFI remotamente;

4.1.2.78 Suportar os protocolos de criptografia SSL para acesso Web e SSH para acesso CLI;

4.1.2.79 Emitir alertas de anormalidade de hardware através do software de gerência e suportar o encaminhamento via e-mail e trap

SNMP;

4.1.2.80 Suportar autenticação local e através de integração com MS Active Directory/LDAP;

4.1.2.81 Deverá suportar autenticação de 2 fatores.

4.1.2.82 Permitir o controle remoto da console do servidor do tipo virtual KVM out-of-band, ou seja, independente de sistema operacional ou software agente;

4.1.2.83 Permitir a captura de vídeo ou tela de situações de falhas críticas de sistemas operacionais e inicialização do sistema (boot), possibilitando uma depuração mais aprimorada;

4.1.2.84 As funcionalidades de gerenciamento e monitoramento de hardware devem ser providas por recursos do próprio equipamento e independente de agentes ou sistema operacional;

4.1.2.85 A console virtual deverá ser acessível via interface HTML5 ou, caso necessite de algum tipo de plugin licenciado, por exemplo JAVA, deverá ser fornecido o licenciamento por pelo menos 5 anos;

4.1.2.86 Suportar os protocolos de gerenciamento, IPMI e SNMP v1/v2c/v3, WMI, SSH, WS MAN e REDFISH;

4.1.2.87 Permitir customizar alertas e automatizar a execução de tarefas baseadas em script;

4.1.2.88 O software de gerenciamento deverá permitir instalação remota de sistemas operacionais como Windows, Linux e VMware vSphere.

4.1.2.89 Permitir integração com o VMware vCenter de modo que o gerenciamento e inventário também possa ser realizado através do vSphere Web Client com informações referentes aos hosts (nome do host, endereço IP do host, configuração de CPU, memória, NIC, firmware), além de listar as versões de software e hardware em uso pelo host, controladoras de rede, RAID.

4.1.2.90 A integração com o VMware vCenter deverá permitir a redução nos tempos de resposta a eventos de hardware através de ações automáticas pré-estabelecidas pelo administrador, tais como, evacuação de máquinas virtuais em execução em host que venha emitir alertas de pré-falha de qualquer componente vital como CPU, memória e disco, e manter a estabilidade e a confiabilidade do ambiente através do gerenciamento de firmwares empregados no ambiente, garantindo conformidade entre todos os hosts ESXi;

4.1.2.91 Permitir configurar os seguintes parâmetros de hardware: WWN, BIOS, RAID, NIC, MAC, Virtual MAC Address, iSCSI Name, VLAN e perfil de QOS, através de templates pré-definidos;

4.1.2.92 Permitir a instalação, update e configuração remota de sistemas operacionais, drivers e firmwares, através de solução de deployment compatível com a solução ofertada;

4.1.2.93 Permitir estabelecer perfis de configuração com o inventário das versões de firmwares disponíveis para execução programada de verificações de conformidade das versões de firmware presentes nos demais equipamentos;

4.1.2.94 Possuir informações de garantia e apresentar, via relatório e/ou scorecard, listando o tipo de garantia e data limite, em caso de limite informar via email de forma automatizada para que seja possível ação da contratante;

4.1.2.95 Permitir a detecção de pré-falhas dos componentes de hardware.

4.1.2.96 Realizar a abertura automática de chamados sem intervenção humana, diretamente ao fabricante dos equipamentos em caso de falha de componentes de hardware;

4.1.2.97 Permitir ligar, desligar e reiniciar os servidores remotamente e independente de sistema operacional;

4.1.2.98 O software de gerenciamento deverá permitir a medição do consumo elétrico de grupos de servidores instalados em um rack, distribuídos em vários racks em um corredor e em todo o data center. Também deverá ser capaz de controlar o consumo elétrico dos servidores e implementar políticas de consumo, reduzindo o consumo individual ou de grupos de equipamentos caso ultrapassem os limites de consumo pré-estabelecidos;

- 4.1.2.99 Deve possuir recurso remoto que permita o completo desligamento e reinicialização (Hard-Reset) remoto do equipamento através da interface de gerência ou através de solução alternativa (Hardware/Software);
- 4.1.2.100 Permitir a emulação de mídias virtuais de inicialização (boot) através de CD/DVD remoto, compartilhamentos de rede NFS/CIFS e dispositivos de armazenamento USB remotos;
- 4.1.2.101 Permitir acesso do tipo Console Virtual, do mesmo fabricante dos servidores ofertados, que permita gerenciar, monitorar e configurar parâmetros físicos dos servidores de forma remota e centralizada;
- 4.1.2.102 O software de gerenciamento deve realizar descoberta automática dos servidores, permitindo inventariar os mesmos e seus componentes;
- 4.1.2.103 Suportar o monitoramento remoto (1:1 e 1:N) do consumo de energia elétrica e temperatura dos servidores, através de exibição gráfica, e permitir gerenciar parâmetros de consumo de CPU, memória, IO e Motherboard, com geração de alertas;
- 4.1.2.104 Possuir configuração de alerta de consumo de energia para grupos de dispositivos;
- 4.1.2.105 Possuir controles de energia baseados no tempo (diariamente, semanalmente e ou faixa de datas);
- 4.1.2.106 Permitir configurar dispositivos individuais, grupos físicos e grupos lógicos;
- 4.1.2.107 Permitir comparação de dispositivos relacionado ao seu consumo, criando reports com equipamentos ociosos em consumo e os de maior consumo;
- 4.1.2.108 Deve possuir funcionalidade que permita que os discos locais do servidor sejam apagados de forma definitiva através de tecnologia de regravação de dados ou similar. Esta funcionalidade deve possibilitar que sejam definitivamente apagados quaisquer discos dentro do servidor, suportando, no mínimo discos físicos (HDDs), discos criptografados (SEDs) e dispositivos de memória não volátil (SSDs e NVMe).
- 4.1.2.109 Deve possibilitar o download automático de atualizações de firmwares, BIOS e drivers diretamente do site do fabricante ou repositório local.
- 4.1.2.110 O servidor deve prover mecanismos preliminares às atualizações de firmware da controladora de gerenciamento remoto (BMC, por exemplo) que assegurem que as imagens de atualização possuam assinatura digital cuja autenticidade possa ser verificada usando chave criptográfica imutável armazenada em hardware;
- 4.1.2.111 Deverá fazer o gerenciamento e inventário para até 1500 dispositivos;

Acessórios

- 4.1.2.112 Devem ser fornecidos junto com o equipamento, todos os acessórios e cabos necessários para o pleno funcionamento do mesmo.

Documentação Técnica

- 4.1.2.113 Deverão ser fornecidos manuais técnicos do usuário e de referência contendo todas as informações sobre os produtos com as instruções para instalação, configuração, operação e administração.

Certificados

- 4.1.2.114 Deverá ser entregue no dia do pregão a certificação comprovando que o equipamento está em conformidade com a norma IEC

60950, Energy Star, Rohs e Inmetro;

- 4.1.2.115 As atualizações de BIOS/UEFI devem possuir autenticação criptográfica (assinatura) segundo as especificações NIST SP800147B, NIST SP800-193 e NIST SP800-155;

4.1.2.116 O fabricante do servidor deve ser membro do DMTF (Desktop Management Task Force) na categoria "BOARD", comprovado através de acesso a página <http://www.dmtf.org/about/list/>;

4.1.2.117 O fabricante do servidor deve ser membro do TCG (Trusted Computing Group) na categoria "PROMOTER", comprovado através do link <https://trustedcomputinggroup.org/membership/member-companies/>;

4.1.2.118 O fabricante do servidor deverá constar na lista pública do TSANet no nível "Elite", de forma a garantir a cooperação entre suportes de fabricantes diferentes acelerando a resolução de problemas, comprovado através do link <https://www.tsanet.org/members/>;

Outros

4.1.2.119 Quando o Licitante não for o próprio fabricante dos equipamentos ofertados, deverá apresentar declaração do

Fabricante específica para o edital, autorizando a empresa licitante a comercializar e prestar os serviços de garantia exigidos;

4.1.2.120 Os componentes do equipamento deverão ser homologados pelo fabricante. Não será aceita a adição ou subtração de qualquer componente não original de fábrica para adequação do equipamento;

4.1.2.121 Apresentação de no mínimo um atestado emitido por pessoa jurídica de direito público ou privado, comprovando que a proponente fornece/forneceu bens compatíveis com os objetos da licitação, emitidos em papel timbrado, com assinatura, identificação e telefone do emitente.

4.1.3 SWITCH L3 COM 48 PORTAS FIXAS 1/10/25GBE E 6 PORTAS 100GBE

Características físicas

4.1.3.1 O equipamento deve possuir no mínimo 48 (quarenta e oito) portas 1/10/25 Gigabit Ethernet SFP28;

4.1.3.2 As portas devem ser do tipo auto-sense, identificando a velocidade de acordo com o transceiver inserido, sem a necessidade de configurações manuais;

4.1.3.4 Deve ocupar no máximo 1 (uma) unidade de rack (1 RU);

4.1.3.5 Deve ser instalável em rack padrão de 19", sendo que deverão ser fornecidos os respectivos kits de fixação;

4.1.3.6 As portas SFP28 devem suportar transceivers dos padrões SFP28 25GBase-SR, 25GBase-LR e 25GBase-ESR; SFP+10GBase-SR, 10GBase-LR e 10GBase-ER; SFP 1000Base-SX, 1000Base-LX, 1000Base-ZX e 1000Base-T e cabos Direct Attach Cable (DAC);

4.1.3.7 Devem ser fornecidos 32 (trinta e dois) cabos Direct Attach Cable (DAC) passivos de 25GbE do tipo SFP28 para SFP28 de 3 metros;

4.1.3.8 Devem ser fornecidos 17 (dezessete) cabos Direct Attach Cable (DAC) ativos de 25GbE do tipo SFP28 para SFP28 de 10 metros;

4.1.3.9 Possuir 06 (seis) portas de 100 Gigabit Ethernet QSFP28 com suporte a velocidades de 40 e 100 Gigabit Ethernet.

4.1.3.10 As portas QSFP28 devem suportar transceivers dos padrões QSFP+ 40GBase-SR4 e 40GBase-LR4; QSFP28 100GBase-SR4, 100GBase-LR4 e 100GBase-SR1.2 e cabos Direct Attach Cable (DAC);

4.1.3.11 Devem ser fornecidos 02 (dois) cabos Direct Attach Cable (DAC) passivos de 100GbE do tipo QSFP28 para QSFP28 de 1 metro;

- 4.1.3.12 Devem ser fornecidos 04 (quatro) cabos Direct Attach Cable (DAC) passivos de 100GbE do tipo QSFP28 para QSFP28 de 3 metros;
- 4.1.3.13 Devem ser fornecidos 02 (dois) transceivers de 100 GbE QSFP28 padrão 100GBase-SR1.2;
- 4.1.3.14 Deve possuir matriz de comutação com capacidade de pelo menos 4 Tbps full duplex;
- 4.1.3.15 Deve possuir capacidade mínima de 3 Bpps full duplex de Throughput;
- 4.1.3.16 Deve possuir buffer mínimo de 32 MB;
- 4.1.3.17 Deve possuir latência menor ou igual a 900 nanosegundos;
- 4.1.3.18 Deve possuir capacidade para no mínimo 160.000 endereços MAC;
- 4.1.3.19 Deve implementar tabela ARP com até 128.000 entradas;
- 4.1.3.20 Deve suportar a Jumbo frames de no mínimo 9000 bytes;
- 4.1.3.21 Deve possuir no mínimo 1 (uma) porta de console com conector RJ-45;
- 4.1.3.22 Deve possuir no mínimo 1 (uma) porta Ethernet RJ-45 para administração fora de banda (out-of-band management);
- 4.1.3.23 Deve ser fornecido com configuração de CPU e memória (RAM e Flash) suficiente para implementação de todas as funcionalidades descritas nesta especificação.
- 4.1.3.24 Deve possuir fontes de alimentação redundantes internas ao equipamento com ajuste automático de tensão 110 ou 220 volts;
- 4.1.3.25 Cada fonte de alimentação deverá vir acompanhada de um cabo de alimentação C13/C14.
- 4.1.3.26 O equipamento deverá ter ventiladores redundantes com opções de fluxo de ar da frente para trás ou de trás para frente (front-to-back ou back-to-front). Os equipamentos devem vir equipados com ventiladores de fluxo de ar de trás para frente;
- 4.1.3.27 As fontes e ventiladores devem ser capazes de serem trocados com o equipamento em pleno funcionamento, sem nenhum impacto na performance (hot-swappable) e devem ser redundantes;
- 4.1.3.28 O equipamento deve ser específico para o ambiente de Datacenter com comutação de pacotes de alto desempenho;
- 4.1.3.29 Deve ser um equipamento homologado pela Agência Nacional de Telecomunicações (Anatel);

Funcionalidades gerais

- 4.1.3.30 Deve possuir LEDs, por porta, que indiquem a integridade e atividade do link;
- 4.1.3.31 Deve possuir LEDs do tipo blue beacon para identificação do switch e da porta a ser acessada, para facilitar a manutenção;
- 4.1.3.32 A solução deve permitir implementar e prover arquitetura de rede de data center utilizando a arquitetura “spine - leaf”, tendo o VxLAN como plano de dados (“data-plane”) e BGP EVPN para o plano de controle (“control-plane”).
- 4.1.3.33 Deve possuir porta de console para gerenciamento e configuração via linha de comando. O conector deve ser RJ-45 ou padrão
- RS-232 (os cabos e eventuais adaptadores necessários para acesso à porta de console devem ser fornecidos);
- 4.1.3.34 Deve ser gerenciável via SSHv2;

- 4.1.3.35 O switch deve ter no mínimo criptografia FIPS 140-2 comprovado pelo NIST;
- 4.1.3.36 O switch suportar o padrão X.509v3 para certificados digitais;
- 4.1.3.37 Deve permitir o espelhamento de uma porta e de um grupo de portas para uma porta especificada;
- 4.1.3.38 Deve permitir o espelhamento de uma porta ou de um grupo de portas para uma porta especificada em um switch remoto no mesmo domínio L2 ou em outro domínio L2 através de tunelamento;
- 4.1.3.39 Deve implementar Netflow, sFlow ou similar;
- 4.1.3.40 Deve suportar SDN ao menos com Openflow 1.3;
- 4.1.3.41 Deve ser gerenciável via SNMPv3;
- 4.1.3.42 Deve implementar o protocolo Syslog para funções de “logging” de eventos;
- 4.1.3.43 Deve implementar o protocolo NTPv4 ou SNTP;
- 4.1.3.44 Deve suportar autenticação RADIUS sobre TLS;
- 4.1.3.45 Deve suportar autenticação TACACS+;
- 4.1.3.46 Deve implementar controle de acesso por porta (IEEE 802.1x);
- 4.1.3.47 Deve implementar listas de controle de acesso (ACLs) baseadas em endereço IPv4 ou IPv6 de origem e destino, portas TCP e UDP de origem e destino e endereços MAC de origem e destino;
- 4.1.3.48 Deve possuir controle de broadcast, multicast e unknown unicast por porta;
- 4.1.3.49 Deve implementar pelo menos uma fila de saída com prioridade estrita (SP Strict Priority) por porta e divisão ponderada (WRED, WRR ou similar) de banda entre as demais filas de saída;
- 4.1.3.50 Deve implementar classificação, marcação e priorização de tráfego baseada nos valores de classe de serviço do frame ethernet (IEEE 802.1p CoS);
- 4.1.3.51 Deve implementar classificação, marcação e priorização de tráfego baseada nos valores do campo “Differentiated Services Code Point” (DSCP) do cabeçalho IP, conforme definições do IETF;
- 4.1.3.52 Deve implementar classificação de tráfego baseada em endereço IP de origem/destino, portas TCP e UDP de origem e destino, endereços MAC de origem e destino;
- 4.1.3.53 Deve formar um virtual switch, de forma que os dois possam ser vistos como uma entidade única, logicamente. Esta funcionalidade pode ser provida através de:
 - 4.1.3.53.1 Suporte à funcionalidade de agregação de portas multi-chassi, através da criação de redundância ativa /ativa livre de loop e sem utilização de protocolo Spanning Tree, conforme as tecnologias MLAG, MC-LAG, M-LAG, Virtual Link Trunking, Multi-Chassis EtherChannel ou equivalentes
- 4.1.3.54 Deverão ser fornecidos todos os componentes necessários para garantia da alta disponibilidade, incluindo todos os módulos e /ou cabos/transceivers para interconexão dos equipamentos, bem como as licenças necessárias, caso aplicável;
- 4.1.3.55 Os equipamentos quando virtualizados deverão possuir processamento local de modo a possuir rápido tempo de convergência em caso de falha de um dos equipamentos do sistema virtualizado;

Funcionalidades de camada 2

4.1.3.56 Deve implementar até 4.000 VLANs IDs conforme definições do padrão IEEE 802.1Q;

4.1.3.57 Deve implementar “VLAN Trunking” conforme padrão IEEE 802.1Q nas portas Ethernet. Deve ser possível estabelecer quais VLANs serão permitidas em cada um dos troncos 802.1Q configurados.

4.1.3.58 Deve implementar a funcionalidade de “Link Aggregation(LAGs)” conforme padrão IEEE 802.3ad;

4.1.3.59 Deve suportar no mínimo 100 grupos por switch com até 16 portas por LAG (IEEE 802.3ad);

4.1.3.60 Deve implementar o padrão IEEE 802.1d, IEEE 802.1s e IEEE 802.1w;

4.1.3.61 Deve implementar mecanismo de proteção da “root bridge” do algoritmo Spanning-Tree;

4.1.3.62 Deve permitir a suspensão de recebimento de BPDUs (Bridge Protocol Data Units) caso a porta esteja colocada no modo “fast forwarding” (conforme previsto no padrão IEEE 802.1w). Sendo recebido um BPDU neste tipo de porta deve ser possível desabilitá-la automaticamente;

4.1.3.63 Deve implementar o protocolo IEEE 802.1AB Link Layer Discovery Protocol (LLDP) e sua extensão LLDP-MED, permitindo a descoberta dos elementos de rede vizinhos;

4.1.3.64 O equipamento deve suportar funcionalidade de virtualização em camada 2 de modo a suportar diversidade de caminhos em camada 2 e agregação de links entre 2 switches distintos (Layer 2 Multipathing);

4.1.3.65 Suporte a DCB (Data Center Bridging), com suporte aos protocolos Priority-based flow control (PFC – IEEE 802.1Qbb), Enhanced Transmissions Selections (ETS – IEEE 802.1Qaz) e DCBx;

Funcionalidades de roteamento

4.1.3.66 Deve possuir roteamento nível 3 entre VLANs;

4.1.3.67 Deve implementar protocolos de roteamento dinâmico OSPFv3;

4.1.3.68 Deve implementar protocolos de roteamento dinâmico BGPv4 e BGPv6;

4.1.3.69 Deve ter suporte a 120.000 (cento e vinte mil) rotas IPv4;

4.1.3.70 Deve ter suporte a 60.000 (sessenta mil) rotas IPv6;

4.1.3.71 Deve trabalhar simultaneamente com protocolos IPv4 e IPv6;

4.1.3.72 Deve implementar VRF ou VRF-Light com suporte a no mínimo 500 instâncias;

4.1.3.73 Deve implementar Policy Based Routing;

4.1.3.74 Deve implementar o protocolo VRRP (Virtual Router Redundancy Protocol) v3;

4.1.4 INFRAESTRUTURA DE ARMAZENAMENTO DE DADOS

Definições

4.1.4.1 Soma da capacidade individual de todos os dispositivos de memória flash e/ou dispositivos 4.1.4 Capacidade bruta: de estado sólido e memória fornecidos antes de formatados. Considera 1GB (Gigabyte) igual a 1000MB (Megabytes), ou seja, adota notação decimal.

4.1.4.2 Capacidade útil: soma dos dispositivos de memória flash e/ou dispositivos de estado sólido fornecidos após formatação. Desconsidera reservas de hot-spare, nível de proteção com paridade, área destinada ao sistema operacional e áreas pré alocadas para suas funcionalidades como snapshots, metadados, replicação, formatação e

demais overheads relacionados ao consumo de capacidade necessário para o completo funcionamento da solução. É a capacidade disponível, dedicada e exclusiva para o armazenamento de dados de usuários e aplicações. Considera 1GB (Gigabyte) igual a 1024MB (Megabytes), ou seja, adota notação binária.

4.1.4.3 Capacidade útil efetiva: considera os ganhos obtidos a partir de tecnologias de redução de dados decorrentes exclusivamente e simultaneamente de mecanismos de deduplicação e compressão, ou seja, não considera ganhos com provisionamento virtual, snapshots, clones ou outros. Considera 1GB (Gigabyte) igual a 1024MB (Megabytes), ou seja, adota notação binária.

4.1.4.4 Modo de operação in-line: mecanismo de redução de dados de deduplicação e compressão antes da gravação e escrita nos dispositivos persistentes. Não se enquadra nesse modo qualquer tipo de tecnologia que realize a compressão e/ou deduplicação pósprocessada.

4.1.4.5 Appliance: par de controladoras operando de forma ativo-ativo no front-end e no back-end. Em caso de falha a controladora remanescente gerencia as LUNs da controladora em falha através de redirecionamento automático.

4.1.4.6 Cluster de armazenamento de dados: subsistema de pares de controladoras com gerenciamento centralizado, conexão intracluster, expansível de 1 (um) a 4 (quatro) pares e com funcionalidade de balanceamento automático de carga no cluster mediante sobrecarga em determina controladora. Referenciado neste documento também como “cluster”.

4.1.4.7 NAS Gateway: qualquer equipamento não nativo da controladora, ou seja, solução independente que opere de modo similar a um servidor de arquivos (file server) acessando volumes lógicos disponibilizados pelo subsistema de armazenamento ou qualquer componente adicional a controladora do equipamento como placas, servidores acessórios ou módulos adicionais para a implementação do NAS sendo respeitados os mesmos níveis de garantia, suporte e funcionalidades exigidos para o equipamento principal.

Características Gerais

4.1.4.8 Subsistema de armazenamento de dados para instalação em rack de 19” (dezenove polegadas) onde deverão ser fornecidos os respectivos kits de fixação;

4.1.4.9 Deverá ser fornecido um subsistema de armazenamento de dados baseado em appliance dedicado para a finalidade do tipo bloco, para uso em SAN (Storage Area Network) e NAS (Network Attached Storage) de forma nativa /integrada sem a utilização de gateways NAS.

4.1.4.10 O appliance deverá ter funcionamento exclusivo all-flash com tecnologia NVMe, para armazenamento baseado em blocos e arquivos, e permitir acesso multiprotocolo com suporte simultâneo aos protocolos de CIFS, FTP, SFTP, NFS, VVOLs, iSCSI e Fibre Channel (Fibre Channel não faz parte do fornecimento). O suporte deverá estar licenciado no subsistema, disponíveis para a utilização, suportando a escalabilidade máxima do equipamento ofertado;

4.1.4.11 O appliance deverá possuir pelo menos 2 (duas) controladoras, redundantes entre si, permitindo acesso aos dados armazenados no equipamento de modo ativo-ativo (assimétrico ou simétrico) e concorrente pelos hosts clientes através das portas de front-end (acesso) das controladoras.

4.1.4.12 Todas as unidades de armazenamento flash deverão possuir duas conexões ao barramento. 4.1.3.14 Não serão aceitos SSD's do tipo SAS ou SATA sob quaisquer condições;

4.1.4.13 Deverá permitir de forma não disruptiva e sem reconfiguração de serviços de dados:

4.1.3.13.1 A inclusão ou remoção em cluster pré-existente de appliance, permitindo ampliação do subsistema de forma escalável horizontalmente (scale-out) desde que preservados os requisitos de performance solicitados;

4.1.4.14 Deve contar com fontes de alimentação redundantes e incluir cabos de alimentação C13/C14.

Dimensionamento Capacidade

4.1.4.15 Deve ser fornecida a capacidade útil conforme definido nos termos deste item.

4.1.4.16 Caso a solução ofertada necessite de área adicional para implementação de qualquer funcionalidade, esta área deverá ser fornecida adicionalmente a capacidade útil solicitada;

4.1.4.17 Não serão admitidos discos SSD's NVMe do tipo QLC, cMLC ou similar;

4.1.4.18 Deverá possibilitar a escalabilidade de unitária de discos de armazenamento de forma online sem a necessidade de criação de um novo grupo de armazenamento;

4.1.4.19 A capacidade útil de armazenamento fornecida deve dispor de proteção, realizada por paridade simples (RAID 5 ou similar), de forma que a proteção seja distribuída em grupos máximos de 9 discos (8+1) em discos SSD NVMe de tamanho máximo de 3.84TB;

4.1.4.20 Caso a solução ofertada não suporte RAID 5, serão aceitas configurações baseadas em RAID 6 ou dupla paridade em grupos máximos de 8 discos (6+2).

4.1.4.21 A solução deverá possibilitar a implementação da funcionalidade de hot-spare ou tecnologias de outra nomenclatura com funcionalidade equivalente, de forma que a área reservada para reserva é distribuída entre todos os drives integrantes do RAID e múltiplos discos participam da reconstrução.

4.1.4.22 A área de hot-spare da configuração inicial deve seguir as melhores práticas do fabricante e não pode ser inferior a proporção mínima de 1 (um) disco spare a cada conjunto de 25 (vinte e cinco) discos e deve ser global.

4.1.4.23 O subsistema ofertado deverá ser fornecido com o mínimo de 18 discos SSD NVMe de 3.84TB, incluindo a área de hotspare equivalente a um disco.

4.1.4.24 O Appliance deve ser escalável até no mínimo 95 discos SSD NVMe com adição de discos e expansões de armazenamento (gavetas).

Volumetria requerida

4.1.4.25 Deverá ser fornecida uma capacidade útil mínima de 49 TiBu (Quarenta e Nove Tebibytes úteis); 4.1.4.25.1 A capacidade útil do subsistema ofertado deverá ser escalável através de ampliação realizada pela inclusão de novos appliances e/ou expansões de armazenamento (gavetas) com os mesmos tipos de discos SSD NVM e do appliance principal;

4.1.4.26 Deverá ser possível obter, com tecnologias de compressão e deduplicação de dados realizados no modo de operação in-line, uma capacidade útil efetiva mínima de 81 TiBe (Oitenta e Um Tebibytes efetivos), permitindo, ganhos efetivos a partir de 1,65:1 sobre a capacidade útil requerida;

4.1.4.27 A FABRICANTE deve GARANTIR a obtenção da capacidade de armazenamento efetiva mínima requerida considerados e os seguintes pontos:

4.1.4.28 Uso exclusivo e simultâneo das tecnologias de compressão inline e deduplicação inline;

4.1.4.29 A aferição da volumetria utilizável será feita pela CONTRATANTE através da análise dos relatórios disponíveis para este fim na ferramenta de gerenciamento da solução de armazenamento;

4.1.4.30 A aferição será feita com a ocupação mínima de 50% da capacidade bruta visando adequada formação do dicionário de deduplicação e consequente eficiência da tecnologia.

4.1.4.31 Para a aferição, todos os dados, incluindo dados de sistemas operacionais, máquinas virtuais e banco de dados, devem estar em seu formato nativo (não criptografados e compactados no nível do host).

4.1.4.32 Arquivos de Áudio, Imagem, PDF e Vídeo não serão incluídos em nenhum cálculo que determine o cumprimento da Garantia. Ou seja, a garantia de taxa de redução de dados requerida não inclui o consumo de armazenamento por arquivos de áudio, documentos com otimização de estrutura (exemplo: PDF), imagens (incluindo dentro do Banco de Dados), XML, vídeos ou armazenamento de backup ou dados com compactação prévia à gravação;

4.1.4.33 Durante a vigência do contrato de garantia do equipamento, a CONTRATANTE irá aferir periodicamente a taxa de redução de dados obtida. A não conformidade desta com a taxa de redução garantida, obriga a CONTRATADA, em até 90 (noventa) dias corridos contados da data de notificação do não atendimento, remediar a ocorrência, incluindo eventual fornecimento de capacidade útil de armazenamento adicional, possibilitando atingir-se a capacidade mínima de armazenamento efetivo exigida nesta especificação para o perfil de armazenamento informado, mantendo os requisitos de desempenho solicitados, sem ônus à CONTRATANTE. A eventual ampliação está condicionada ao consumo do armazenamento por dados com o perfil para o qual a garantia de redução de dados é requerida (ver 5 primeiros pontos deste mesmo tópico).

Desempenho

4.1.4.34 Cada appliance deve possuir no mínimo:

4.1.4.34.1 Um processador por controladora, cada um contendo no mínimo 12 (doze) cores de processamento, de 2.2 GHz ou superior, totalizando no mínimo dois processadores no appliance;

4.1.4.34.2 Memória RAM de no mínimo 192GB (cento e noventa e dois gigabytes), não permitido a utilização de SSD /FLASH como mecanismo de expansão;

4.1.4.35 O dimensionamento deve considerar a seguinte carga de trabalho em bloco (iSCSI):

4.1.4.35.1 Volumetria: 81 TiBe (Oitenta e Um Tebibytes efetivos);

4.1.4.35.2 São 60.000 IOPS, com deduplicação e compressão ativadas (ambas inline) com escalabilidade até 85.000 IOPS 4.1.4.35.3 Perfil de IO: 70% de leitura e 30% de escrita, 100% randômico, blocos de 8KB para leitura, 8KB para escrita e Cache Hit = 0%.

4.1.4.35.4 Latência inferior a 1ms.

4.1.4.36 Para fins de comprovação do desempenho requerido deverá ser apresentado, juntamente com a documentação de comprovação de especificação e funcionalidades do equipamento, relatório complementar gerado pela ferramenta de dimensionamento oficial do fabricante, comprovando que o equipamento atende a carga de trabalho especificada.

Replicação de dados

4.1.4.37 O sistema deve permitir a replicação síncrona e assíncrona de dados entre o subsistema e outro da mesma família/tecnologia. As licenças necessárias devem ser incluídas no fornecimento.

4.1.4.38 Para os volumes de dados VMWARE, o sistema deve suportar a criação de alta disponibilidade (HA) entre o subsistema e outro da mesma família/tecnologia, realizando a cópia síncrona bidirecional dos dados dos volumes, mantendo uma cópia ativa em cada subsistema, de forma que na eventual falha completa ou indisponibilidade de um dos subsistemas as operações de leitura e gravação destinadas aos volumes configurados em HA não sofram interrupções ou falhas no acesso. As licenças necessárias devem ser incluídas no fornecimento.

Conectividade de front-end

4.1.4.39 O subsistema deverá possuir no mínimo 8 (oito) interfaces Ethernet 10/25Gb SFP28, distribuídas de forma balanceada pelas controladoras (4 interfaces por controladora);

4.1.4.40 São 02 (duas) interfaces ativas de 1 (um) Gigabit Ethernet exclusiva para conexões externas e gerência.

Recursos de software

4.1.4.41 Deverá suportar a funcionalidade de data-reduction (deduplicação e compressão) de volumes. Tal recurso deverá ser nativo do subsistema de armazenamento e de forma "in-line" (em linha), não sendo aceitas soluções externas ou de outros fabricantes para realizar tal operação. Caso o ganho de capacidade efetiva (pós otimização) obtida dependa de licenciamento, o subsistema deverá ser licenciado para a capacidade máxima de área efetiva suportado pelo equipamento.

4.1.4.42 Deverá suportar os padrões de interoperabilidade: REST; SNMP v3.

4.1.4.43 A solução de armazenamento deve possuir software de gerenciamento centralizado para todo cluster com funções como:

4.1.3.43.1 Criação/administração de volumes, snapshots, clones ou thin clones, QoS para blocos e vVol's e configuração de usuários.

4.1.3.43.2 Monitoração de eventos, geração de relatórios de desempenho, alertas de capacidade, status de funcionamento dos componentes físicos tais como fontes, discos, controladoras, ventiladores bem como a manutenção de dados históricos do ambiente proposto pelo período de 12 meses.

4.1.4.44 Disponibilização de console e/ou portal de gerenciamento contendo Dashboard com informações de configuração, performance, health-check e capacidade. O portal, através de inteligência analítica e análise preditiva, deve:

4.1.4.44.1 Prover informações de saúde do ambiente.

4.1.4.44.2 Identificar preventivamente possíveis anomalias no subsistema.

4.1.4.44.3 Enviar alertas/notificações e recomendar ações para rápido auxílio em resolução de falhas.

4.1.4.44.4 Indicar a taxa de redução de dados geral do ambiente.

4.1.4.44.5 Identificar área apta a ser reclamada para otimização do espaço do subsistema.

4.1.4.44.6 Granularidade de intervalo de coleta de performance configurável de pelo menos 60 segundos para investigação de falhas.

4.1.4.44.7 Reter os dados de performance e capacidade por pelo menos 12 meses.

4.1.4.45 O fluxo de informações do subsistema para o portal deve ser seguro por conexão protegida por VPN 4 ou SSL, realizado diretamente pelo subsistema ou com apoio de ferramenta de proxy instalada em máquina virtual da infraestrutura da CONTRATANTE, não permitindo acesso reverso e externo ao subsistema através de tal conexão sem solicitação de autorização do acesso. 4.1.4.45 Deverá possuir função de call-home por meio de e-mail, conexão segura SSL ou VPN (Virtual Private Network) diretamente com o fabricante da solução, para diagnóstico remoto em caso de erros/defeitos.

4.1.4.46 Deverá incluir plug in de interface CSI para integração com Kubernetes suportando ao menos provisionamento de

Persistent Volume e configuração de snapshots. O plug in deve estar disponível em: <https://kubernetes.csi.github.io/docs/drivers.html>

4.1.4.47 O plug-in de Kubernetes deve suportar no mínimo: Funcionalidades de criação e deleção de volumes persistentes com provisionamento dinâmico. Conexões iSCSI e Fibre Channel;

4.1.4.48 Deverá possuir mecanismos que permitam a utilização das técnicas de volumes para recuperação rápida de volumes por meio de point-in-time (snapshot). A solução deverá suportar a criação de no mínimo 256 (duzentos e cinquenta e seis) snapshots por LUN.

4.1.4.49 Deverá permitir a criação granular de cópias do tipo snapshot ROW (redirect-on-write) sem dependência da área de reserva de snapshot, sem necessidade de movimentação de blocos já armazenados/alterados no volume primário em qualquer fase da cópia e sem onerar desempenho do equipamento.

4.1.4.50 Deverá possibilitar a criação de até 50.000 (cinquenta mil) snapshots;

4.1.4.50.1 Esses snapshots deverão permitir imutabilidade e prevenção contra deleção até mesmo pelo administrador do subsistema de armazenamento.

4.1.4.51 Deverá suportar a configuração de até 1.500 (mil e quinhentos) volumes lógicos (LUNS) sem a utilização da funcionalidade “LUN Extensions” e 2.000 (dois mil) initiators.

4.1.4.52 A implementação de qualquer uma das funcionalidades requeridas deve ser feita de forma independente, não podendo gerar qualquer indisponibilidade no ambiente ou a parada da funcionalidade previamente instalada.

4.1.4.53 O fabricante deve estar enquadrado, no mínimo, na categoria “Voting Members” do SNIA (Storage Networking Industry Association), confirmada via consulta ao site: https://www.snia.org/member_com/member_directory.

4.1.4.54 A solução de armazenamento deverá suportar VMware Site Recovery Manager via plugin e a compatibilidade deverá constar na matriz de compatibilidade HCL disponível no site da VMware, através do seguinte caminho: <https://www.vmware.com/resources/compatibility/search.php?deviceCategory=sra> (Storage & Availability – Site Recovery Manager (SRM) for SRA).

4.1.4.55 Suportar Criptografia dos dados armazenados nos dispositivos flash, do tipo “Data at Rest” e utilizando algoritmo AES- 256.

4.1.4.55.1 A criptografia em armazenamento persistente deve estar em conformidade com FIPS (Federal Information Processing Standard) 140-2 level 2 e SHA2. Este requisito deverá ser nativo do subsistema e estar devidamente licenciado para tal.

4.1.4.56 Os equipamentos ofertados deverão ser compatíveis com o padrão RoHS (restriction of hazardous substances), que inibe o fornecimento de equipamentos cujos componentes possuam substâncias tóxicas.

4.1.4.57 O fabricante do storage deverá constar na lista pública do TSANet (<https://tsanet.org/members/>) em nível mínimo Premium Membership de forma a garantir a cooperação entre suportes de fabricantes diferentes acelerando a resolução de problemas.

4.1.4.58 O FABRICANTE deverá possuir site de monitoração com acesso a partir da internet (web), aplicação de celular ou tablet, mediante autenticação por senha controlado pelo administrador do sistema de gerenciamento do equipamento. O sistema deverá apresentar dados de saúde dos equipamentos a partir de uma única tela e permitir a navegação em cada um deles apresentando dados e gráficos sobre a utilização de recursos, projeção de tendência de crescimento e eventuais alertas existentes para os equipamentos.

4.1.5 SERVIDOR RACK TIPO 2U – 2 PROCS / 128 GB RAM

Gabinete

4.1.5.1. Gabinete para instalação em rack de 19” através de sistema de trilhos deslizantes;

4.1.5.2. Altura máxima de 2U;

4.1.5.3. Deve possuir botão liga/desliga na parte frontal do equipamento;

4.1.5.4. Possuir display ou leds embutido no painel frontal do gabinete para exibição de alertas de funcionamento dos componentes internos, tais como falhas de memória RAM, fontes de alimentação e disco rígido e ventilador;

4.1.5.5. Deve possuir suporte de no mínimo 24 (vinte e quatro) baias para instalação de drives do tipo SAS/SATA;

4.1.5.6. Deverá ser entregue junto com o servidor, um kit de fixação para rack, do tipo retrátil, permitindo o deslizamento do servidor a fim de facilitar sua manutenção;

4.1.5.7. Possuir projeto tool-less, ou seja, não necessita de ferramentas para instalação/desinstalação de placas de expansão;

4.1.5.8. Deve possuir sistema de ventilação redundante e hot-pluggable para que a CPU suporte a configuração máxima e dentro dos limites de temperatura adequados para o perfeito funcionamento do equipamento, e que permita a substituição mesmo com o equipamento em funcionamento.

Fonte de Alimentação

- 4.1.5.9. Mínimo de 2 (duas) fontes, suportando o funcionamento do equipamento na configuração ofertada mesmo em caso de falha de uma das fontes;
- 4.1.5.10. Deverá ser fornecido com sua quantidade máxima de fontes;
- 4.1.5.11. As fontes deverão ser redundantes e hot-pluggable permitindo a substituição de qualquer uma das fontes em caso de falha sem parada ou comprometimento do funcionamento do equipamento;
- 4.1.5.12. A fonte deve ter potência mínima de 800 Watts;
- 4.1.5.13. As fontes devem possuir tensão de entrada de 100VAC a 240VAC a 60Hz, com ajuste automático de tensão;
- 4.1.5.14. Deverá acompanhar cabo de alimentação C13/C14 para cada fonte de alimentação fornecida.

Processador

- 4.1.5.15. O servidor deverá suportar processadores do tipo single-threaded, com até 144 núcleos, ou multi-threaded, com até 86 núcleos, por processador;
- 4.1.5.16. Equipado com 2 (dois) processadores de 8 (oito) núcleos do tipo multi-threaded, com arquitetura x86;
- 4.1.5.17. Deverá implementar mecanismos de gerenciamento do consumo de energia compatível com o padrão ACPI;
- 4.1.5.18. Deve suportar conjunto de instruções estendido compatível com padrão AVX-512;
- 4.1.5.19. Consumir no máximo 150W;
- 4.1.5.20. Frequência de clock interno de no mínimo 3.5 GHz;
- 4.1.5.21. Controladora de memória com suporte a DDR5 de no mínimo 6400 MT/s para 1 DIMM por canal, ou 5200 MT/s para 2 DIMMs por canal;
- 4.1.5.22. Link de comunicação do processador com o restante do sistema de 24 GT/s;
- 4.1.5.23. Memória cache de 48 MB – L3.

Desempenho

- 4.1.5.24. O processador ofertado deverá ter índice SPEC CPU2017 Integer Rate Results (Baseline) auditado de no mínimo 208 para 2 processadores. Os índices SPEC CPU2017 Integer Rate Results (Baseline) utilizados como referência serão validados junto ao site da Internet <https://www.spec.org/> Standard Performance Evaluation Corporation. Não serão aceitas estimativas para modelos / famílias de processadores não auditados pelo SPEC, resultados obtidos com a utilização de servidores em cluster, bem como estimativas em resultados inferiores ao mínimo especificado;
- 4.1.5.25. Não será aceito modelo de servidor não auditada pelo Standard Performance Evaluation Corporation ou auditada antes de 2017.

Memória RAM

- 4.1.5.26. Módulos de memória RAM tipo DDR5 RDIMM (Registered DIMM) com tecnologia de correção ECC (Error Correcting Code) e velocidade de, no mínimo, 6400 MT/s;
- 4.1.5.27. Deve possuir no mínimo 32 slots de memória DIMM;
- 4.1.5.28. Deve possuir 128 GB de memória instalada;

Circuitos integrados (chipset) e placa mãe

- 4.1.5.29. O chipset deve ser da mesma marca do fabricante do processador;

4.1.5.30. Possuir, no mínimo, 2 slots OCP 3.0 e 4 slots PCI Express 5.0;

4.1.5.31. Placa mãe da mesma marca do fabricante do equipamento, desenvolvida especificamente para o modelo ofertado. Não serão aceitas placas de livre comercialização no mercado;

BIOS ou UEFI

4.1.5.32. Possuir UEFI (Unified Extensible Firmware Interface) ou BIOS (Basic Input Output System) totalmente compatível e desenvolvida para o servidor fornecido;

4.1.5.33. A BIOS/UEFI deve ser atualizável por software;

4.1.5.34. O servidor deve implementar mecanismos de garantia de integridade e autenticidade do código da BIOS /UEFI, antes de sua execução, por meio de assinatura digital que poderá ser validada usando chave criptográfica imutável armazenada em hardware;

4.1.5.35. O servidor deve prover mecanismos preliminares às atualizações de firmware da BIOS/UEFI e de firmware da controladora de gerenciamento remoto que assegurem que os pacotes de atualização de firmware possuam assinatura digital cuja autenticidade poderá ser verificada usando chave criptográfica imutável armazenada em hardware;

4.1.5.36. O servidor deverá ser capaz de restaurar, automaticamente, o estado da BIOS/UEFI para uma versão íntegra anterior, armazenada em área de memória oculta e protegida contra gravação, em casos de corrupção identificados durante a inicialização da BIOS/UEFI;

4.1.5.37. Deverá suportar escaneamento de BIOS Firmware em tempo real para detecção de código malicioso;

4.1.5.38. Deve possuir funcionalidade que permita que os discos locais do servidor sejam apagados de forma definitiva através de tecnologia de regravação de dados ou similar. Esta funcionalidade deve possibilitar que sejam definitivamente apagados quaisquer discos dentro do servidor, suportando discos físicos (HDDs), discos criptografados (SEDs) e dispositivos de flash SSDs e NVMe;

4.1.5.39. A console de gerenciamento local deverá implementar modo "System Lockdown", o qual deve impedir que usuários com menos privilégios façam alterações nas configurações do servidor;

4.1.5.40. A console de gerenciamento local deve possuir uma área de armazenamento oculta para a rápida recuperação da BIOS e do Sistema Operacional quando comprometidos;

4.1.5.41. Deverá permitir que as portas USB possam ser desativadas de maneira programada;

Portas de comunicação

4.1.5.42. Todos os conectores das portas de entrada/saída devem ser identificados pelos nomes ou símbolos;

4.1.5.43. Possuir 3 (três) interfaces USB sendo, no mínimo duas destas interfaces no padrão 3.0;

4.1.5.44. Possuir, no mínimo, 1 (uma) porta de vídeo padrão VGA (DB-15) ou Mini-DisplayPort localizada na parte traseira do gabinete;

Interface de rede

4.1.5.45. Possuir 02 (duas) interfaces de rede de 10/25Gb DA/SFP28 em 1 adaptador distinto suportando taxas de transferência de 10Gbps e 25Gbps;

4.1.5.46. Suporte ao protocolo de virtualização VMQ

4.1.5.47. Suporte ao protocolo VXLAN

4.1.5.48. Possuir tecnologia de processamento TCP/IP offload LSO, RSS e TSS

Controladora RAID

4.1.5.49. Controladora RAID, compatível com discos padrão SAS 22.5 Gbps, SAS 12 Gbps, SATA/SAS 6 Gbps e drives NVMe;

4.1.5.50. Memória cache de no mínimo, 8GB (oito gigabytes) sendo que esta quantidade total poderá ser atendida através de uma ou no máximo duas placas instaladas no servidor;

4.1.5.51. Suportar e implementar RAID 0, 1, 5, 6, 10, 50 e 60;

4.1.5.52. Suportar expansão de capacidade de formatação on-line;

4.1.5.53. Permita detecção e recuperação automática de falhas e reconstrução, também de forma automática, dos volumes de RAID sem necessidade de reiniciar o equipamento;

4.1.5.54. Deverá permitir a operação em modo RAID e pass-through em discos distintos. Ou fornecer controladora RAID e controladora pass-through.

4.1.5.55. Suporte a recursos de hot swap para as unidades de disco;

4.1.5.56. Suportar implementação de disco Global Hot-spare;

4.1.5.57. Suportar Self-Monitoring Analysis and Reporting Technology (SMART).

Dispositivos de armazenamento padrão SSD com as seguintes características

4.1.5.58. Para a instalação do Sistema Operacional devem ser fornecidos 2 (dois) drives do tipo SSD (Solid State Drive) no formato de 2,5 polegadas de, no mínimo, 1,92TB cada um, ligados em RAID1 através da controladora de discos especificada acima;

4.1.5.59. Devem ser fornecidos 7 (sete) drives do tipo SSD (Solid State Drive) no formato de 2,5 polegadas de, no mínimo, 960GB cada um, ligados em RAID5 (5+1) + Hot Spare através da controladora de discos especificada acima;

4.1.5.60. Não serão aceitos discos em gabinetes externos ao servidor;

4.1.5.61. Não serão aceitas soluções baseadas em cartão SD ou similar.

Sistema operacional

4.1.5.62. O servidor deverá ser ofertado SEM sistema operacional;

4.1.5.63. O fabricante deve disponibilizar no seu respectivo web site, download gratuito de todos os Drivers dos dispositivos, BIOS e Firmwares para o equipamento ofertado;

4.1.5.64. Apresentar declaração do fabricante informando que todos os componentes do objeto são novos (sem uso, reforma ou recondicionamento) e que não estão fora de linha de fabricação;

4.1.5.65. O modelo do equipamento ofertado deverá suportar o sistema operacional Windows Server 2022 ou superior. Esse item deverá ser comprovado através do HCL (Hardware Compatibility List) da Microsoft no link:

[https://www.windowsservercatalog.com](https://www.windowsservercatalog.com;);

4.1.5.66. O modelo do equipamento ofertado deverá suportar o sistema operacional Red Hat Enterprise Linux 9.4 ou posterior. Esse item deverá ser comprovado através do HCL (Hardware Compatibility List) da Red Hat no link:

<https://hardware.redhat.com/hwcert/index.cgi>;

4.1.5.67. O modelo do equipamento ofertado deverá suportar o sistema de virtualização VMware ESXi 8.0 U3 ou posterior. Esse item deverá ser comprovado através do Compatibility Guide da Broadcom no link:

<https://compatibilityguide.broadcom.com/search?program=server&persona=live&column=partnerName&order=asc>;

4.1.5.68. O modelo do equipamento ofertado deverá suportar o sistema operacional Oracle Linux 8. Esse item deverá ser comprovado através do HCL (Hardware Certification List) da Oracle no link:

Gerenciamento e inventário

4.1.5.69. O equipamento deve possuir solução de gerenciamento do próprio fabricante através de recursos de hardware e software com capacidade de prover as seguintes funcionalidades:

4.1.5.70. O software de gerenciamento deverá estar licenciado para todas as funcionalidades requisitadas nestas especificações e unificar as operações de administração, monitoramento e gestão de tarefas de gerenciamento de todos os servidores fornecidos em uma única console gráfica.

4.1.5.71. O equipamento deve possuir interface de rede dedicada para gerenciamento que suporte nativamente a atribuição de endereçamento IP dinâmico;

4.1.5.72. Permitir o monitoramento remoto, de todo o hardware das condições de funcionamento dos equipamentos e seus componentes, tais como: processadores, memória RAM, controladora RAID, discos, fontes de alimentação, NICs e ventiladores;

4.1.5.73. Permitir acessar a BIOS ou UEFI remotamente;

4.1.5.74. Suportar os protocolos de criptografia SSL para acesso Web e SSH para acesso CLI;

4.1.5.75. Emitir alertas de anormalidade de hardware através do software de gerência e suportar o encaminhamento via e-mail e trap SNMP;

4.1.5.76. Suportar autenticação local e através de integração com MS Active Directory/LDAP;

4.1.5.77. Deverá suportar autenticação de 2 fatores.

4.1.5.78. Permitir o controle remoto da console do servidor do tipo virtual KVM out-of-band, ou seja, independente de sistema operacional ou software agente;

4.1.5.79. Permitir a captura de vídeo ou tela de situações de falhas críticas de sistemas operacionais e inicialização do sistema (boot), possibilitando uma depuração mais aprimorada;

4.1.5.80. As funcionalidades de gerenciamento e monitoramento de hardware devem ser providas por recursos do próprio equipamento e independente de agentes ou sistema operacional;

4.1.5.81. A console virtual deverá ser acessível via interface HTML5 ou, caso necessite de algum tipo de plugin licenciado, por exemplo JAVA, deverá ser fornecido o licenciamento por pelo menos 5 anos;

4.1.5.82. Suportar os protocolos de gerenciamento, IPMI e SNMP v1/v2c/v3, WMI, SSH, WS MAN e REDFISH;

4.1.5.83. Permitir customizar alertas e automatizar a execução de tarefas baseadas em script;

4.1.5.84. O software de gerenciamento deverá permitir instalação remota de sistemas operacionais como Windows, Linux e VMware vSphere.

4.1.5.85. Permitir integração com o VMware vCenter de modo que o gerenciamento e inventário também possa ser realizado através do vSphere Web Client com informações referentes aos hosts (nome do host, endereço IP do host, configuração de CPU, memória, NIC, firmware), além de listar as versões de software e hardware em uso pelo host, controladoras de rede, RAID.

4.1.5.86. A integração com o VMware vCenter deverá permitir a redução nos tempos de resposta a eventos de hardware através de ações automáticas pré-estabelecidas pelo administrador, tais como, evacuação de máquinas virtuais em execução em host que venha emitir alertas de pré-falha de qualquer componente vital como CPU, memória e disco, e manter a estabilidade e a confiabilidade do ambiente através do gerenciamento de firmwares empregados no ambiente, garantindo conformidade entre todos os hosts ESXi;

4.1.5.87. Permitir configurar os seguintes parâmetros de hardware: WWN, BIOS, RAID, NIC, MAC, Virtual Mac address, iSCSI Name, Vlan e perfil de QOS, através de templates pré-definidos;

- 4.1.5.88. Permitir a instalação, update e configuração remota de sistemas operacionais, drivers e firmwares, através de solução de deployment compatível com a solução ofertada;
- 4.1.5.89. Permitir estabelecer perfis de configuração com o inventário das versões de firmwares disponíveis para execução programada de verificações de conformidade das versões de firmware presentes nos demais equipamentos;
- 4.1.5.90. Possuir informações de garantia e apresentar, via relatório e/ou scorecard, listando o tipo de garantia e data limite, em caso de limite informar via e-mail de forma automatizada para que seja possível ação da contratante;
- 4.1.5.91. Permitir a detecção de pré-falhas dos componentes de hardware.
- 4.1.5.92. Realizar a abertura automática de chamados sem intervenção humana, diretamente ao fabricante dos equipamentos em caso de falha de componentes de hardware;
- 4.1.5.93. Permitir ligar, desligar e reiniciar os servidores remotamente e independente de sistema operacional;
- 4.1.5.94. O software de gerenciamento deverá permitir a medição do consumo elétrico de grupos de servidores instalados em um rack, distribuídos em vários racks em um corredor e em todo o data center. Também deverá ser capaz de controlar o consumo elétrico dos servidores e implementar políticas de consumo, reduzindo o consumo individual ou de grupos de equipamentos caso ultrapassem os limites de consumo pré-estabelecidos
- 4.1.5.95. Deve possuir recurso remoto que permita o completo desligamento e reinicialização (Hard-Reset) remoto do equipamento através da interface de gerência ou através de solução alternativa (Hardware/Software);
- 4.1.5.96. Permitir a emulação de mídias virtuais de inicialização (boot) através de CD/DVD remoto, compartilhamentos de rede NFS/CIFS e dispositivos de armazenamento USB remotos;
- 4.1.5.97. Permitir acesso do tipo Console Virtual, do mesmo fabricante dos servidores ofertados, que permita gerenciar, monitorar e configurar parâmetros físicos dos servidores de forma remota e centralizada;
- 4.1.5.98. O software de gerenciamento deve realizar descoberta automática dos servidores, permitindo inventariar os mesmos e seus componentes;
- 4.1.5.99. Suportar o monitoramento remoto (1:1 e 1:N) do consumo de energia elétrica e temperatura dos servidores, através de exibição gráfica, e permitir gerenciar parâmetros de consumo de CPU, memória, IO e Motherboard, com geração de alertas;
- 4.1.5.100. Possuir configuração de alerta de consumo de energia para grupos de dispositivos;
- 4.1.5.101. Possuir controles de energia baseados no tempo (diariamente, semanalmente e ou faixa de datas);
- 4.1.5.102. Permitir configurar dispositivos individuais, grupos físicos e grupos lógicos;
- 4.1.5.103. Permitir comparação de dispositivos relacionado ao seu consumo, criando reports com equipamentos ociosos em consumo e os de maior consumo;
- 4.1.5.104. Deve possuir funcionalidade que permita que os discos locais do servidor sejam apagados de forma definitiva através de tecnologia de regravação de dados ou similar. Esta funcionalidade deve possibilitar que sejam definitivamente apagados quaisquer discos dentro do servidor, suportando, no mínimo discos físicos (HDDs), discos criptografados (SEDs) e dispositivos de memória não volátil (SSDs e NVMe).
- 4.1.5.105. Deve possibilitar o download automático de atualizações de firmwares, BIOS e drivers diretamente do site do fabricante ou repositório local.
- 4.1.5.106. O servidor deve prover mecanismos preliminares às atualizações de firmware da controladora de gerenciamento remoto (BMC, por exemplo) que assegurem que as imagens de atualização possuam assinatura digital cuja autenticidade possa ser verificada usando chave criptográfica imutável armazenada em hardware;
- 4.1.5.107. Deverá fazer o gerenciamento e inventário para até 1500 dispositivos;

Acessórios

4.1.5.108. Devem ser fornecidos junto com o equipamento, todos os acessórios e cabos necessários para o pleno funcionamento do mesmo.

Documentação técnica

4.1.5.109. Deverão ser fornecidos manuais técnicos do usuário e de referência contendo todas as informações sobre os produtos com as instruções para instalação, configuração, operação e administração.

Certificados

4.1.5.110. Deverá ser entregue no dia do pregão a certificação comprovando que o equipamento está em conformidade com a norma IEC 60950, Energy Star, Rohs e Inmetro;

4.1.5.111. As atualizações de BIOS/UEFI devem possuir autenticação criptográfica (assinatura) segundo as especificações NIST SP800-147B, NIST SP800-193 e NIST SP800-155;

4.1.5.112. O fabricante do servidor deve ser membro do DMTF (Desktop Management Task Force) na categoria "BOARD", comprovado através de acesso a página <http://www.dmtf.org/about/list/>;

4.1.5.113. O fabricante do servidor deve ser membro do TCG (Trusted Computing Group) na categoria "PROMOTER", comprovado através do link <https://trustedcomputinggroup.org/membership/member-companies/>;

4.1.5.114. O fabricante do servidor deverá constar na lista pública do TSANet no nível "Elite", de forma a garantir a cooperação entre suportes de fabricantes diferentes acelerando a resolução de problemas, comprovado através do link <https://www.tsanet.org/members/>;

Outros

4.1.5.115. Quando o Licitante não for o próprio fabricante dos equipamentos ofertados, deverá apresentar declaração do Fabricante específica para o edital, autorizando a empresa licitante a comercializar e prestar os serviços de garantia exigidos;

4.1.5.116. Os componentes do equipamento deverão ser homologados pelo fabricante. Não será aceita a adição ou subtração de qualquer componente não original de fábrica para adequação do equipamento;

4.1.5.117. Apresentação de no mínimo um atestado emitido por pessoa jurídica de direito público ou privado, comprovando que a proponente fornece/forneceu bens compatíveis com os objetos da licitação, emitidos em papel timbrado, com assinatura, identificação e telefone do emitente.

4.1.6 APPLIANCE SCALE-OUT NAS PARA ARMAZENAMENTO DE DADOS

4.1.6.1 Appliance Scale-Out NAS para armazenamento de dados não estruturados para instalação em rack de 19" (dezenove polegadas) onde deverão ser fornecidos os respectivos kits de fixação;

4.1.6.2 Não serão aceitos sistemas de armazenamento do tipo UNIFIED que consolidam sistemas de armazenamento com arquitetura de Bloco, sistemas de armazenamento de Arquivos (NAS) e sistemas de armazenamento de Objetos.

4.1.6.3 A solução de armazenamento NAS deve ser um cluster com arquitetura scale-out, composta por nós /controladoras, dispositivos SSD, discos mecânicos SATA/NL-SAS, Portas de Front-End e portas de Back-End, conforme a seguir;

4.1.6.4 Cada Nó/Controladora da solução Scale-Out NAS deve conter, no mínimo:

4.1.6.4.1 Capacidade individual bruta máxima de discos SATA/NL-SAS de até 8 TB;

4.1.6.4.2 Capacidade total bruta mínima de 3.2 TB, em drives SSD, composta com no mínimo dois drives;

4.1.6.4.3 Mínimo de 2 portas ethernet 25 Gb/s SFP28 exclusivamente para front-end;

4.1.6.4.4 Mínimo de 2 portas ethernet 100 Gb/s QSFP28 exclusivamente para Back-end;

4.1.6.4.5 Mínimo de 96 GB de memória RAM;

4.1.6.5. Entende-se por Nó/Controladora, um conjunto autônomo contendo CPUs, interfaces de comunicação, memórias, controladoras de discos de modo a permitir um crescimento linear da capacidade de processamento, throughput e área de armazenamento de dados.

4.1.6.6 Cada Nó/Controladora deve ser autônomo, contendo internamente todos os componentes descritos acima. Não serão aceitas soluções que contenham nós intermediários, ou que possuam funções específicas de acesso ou armazenamento no cluster.

4.1.6.7 Os Nós/Controladoras deverão se agregar em regime scale-out ao cluster, expandindo a sua área útil de acordo com a capacidade solicitada.

4.1.6.8 A solução ofertada deverá fazer uso de no mínimo, 4 (quatro) nós/controladoras, visando garantir alta disponibilidade e resiliência dos dados, bem como performance. Em caso de soluções que precisem de nós /controladoras somente para processamento, também deverá ser considerado o mesmo número de nós/controladoras para esta finalidade.

4.1.6.9 Cada sistema de armazenamento deve possuir a capacidade utilizável mínima de 162 TiB (Cento e Sessenta e Dois Tebibytes) líquidos/utilizáveis, e deve suportar escalabilidade do tipo Scale-Out podendo chegar à capacidade de no mínimo 10 PiB (dez PebiBytes), bem como agregar performance para acompanhar o crescimento da solução. A escalabilidade deverá ocorrer em um único cluster, sistema de arquivos e namespace com todo o volume NAS disponível. Não será permitida a utilização de agregação de namespaces para atingir a escalabilidade solicitada.

4.1.6.9 A capacidade disponível para armazenamento de dados não deve considerar compactação, deduplicação, reservas necessárias para sistema e controles internos, proteção/resiliência, paridade ou discos hot-spare.

4.1.6.10 Deve-se considerar 1GB (um gigabyte) igual a 1024MB (mil e vinte e quatro megabytes), ou seja, deve-se considerar notação binária (Base2) para os cálculos de capacidade de armazenamento.

4.1.6.11 A solução deverá suportar a expansão da área útil de armazenamento de forma transparente para os clientes, ou seja, não serão aceitas soluções que exijam qualquer procedimento de reinicialização, ou mesmo soluções que exijam o “desmapeamento” de unidades lógicas ou mount points de rede para reconhecimento da área de armazenamento expandida.

4.1.6.12 A solução deve possuir um desempenho de no mínimo de 4.8 GB/s (Quatro Gigabytes e Oitocentos Megabytes por segundo de leitura) e 2,4 GB/s (Dois Gigabytes e Quatrocentos Megabytes por segundo de escrita) em NFS versão 3, com tamanho mínimo de bloco de 128 Kilobytes. A comprovação de performance deverá ser feita por relatórios de desempenho (sizing) do fabricante com base nos requerimentos desta solicitação.

4.1.6.13 A solução ofertada deve suportar escalabilidade do tipo scale-out, devendo agregar capacidade e performance sem a necessidade de interrupção no acesso aos dados pelas aplicações e clientes. O sistema deve suportar ser expandido para, no mínimo, 24 (Vinte e Quatro) Nós/Controladoras em único cluster para comportar futuras expansões.

4.1.6.14 Deverá ser capaz de suportar falhas de, no mínimo, 2 (dois) drives simultaneamente ou 1 (um) nó /controladora], devendo ser fornecido com técnica de proteção/resiliência baseado em RAID ou Erasure Code.

4.1.6.15 Em caso de falha de nó/controladora a solução não pode perder mais do que 25% do Processamento e Desempenho em throughput.

4.1.6.16 A solução deve permitir acesso para compartilhamento de arquivos, utilizando no mínimo os protocolos: FTP, HTTP/HTTPS, NFSv3, NFSv4, NFSv4.1, NFSv4.2, SMB 1, SMB 2.0, SMB 2.1, SMB 3.0, SMB 3.1.1, HDFS e S3 de forma nativa e sem a necessidade de softwares de terceiros. Estes protocolos devem estar disponíveis para todo o conjunto de interfaces e para toda a capacidade líquida da solução, suportando inclusive a escalabilidade solicitada.

4.1.6.17 Deverá ser compatível com distribuições Hadoop Cloudera (CDH) e Hortonworks (HDP).

4.1.6.18 O sistema operacional dos nós/controladoras deverão ser nativos do produto e não serão permitidos sistemas operacionais de propósito geral, baseado em Windows ou Unix/Linux e suas variações, exceto se completamente customizado e suportado integralmente pelo fabricante da solução.

4.1.6.19 Não serão permitidas soluções baseadas em virtualização de subsistemas, gateways ou sistemas de soluções baseadas em SDS (Software Defined Storage).

4.1.6.20 Não serão permitidas soluções baseadas em softwares de clusterização de mercado, como Veritas Cluster, Microsoft Cluster, Ceph, Minio ou similares.

4.1.6.21 A solução deverá suportar, no mínimo, 20 bilhões de arquivos em um único file system.

4.1.6.22 Os Nós/Controladoras deverão possuir redundância de fontes de alimentação, ventilação, Rede de Back-End para interconexão do cluster, além de permitir a substituição de qualquer um destes componentes de maneira não disruptiva.

4.1.6.23 Cada fonte de alimentação deverá vir acompanhada de um cabo de alimentação C13/C14.

4.1.6.24 A Solução deverá permitir a atualização do sistema operacional entre versões para correção e atualização global do sistema de armazenamento, sem parada do global namespace.

4.1.6.25 A solução deverá permitir a troca de drives, sem interrupção das operações de I/O, para escrita e leitura.

4.1.6.26 As atividades de administração do equipamento deverão ser realizadas via interfaces Ethernet. Estas interfaces podem ou não ser compartilhadas com acesso aos dados (CIFS/SMB, NFS, HDFS e S3).

4.1.6.27 A solução deverá permitir o gerenciamento centralizado, através de interface web, para todos os componentes da solução.

4.1.6.28 A solução ofertada deverá incluir todos os componentes necessários para instalação e funcionamento como os switches de rede de Back-End com conectividade de 100 Gbps (cem gigabits por segundo), cabos DAC ou transceptores e fibras óticas.

4.1.6.29 Em relação aos cabos DAC ou transceptores e fibras óticas de front-end (que servirão para a conexão com as redes do datacenter), eles podem ser fornecidos no item referente aos switches de 48 portas.

4.1.6.30 Deverá incluir o rack de 19 polegadas e de 42U de altura com, no mínimo, 2 PDUs que suportem, no mínimo, 14 KVA de consumo elétrico.

4.1.6.31 Deverá incluir todas as licenças para habilitar todas as funcionalidades para uso simultâneo e em toda capacidade contratada para o sistema.

4.1.6.32 O gerenciamento deve permitir a criação de níveis de acesso de usuários (super usuário, administrador e operador).

4.1.6.33 A solução deverá permitir acesso via SSH para administração remota.

4.1.6.34 A arquitetura da solução deverá ser distribuída e composta por Nós/Controladoras que atuem de forma paralela, com processamento simétrico. Todos os Nós/Controladoras que compõem a solução deverão ser ativos.

4.1.6.35 A rede interna de comunicação, que proporciona a sincronização entre os nós do cluster, deverá ser exclusiva, especialmente desenhada, implantada e separada da rede de serviços de compartilhamento de áreas de armazenamento.

4.1.6.36 A rede de comunicação entre os nós deverá ser implantada com alta disponibilidade de maneira ponto a ponto, com velocidade mínima de 100 Gbps (cem gigabits por segundo) por porta, nos Nós/Controladoras.

4.1.6.37 A solução deverá balancear o armazenamento dos dados de forma automática entre todos os nós que compõem o cluster de alto processamento, sem utilização de nenhum componente externo.

4.1.6.38 A solução deverá fornecer um mecanismo de balanceamento de acesso dos clientes em suas interfaces de rede de frontend.

4.1.6.39 A solução deverá possuir tecnologia de deduplicação e compressão inline para redução de dados antes da escrita dos dados nos drives. Estas funcionalidades devem estar habilitadas para todo o cluster, mesmo não sendo consideradas para o cálculo da capacidade solicitada.

4.1.6.40 A solução deverá implantar movimentação automática de arquivos ou blocos, entre diferentes camadas de armazenamento (tiering), disponíveis no cluster, definidas por tipo e velocidade de acesso aos dados.

4.1.6.41 A movimentação deverá ocorrer com o uso de recursos internos da solução, sem softwares ou appliances externos.

4.1.6.42 A movimentação deve ocorrer periodicamente, entre diferentes camadas de armazenamento existentes no equipamento, de acordo com políticas definidas pelo administrador.

4.1.6.43 É necessário que o administrador do sistema possa realizar a configuração das políticas que definirão em que camada de armazenamento o arquivo deve residir.

4.1.6.44 A solução deverá ter integração nativa e completa com solução de Armazenamentos do tipo Objetos e suportar a expansão da sua capacidade para este sistema (tierização ou transbordo), via protocolo S3.

4.1.6.45 A extensão de armazenamento para o Storage de Objetos deverá ser imperceptível para as aplicações e/ou usuários, onde os arquivos ou blocos enviados para tal camada, deverão ser substituídos por stubs ou links automaticamente em suas localizações originais.

4.1.6.46 Deverá ser possível criar regras/políticas para a movimentação de arquivos ou blocos para o storage de objetos.

4.1.6.47 A solução deverá se integrar com serviços de diretório, para promover a autenticação e autorização dos usuários, pelos sistemas de arquivos: Active Directory (AD) da Microsoft, LDAP, NIS e autenticação local (RBAC).

4.1.6.48 O cluster scale-out deve ser capaz de se integrar simultaneamente a no mínimo 10 servidores Active Directory (AD), mesmo que de florestas distintas e sem relação de confiança (trust) entre eles.

4.1.6.49 A solução deverá possuir mecanismo de "Single Sign-On" (SSO) como ponto único e centralizado de administração por linha de comando ou Web baseado em "SAML" (Security Assertion Markup Language), preferencialmente com o Active Directory Federation Services (AD FS). Caso o

PROPONENTE não tenha compatibilidade com os provedores de identidade (IDPs) no Active Directory Federation Services (AD FS) poderá fornecer em outras plataformas, porém toda implementação, inclusive os softwares necessários bem como os tokens de acesso, será de responsabilidade do PROPONENTE.

4.1.6.50 A solução deverá permitir a configuração de limites no número máximo de operações de protocolo (QoS) para a taxa de transferência de dados (throughput) ou de operações de protocolos (OPS) no mínimo para os protocolos NFS, SMB e S3.

4.1.6.51 A solução deverá possibilitar integração com sistemas de antivírus utilizando técnicas de ICAP Server e CAVA, de forma que qualquer arquivo manipulado pelo usuário seja verificado por um processo de procura e verificação de vírus.

4.1.6.52 A solução deverá ser homologada no mínimo para os antivírus dos seguintes fabricantes: Symantec, TrendMicro e McAfee.

4.1.6.53 A solução deverá suportar nativamente IPv4 e IPv6.

4.1.6.54 A solução deverá suportar monitoramento de utilização de seus componentes com armazenamento de dados históricos, de forma que os dados possam ser analisados e utilizados para provisionamento e upgrades futuros.

4.1.6.55 A solução deverá suportar cotas de armazenamento para usuários e as cotas deverão ser aplicadas em pasta vazias, pastas já em uso e em qualquer nível de profundidade da árvore de subdiretórios.

4.1.6.56 As cotas deverão ser implementadas através de políticas pré-definidas pelo administrador, aplicáveis a qualquer usuário ou grupo de usuários configurado no “namespace global”.

4.1.6.57 A implementação de cotas deverá monitorar a utilização de espaço de armazenamento pelos usuários e garantir que os mesmos não ultrapassem os limites configurados, permitindo que a solução tenha a opção de bloquear a escrita e/ou enviar alertas amigáveis para usuários.

4.1.6.58 A política de cotas deverá possuir suporte ao provisionamento dinâmico, ou seja, deverá permitir que o administrador da solução entregue aos usuários uma capacidade de armazenamento maior do que a capacidade efetiva do equipamento.

4.1.6.59 A solução deverá registrar todas as atividades administrativas, eventos e falhas de componentes, em um sistema unificado de registro de eventos.

4.1.6.60 A solução deverá implantar auditoria do sistema de arquivos, ao menos para os protocolos SMB, NFS e S3.

4.1.6.61 Os dados coletados pelo subsistema de auditoria devem ser automaticamente exportados para sistemas centralizados de armazenamento de log de terceiros, através dos protocolos padrões de mercado para este fim, sendo possível enviar as informações de auditoria para um servidor syslog.

4.1.6.62 A solução deverá possibilitar a implantação de Snapshots para os dados armazenados, sendo permitida a criação de snapshots por volume ou pasta.

4.1.6.63 A solução deverá ser capaz de expandir sua capacidade para uma camada de armazenamento em nuvem pública de forma imperceptível para as aplicações e usuários, onde os arquivos tierizados para tal camada, deverão ser substituídos por “Stubs” ou “links” automaticamente em suas localizações originais.

4.1.6.64 A solução deve suportar, no mínimo os provedores de nuvem pública GCP (Google), AWS (Amazon) e Azure (Microsoft) para esta finalidade.

4.1.6.65 Não será necessário prover licença neste certame, mas deverá ter a capacidade para prover a funcionalidade

4.1.6.66 Além da tierização, deverá ser possível criar regras para a cópia de arquivos para a nuvem pública (Bucket S3), utilizando recursos nativos sem a necessidade de ferramentas externas.

4.1.6.67 A solução deve suportar, no mínimo 1 (um) provedor de nuvem pública para esta finalidade.

4.1.6.68 A solução deverá permitir a implementação de técnicas de backup de filesystem / diretório / arquivos, utilizando-se o protocolo NDMP versão 4.

4.1.6.69 Deverá ser compatível com topologia 2-Way NDMP e 3-Way NDMP.

4.1.6.70 A solução ofertada deverá suportar a funcionalidade de mídia WORM (Write Once Read Many), garantindo a não alteração dos dados armazenados. A funcionalidade de WORM da solução deve ser inerente a solução, não sendo permitido a disponibilização por meio de softwares externos e deve atender a norma de compliance SEC-17a4.

4.1.6.71 O prazo de retenção deverá ser atribuído a cada pasta e seu conteúdo armazenado, permitindo diferentes períodos de retenção por pasta. Não podendo ser atribuído unicamente a todo volume.

4.1.6.72 A solução ofertada deverá prover CSI (Container Storage Interface) driver para provisionamento de armazenamento persistente e reduzir a complexidade para K8s (Kubernetes) em ambiente moderno de aplicativos.

4.1.6.73 O fabricante deve estar enquadrado, na categoria “Board” do Consórcio DMTF (Distributed Management Task Force), descrito no site oficial <http://www.dmtf.org/about/list>.

4.1.7 SERVIDOR RACK TIPO 1U – 2 PROCS / 256 GB RAM

Gabinete

- 4.1.7.1. Gabinete para instalação em rack de 19" através de sistema de trilhos deslizantes;
- 4.1.7.2 Altura máxima de 1U;
- 4.1.7.3 Deve possuir botão liga/desliga na parte frontal do equipamento;
- 4.1.7.4 Deve possuir suporte de no mínimo 10 (dez) baias para instalação de drives do tipo SAS/SATA;
- 4.1.7.5 Deverá ser entregue junto com o servidor, um kit de fixação para rack, do tipo retrátil, permitindo o deslizamento do servidor a fim de facilitar sua manutenção;
- 4.1.7.6 Possuir projeto tool-less, ou seja, não necessita de ferramentas para instalação/desinstalação de placas de expansão;
- 4.1.7.7 Deve possuir sistema de ventilação redundante e hot-pluggable para que a CPU suporte a configuração máxima e dentro dos limites de temperatura adequados para o perfeito funcionamento do equipamento, e que permita a substituição do mesmo com o equipamento em funcionamento.
- 4.1.7.8 Deverá ser fornecido com Módulo TPM 2.0 FIPS ou superior;

Fonte de Alimentação

- 4.1.7.9 Mínimo de 2 (duas) fontes, suportando o funcionamento do equipamento na configuração ofertada mesmo em caso de falha de uma das fontes;
- 4.1.7.9 Deverá ser fornecido com sua quantidade máxima de fontes;
- 4.1.7.10 As fontes deverão ser totalmente redundantes e hot-pluggable permitindo a substituição de qualquer uma das fontes em caso de falha sem parada ou comprometimento do funcionamento do equipamento;
- 4.1.7.11 As fontes de alimentação devem possuir certificação 80Plus, no mínimo na categoria TITANIUM.
- 4.1.7.12 A fonte deve ter potência mínima de 1.500 watts;
- 4.1.7.13 As fontes devem possuir tensão de entrada de 100VAC a 240VAC a 60Hz, com ajuste automático de tensão;
- 4.1.7.14 Deverá acompanhar cabo de alimentação C13/C14 para cada fonte de alimentação fornecida.

Processador

- 4.1.7.15 O servidor deverá suportar processadores do tipo single-threaded, com até 144 núcleos, ou multi-threaded, com até 86 núcleos, por processador;
- 4.1.7.16 Equipado com 2 (dois) processadores de 32 núcleos do tipo multi-threaded, com arquitetura x86;
- 4.1.7.17 Deverá implementar mecanismos de gerenciamento do consumo de energia compatível com o padrão ACPI;
- 4.1.7.18 Deve suportar conjunto de instruções estendido compatível com padrão AVX-512;
- 4.1.7.19 Consumir no máximo 250W;
- 4.1.7.20 Frequência de clock interno de no mínimo 2.5 GHz;
- 4.1.7.21 Controladora de memória com suporte a DDR5 de no mínimo 6400 MT/s para 1 DIMM por canal, ou 5200 MT/s para 2 DIMMs por canal;
- 4.1.7.22 Link de comunicação do processador com o restante do sistema de 24 GT/s;
- 4.1.7.23 Memória cache de 288 MB – L3.

Desempenho

4.1.7.24 O processador ofertado deverá ter índice SPEC CPU2017 Integer Rate Results (Baseline) auditado de no mínimo 721 para 2 processadores. Os índices SPEC CPU2017 Integer Rate Results (Baseline) utilizados como referência serão validados junto ao site da Internet <https://www.spec.org/> Standard Performance Evaluation Corporation. Não serão aceitas estimativas para modelos / famílias de processadores não auditados pelo SPEC, resultados obtidos com a utilização de servidores em cluster, bem como estimativas em resultados inferiores ao mínimo especificado;

4.1.7.25 Não será aceito modelo de servidor não auditada pelo Standard Performance Evaluation Corporation ou auditada antes de 2017.

Memória RAM

4.1.7.26 Módulos de memória RAM tipo DDR5 RDIMM (Registered DIMM) com tecnologia de correção ECC (Error Correcting Code) e velocidade de, no mínimo, 6400 MT/s;

4.1.7.27 Deve possuir no mínimo 32 slots de memória DIMM;

4.1.7.28 Deve possuir 256 GB de memória instalada;

Circuitos Integrados (Chipset) e Placa Mãe

4.1.7.29 O chipset deve ser da mesma marca do fabricante do processador;

4.1.7.30 Possuir, no mínimo, 2 slots OCP 3.0 e 2 slots PCI Express 5.0;

4.1.7.31 Placa mãe da mesma marca do fabricante do equipamento, desenvolvida especificamente para o modelo ofertado. Não serão aceitas placas de livre comercialização no mercado;

Controladora de Vídeo

4.1.7.32 Deve ser do tipo on board (integrado na placa mãe) ou placa de vídeo PCIe;

4.1.7.33 Resolução gráfica de 1024 x 768 pixels ou superior.

BIOS ou UEFI

4.1.7.34 Possuir UEFI (Unified Extensible Firmware Interface) ou BIOS (Basic Input Output System) totalmente compatível e desenvolvida para o servidor fornecido;

4.1.7.35 A BIOS/UEFI deve ser atualizável por software;

4.1.7.36 O servidor deve implementar mecanismos de garantia de integridade e autenticidade do código da BIOS /UEFI, antes de sua execução, por meio de assinatura digital que poderá ser validada usando chave criptográfica imutável armazenada em hardware;

4.1.7.37 O servidor deve prover mecanismos preliminares às atualizações de firmware da BIOS/UEFI e de firmware da controladora de gerenciamento remoto que assegurem que os pacotes de atualização de firmware possuam assinatura digital cuja autenticidade poderá ser verificada usando chave criptográfica imutável armazenada em hardware;

4.1.7.38 O servidor deverá ser capaz de restaurar, automaticamente, o estado da BIOS/UEFI para uma versão íntegra anterior, armazenada em área de memória oculta e protegida contra gravação, em casos de corrupção identificados durante a inicialização da BIOS/UEFI;

4.1.7.39 Deverá suportar escaneamento de BIOS Firmware em tempo real para detecção de código malicioso;

4.1.7.40 Deve possuir funcionalidade que permita que os discos locais do servidor sejam apagados de forma definitiva através de tecnologia de regravação de dados ou similar. Esta funcionalidade deve possibilitar que sejam definitivamente apagados quaisquer discos dentro do servidor, suportando discos físicos (HDDs), discos criptografados (SEDs) e dispositivos de flash SSDs e NVMe;

4.1.7.41 A console de gerenciamento local deverá implementar modo "System Lockdown", o qual deve impedir que usuários com menos privilégios façam alterações nas configurações do servidor;

4.1.7.42 A console de gerenciamento local deve possuir uma área de armazenamento oculta para a rápida recuperação da BIOS e do Sistema Operacional quando comprometidos;

4.1.7.43 Deverá permitir que as portas USB possam ser desativadas de maneira programada;

Portas de Comunicação

4.1.7.44 Todos os conectores das portas de entrada/saída devem ser identificados pelos nomes ou símbolos;

4.1.7.45 Possuir 3 (três) interfaces USB sendo, no mínimo duas destas interfaces no padrão 3.0;

4.1.7.46 Possuir, no mínimo, 1 (uma) porta de vídeo padrão VGA (DB-15);

Interface de rede

4.1.7.47 Possuir 02 (duas) interfaces de rede de 10/25Gb DA/SFP28 em 1 adaptador distinto suportando taxas de transferência de 10Gbps e 25Gbps;

4.1.7.48 Suporte ao protocolo de virtualização VMQ

4.1.7.49 Suporte ao protocolo VXLAN

4.1.7.50 Possuir tecnologia de processamento TCP/IP offload LSO, RSS e TSS.

Controladora RAID

4.1.7.51 Controladora RAID, compatível com discos padrão SAS 22.5 Gbps, SAS 12 Gbps, SATA/SAS 6 Gbps e drives NVMe;

4.1.7.52 Memória cache de no mínimo, 8GB (oito gigabytes) sendo que esta quantidade total poderá ser atendida através de uma ou no máximo duas placas instaladas no servidor;

4.1.7.53 Suportar e implementar RAID 0, 1, 5, 6, 10, 50 e 60;

4.1.7.54 Suportar expansão de capacidade de formatação on-line;

4.1.7.55 Permita detecção e recuperação automática de falhas e reconstrução, também de forma automática, dos volumes de RAID sem necessidade de reiniciar o equipamento;

4.1.7.56 Deverá permitir a operação em modo RAID e pass-through em discos distintos. Ou fornecer controladora RAID e controladora pass-through.

4.1.7.57 Suporte a recursos de hot swap para as unidades de disco;

4.1.7.58 Suportar implementação de disco Global Hot-spare;

4.1.7.59 Suportar Self-Monitoring Analysis and Reporting Technology (SMART).

Dispositivos de armazenamento padrão SSD com as seguintes características

4.1.7.60 Para a instalação do Sistema Operacional devem ser fornecidos 2 (dois) drives do tipo SSD (Solid State Drive) NVMe no formato M.2 de, no mínimo, 480GB cada um, ligados em RAID1 através de uma controladora de discos exclusiva e dedicada para estes drives;

4.1.7.61 Devem ser fornecidos 5 (cinco) drives do tipo SSD (Solid State Drive) no formato de 2,5 polegadas de, no mínimo, 960GB cada um, ligados em RAID5 (3+1) + Hot Spare através da controladora de discos especificada acima;

4.1.7.61.1 Estes drives de 960GB devem ser do tipo hot plug e hot swap, que permita sua substituição sem a necessidade de desligar o equipamento, garantindo a continuidade das operações sem impacto para as aplicações;

4.1.7.61.2 Estes drives de 960GB devem possuir DWPD igual a 1 medido pelo período de 5 anos;

4.1.7.62 Devem possuir taxa de transferência de, no mínimo, 6Gb/s;

4.1.7.63 Devem ser do tipo SATA Read Intensive;

4.1.7.64 Não serão aceitos discos em gabinetes externos ao servidor;

4.1.7.65 Não serão aceitas soluções baseadas em cartão SD ou similar.

Sistema Operacional

4.1.7.66 O servidor deverá ser ofertado com o sistema operacional SUSE Linux Enterprise Server com SUSE Manager Lifecycle Management licenciado para todos os núcleos de todos os processadores;

4.1.7.67 O fabricante deve disponibilizar no seu respectivo web site, download gratuito de todos os Drivers dos dispositivos, BIOS e Firmwares para o equipamento ofertado;

4.1.7.68 Apresentar declaração do fabricante informando que todos os componentes do objeto são novos (sem uso, reforma ou recondicionamento) e que não estão fora de linha de fabricação;

4.1.7.69 O modelo do equipamento ofertado deverá suportar o sistema operacional Windows Server 2022 ou superior. Esse item deverá ser comprovado através do HCL (Hardware Compatibility List) da Microsoft no link: <https://www.windowsservercatalog.com>;

4.1.7.70 O modelo do equipamento ofertado deverá suportar o sistema operacional Red Hat Enterprise Linux 9.4 ou posterior. Esse item deverá ser comprovado através do HCL (Hardware Compatibility List) da Red Hat no link: <https://hardware.redhat.com/hwcert/index.cgi>;

4.1.7.71 O modelo do equipamento ofertado deverá suportar o sistema de virtualização VMware ESXi 8.0 ou posterior. Esse item deverá ser comprovado através do Compatibility Guide da Broadcom no link: <https://compatibilityguide.broadcom.com/search?program=server&persona=live&column=partnerName&order=asc>;

4.1.7.72 O modelo do equipamento ofertado deverá suportar o sistema operacional SUSE Linux Enterprise Server 15 SP6 ou posterior para Intel 64. Esse item deverá ser comprovado através do HCL (Hardware Compatibility List) da SUSE no link: <https://www.suse.com/yesCertified/home>.

Gerenciamento e Inventário

4.1.7.73 O equipamento deve possuir solução de gerenciamento do próprio fabricante através de recursos de hardware e software com capacidade de prover as seguintes funcionalidades:

4.1.7.74 O software de gerenciamento deverá estar licenciado para todas as funcionalidades requisitadas nestas especificações e unificar as operações de administração, monitoramento e gestão de tarefas de gerenciamento de todos os servidores fornecidos em uma única console gráfica.

4.1.7.75 O equipamento deve possuir interface de rede dedicada para gerenciamento que suporte nativamente a atribuição de endereçamento IP dinâmico;

4.1.7.76 Permitir o monitoramento remoto, de todo o hardware das condições de funcionamento dos equipamentos e seus componentes, tais como: processadores, memória RAM, controladora RAID, discos, fontes de alimentação, NICs e ventiladores;

4.1.7.77. Permitir acessar a BIOS ou UEFI remotamente;

4.1.7.78 Suportar os protocolos de criptografia SSL para acesso Web e SSH para acesso CLI;

4.1.7.79 Emitir alertas de anormalidade de hardware através do software de gerência e suportar o encaminhamento via e-mail e trap SNMP;

4.1.7.80 Suportar autenticação local e através de integração com MS Active Directory/LDAP;

4.1.7.81 Deverá suportar autenticação de 2 fatores.

4.1.7.82 Permitir o controle remoto da console do servidor do tipo virtual KVM out-of-band, ou seja, independente de sistema operacional ou software agente;

4.1.7.83 Permitir a captura de vídeo ou tela de situações de falhas críticas de sistemas operacionais e inicialização do sistema (boot), possibilitando uma depuração mais aprimorada;

4.1.7.84 As funcionalidades de gerenciamento e monitoramento de hardware devem ser providas por recursos do próprio equipamento e independente de agentes ou sistema operacional;

4.1.7.85 A console virtual deverá ser acessível via interface HTML5 ou, caso necessite de algum tipo de plugin licenciado, por exemplo JAVA, deverá ser fornecido o licenciamento por pelo menos 5 anos;

4.1.7.86 Suportar os protocolos de gerenciamento, IPMI e SNMP v1/v2c/v3, WMI, SSH, WS MAN e REDFISH;

4.1.7.87 Permitir customizar alertas e automatizar a execução de tarefas baseadas em script;

4.1.7.88 O software de gerenciamento deverá permitir instalação remota de sistemas operacionais como Windows, Linux e VMware vSphere.

4.1.7.89 Permitir integração com o VMware vCenter de modo que o gerenciamento e inventário também possa ser realizado através do vSphere Web Client com informações referentes aos hosts (nome do host, endereço IP do host, configuração de CPU, memória, NIC, firmware), além de listar as versões de software e hardware em uso pelo host, controladoras de rede, RAID.

4.1.7.90 A integração com o VMware vCenter deverá permitir a redução nos tempos de resposta a eventos de hardware através de ações automáticas pré-estabelecidas pelo administrador, tais como, evacuação de máquinas virtuais em execução em host que venha emitir alertas de pré-falha de qualquer componente vital como CPU, memória e disco, e manter a estabilidade e a confiabilidade do ambiente através do gerenciamento de firmwares empregados no ambiente, garantindo conformidade entre todos os hosts ESXi;

4.1.7.91 Permitir configurar os seguintes parâmetros de hardware: WWN, BIOS, RAID, NIC, MAC, Virtual MAC Address, iSCSI Name, VLAN e perfil de QOS, através de templates pré-definidos;

4.1.7.92 Permitir a instalação, update e configuração remota de sistemas operacionais, drivers e firmwares, através de solução de deployment compatível com a solução ofertada;

4.1.7.93 Permitir estabelecer perfis de configuração com o inventário das versões de firmwares disponíveis para execução programada de verificações de conformidade das versões de firmware presentes nos demais equipamentos;

4.1.7.94 Possuir informações de garantia e apresentar, via relatório e/ou scorecard, listando o tipo de garantia e data limite, em caso de limite informar via email de forma automatizada para que seja possível ação da contratante;

4.1.7.95 Permitir a detecção de pré-falhas dos componentes de hardware.

4.1.7.96 Realizar a abertura automática de chamados sem intervenção humana, diretamente ao fabricante dos equipamentos em caso de falha de componentes de hardware;

4.1.7.97 Permitir ligar, desligar e reiniciar os servidores remotamente e independente de sistema operacional;

4.1.7.98 O software de gerenciamento deverá permitir a medição do consumo elétrico de grupos de servidores instalados em um rack, distribuídos em vários racks em um corredor e em todo o data center. Também deverá ser capaz de controlar o consumo elétrico dos servidores e implementar políticas de consumo, reduzindo o consumo individual ou de grupos de equipamentos caso ultrapassem os limites de consumo pré-estabelecidos;

4.1.7.99 Deve possuir recurso remoto que permita o completo desligamento e reinicialização (Hard-Reset) remoto do equipamento através da interface de gerência ou através de solução alternativa (Hardware/Software);

- 4.1.7.100 Permitir a emulação de mídias virtuais de inicialização (boot) através de CD/DVD remoto, compartilhamentos de rede NFS/CIFS e dispositivos de armazenamento USB remotos;
- 4.1.7.101 Permitir acesso do tipo Console Virtual, do mesmo fabricante dos servidores ofertados, que permita gerenciar, monitorar e configurar parâmetros físicos dos servidores de forma remota e centralizada;
- 4.1.7.102 O software de gerenciamento deve realizar descoberta automática dos servidores, permitindo inventariar os mesmos e seus componentes;
- 4.1.7.103 Suportar o monitoramento remoto (1:1 e 1:N) do consumo de energia elétrica e temperatura dos servidores, através de exibição gráfica, e permitir gerenciar parâmetros de consumo de CPU, memória, IO e Motherboard, com geração de alertas;
- 4.1.7.104 Possuir configuração de alerta de consumo de energia para grupos de dispositivos;
- 4.1.7.105 Possuir controles de energia baseados no tempo (diariamente, semanalmente e ou faixa de datas);
- 4.1.7.106 Permitir configurar dispositivos individuais, grupos físicos e grupos lógicos;
- 4.1.7.107 Permitir comparação de dispositivos relacionado ao seu consumo, criando reports com equipamentos ociosos em consumo e os de maior consumo;
- 4.1.7.108 Deve possuir funcionalidade que permita que os discos locais do servidor sejam apagados de forma definitiva através de tecnologia de regravação de dados ou similar. Esta funcionalidade deve possibilitar que sejam definitivamente apagados quaisquer discos dentro do servidor, suportando, no mínimo discos físicos (HDDs), discos criptografados (SEDs) e dispositivos de memória não volátil (SSDs e NVMe).
- 4.1.7.109 Deve possibilitar o download automático de atualizações de firmwares, BIOS e drivers diretamente do site do fabricante ou repositório local.
- 4.1.7.110 O servidor deve prover mecanismos preliminares às atualizações de firmware da controladora de gerenciamento remoto (BMC, por exemplo) que assegurem que as imagens de atualização possuam assinatura digital cuja autenticidade possa ser verificada usando chave criptográfica imutável armazenada em hardware;
- 4.1.7.111 Deverá fazer o gerenciamento e inventário para até 1500 dispositivos;

Acessórios

- 4.1.7.112 Devem ser fornecidos junto com o equipamento, todos os acessórios e cabos necessários para o pleno funcionamento do mesmo.

Documentação Técnica

- 4.1.7.113 Deverão ser fornecidos manuais técnicos do usuário e de referência contendo todas as informações sobre os produtos com as instruções para instalação, configuração, operação e administração.

Certificados

- 4.1.7.114 Deverá ser entregue no dia do pregão a certificação comprovando que o equipamento está em conformidade com a norma IEC 60950, Energy Star, Rohs e Inmetro;
- 4.1.7.115 As atualizações de BIOS/UEFI devem possuir autenticação criptográfica (assinatura) segundo as especificações NIST SP800-147B, NIST SP800-193 e NIST SP800-155;
- 4.1.7.116 O fabricante do servidor deve ser membro do DMTF (Desktop Management Task Force) na categoria "BOARD", comprovado através de acesso a página <http://www.dmtf.org/about/list/>;
- 4.1.7.117 O fabricante do servidor deve ser membro do TCG (Trusted Computing Group) na categoria "PROMOTER", comprovado através do link <https://trustedcomputinggroup.org/membership/member-companies/>;

4.1.7.118 O fabricante do servidor deverá constar na lista pública do TSANet no nível “Elite”, de forma a garantir a cooperação entre suportes de fabricantes diferentes acelerando a resolução de problemas, comprovado através do link <https://www.tsanet.org/members/>;

Outros

4.1.7.119 Quando o Licitante não for o próprio fabricante dos equipamentos ofertados, deverá apresentar declaração do Fabricante específica para o edital, autorizando a empresa licitante a comercializar e prestar os serviços de garantia exigidos;

4.1.7.120 Os componentes do equipamento deverão ser homologados pelo fabricante. Não será aceita a adição ou subtração de qualquer componente não original de fábrica para adequação do equipamento;

4.1.7.121 Apresentação de no mínimo um atestado emitido por pessoa jurídica de direito público ou privado, comprovando que a proponente fornece/forneceu bens compatíveis com os objetos da licitação, emitidos em papel timbrado, com assinatura, identificação e telefone do emitente.

4.1.8 SOFTWARE DE PROTEÇÃO E RECUPERAÇÃO DE DADOS

Definições Gerais

4.1.8.1 Poderão ser fornecidos mais de um produto a fim de que todas as funcionalidades sejam atendidas desde que tais softwares sejam do mesmo fabricante e estejam contidos no mesmo pacote de licenciamento.

4.1.8.2 Deve ser ofertada a versão mais atual do(s) software(s), liberada oficialmente pelo fabricante. Caso haja necessidade, por razões de compatibilidade com os demais componentes de hardware e software do ambiente de backup, a Contratante se reserva o direito de utilizar a versão do software imediatamente anterior à versão mais atual, sem nenhum ônus adicional para a CONTRATANTE;

4.1.8.3 Todas as funcionalidades descritas poderão ser implementadas de maneira isolada pelo software de backup ou pela integração com um appliance de deduplicação (ou de backup), desde que devidamente homologadas pelo fabricante do appliance. Neste certame deverá ser fornecido o appliance de deduplicação;

4.1.8.4 Deve implementar política de gerenciamento centralizada para múltiplos servidores de backup, mesmo que em diferentes plataformas, através de console única com interface gráfica;

4.1.8.5 O licenciamento do software deve ser por capacidade (tebibytes) ou por processador (socket), permitindo utilizar em quantidade ilimitada os agentes e módulos do software de backup, enquanto mantendo-se o limite da quantidade contratada;

4.1.8.6 Caso o licenciamento de software seja ofertado no modelo por processador (socket), deve ser considerada a quantidade de 18 processadores físicos (sockets) para os servidores que devem ter backup;

4.1.8.7 Caso o licenciamento de software seja ofertado no modelo de capacidade, deve ser considerado o volume de 80 TiB (Oitenta Tebibytes utilizando base 2) de dados medidos na origem que devem ter backup.

4.1.8.8 O licenciamento do software deverá ser fornecido no formato perpétuo ou por subscrição;

4.1.8.9 O servidor de backup poderá ser disponibilizado no formato de “vApp”, ou seja, uma Imagem de appliance virtual composto de sistema operacional otimizado e camada de software para deploy em Hypervisor Vmware;

4.1.8.10 Outra forma de disponibilização do servidor de backup pode ser através da instalação do software de backup em um servidor físico via bare metal. Neste certame deverá ser fornecido o servidor físico junto com o sistema operacional licenciado e compatível com o software de backup.

4.1.8.11 Só serão aceitos servidor e sistema operacional que possuam o mesmo nível de serviço solicitado para a solução de backup;

4.1.8.12 O licenciamento deve permitir em quantidade ilimitada, integrações com uma ampla variedade de aplicações, permitindo desta forma o backup consistente, atendendo a lista abaixo:

4.1.8.12.1 Linux, Windows;

4.1.8.12.2 Ambientes Virtuais;

4.1.8.12.3 Oracle;

4.1.8.12.4 SQL e Exchange;

4.1.8.12.5 Kubernetes;

4.1.8.13 Deve possuir interface gráfica baseada em HTML5 sem necessidade de plug-in Flash ou Java;

4.1.8.14 Deve possuir em sua interface gráfica a funcionalidade de agendamento de processos de backup segundo políticas a serem definidas (periodicidade, período de retenção, agendamento, tipo de backup);

4.1.8.15 Deve possuir um banco de dados ou catálogo interno, contendo informações sobre todos os arquivos e mídias onde os backups foram armazenados. Caso o software não utilize bancos de dados proprietário, a licença do mesmo deve ser fornecida pela Contratada, com os mesmos níveis de suporte exigidos neste termo;

4.1.8.16 Possibilitar a reconstrução parcial ou total do catálogo ou banco de dados no caso de perda do mesmo;

4.1.8.17 Deve gerar automaticamente cópia de segurança da própria base de catálogos e configuração;

4.1.8.18 Possuir ambiente de gerenciamento de backup e restore via interface gráfica;

4.1.8.19 Deve suportar backup via LAN e WAN;

4.1.8.20 Deve suportar múltiplas operações de backup e restore simultâneas;

4.1.8.21 Deve permitir o estabelecimento de níveis de serviços (SLA) para as políticas de proteção baseados nos objetivos de nível de serviços (SLO);

4.1.8.22 Deve possuir funcionalidade de gerenciamento dos prazos de retenção por políticas definidas centralmente;

4.1.8.23 Deve possuir a funcionalidade de recuperar dados para servidores diferentes do equipamento de origem;

4.1.8.24 Deve fazer uso do serviço de VSS (Volume Shadow Copy) para toda plataforma Microsoft que possua o serviço;

4.1.8.25 O software de backup deve possuir recurso que permita que o servidor cliente de backup envie os dados diretamente para um appliance de backup em disco, sem necessidade que este dado seja transferido para o servidor de mídia de backup;

4.1.8.26 Deve implementar diferentes perfis de usuários, ao menos administradores e usuários simples;

4.1.8.27 Aos diferentes perfis de usuários, deve ser permitido atribuir ou revogar diferentes níveis de privilégios, tais como:

4.1.8.28 Acesso a logs de auditoria, configuração de assets, gerenciamento de segurança, gerenciamento de armazenamento, para usuários com perfil de administradores;

4.1.8.29 Acesso a monitoração do ambiente, acesso a visualização de logs, acesso a execução de atividades de backup e restore, para o perfil de usuário simples.

4.1.8.30 Deve suportar LDAP para autenticação de usuários;

4.1.8.31 Possuir interfaces de gerenciamento/monitoração por Browser;

4.1.8.32 Deve possibilitar a criação de diferentes usuários com diferentes perfis de acesso (preferencialmente através de integração com AD);

4.1.8.33 Deve possuir detecção automática de comportamentos anômalos nos backups (ex: ransomware, alterações suspeitas em arquivos) para todos os workloads suportados, incluindo assets NAS.

- 4.1.8.34 Deve possuir funcionalidade para envio de alertas através de e-mail, Script ou via Windows Event Log;
- 4.1.8.35 Deve disponibilizar console Web para busca granular dos arquivos protegidos nos servidores.
- 4.1.8.36 A solução deverá permitir o controle do envio de dados de backup para armazenamento em nuvem a partir do appliance de backup;
- 4.1.8.37 Para cada socket ou TB de Front End licenciado, deve permitir o armazenamento de no mínimo 1TB de dados livres de compressão ou deduplicação em Virtual Appliance ou VM dedicada a fim de permitir maior segurança e segmentar os dados de backup dos dados de produção. Todo licenciamento de software de Sistema Operacional e qualquer software necessário para funcionando desse Virtual Appliance ou VM dedicada deve fazer parte da solução;
- 4.1.8.37.1 O Virtual Appliance ou o Appliance de Backup deverá estar licenciado e suportar nativamente enviar de forma deduplicada e criptografada os dados de backup para um armazenamento em nuvem pública ou privada utilizando-se de políticas internas de movimentação baseadas no tempo de acesso dos dados.
- 4.1.8.37.2 O Virtual Appliance, VM dedicada ou Appliance de Backup deve utilizar recursos de deduplicação inline e global através do uso de blocos variáveis dos dados para eliminar segmentos redundantes e compactar os dados, de forma a reduzir a capacidade de disco utilizada.

Monitoração e relatórios

- 4.1.8.38 Deve possuir serviço de monitoração e relatórios baseado em nuvem (SaaS), permitindo que qualquer usuário autorizado com acesso à internet possa, à partir de um portal, verificar as seguintes informações do ambiente via navegador suportado:
- 4.1.8.38.1 Status das políticas de backup;
 - 4.1.8.38.2 Sumário da proteção dos ativos;
 - 4.1.8.38.3 Lista das maiores violações de níveis de serviços estabelecidos para o backup;
 - 4.1.8.38.4 Lista de conformidade de ativos de acordo com os níveis de serviços estabelecidos;
 - 4.1.8.38.5 Alertas críticos das últimas 24 horas;
 - 4.1.8.38.6 Capacidade ocupada de sistemas de armazenamento do backup;
 - 4.1.8.38.7 Reportes de ativos protegidos, podendo ser exportado pelo menos no formato CSV;
 - 4.1.8.38.8 Reportes de conformidade da proteção dos ativos protegidos podendo ser exportado pelo menos no formato CSV;
 - 4.1.8.38.9 Possibilidade de aplicar filtros, incluir e excluir campos no relatório;

Proteção de file systems de hosts

- 4.1.8.39 O agente deve implementar deduplicação na origem dos dados;
- 4.1.8.40 Deve permitir o backup full e incremental;
- 4.1.8.41 Deve permitir execução de backups tipo full sintético, que permite a criação de uma única imagem de backup a partir de um backup full e qualquer quantidade de backup incrementais. O restore deverá ser efetuado a partir da nova imagem full sintética;
- 4.1.8.42 Deve permitir o backup e restore centralizado com datapath direto para o repositório de dados;
- 4.1.8.43 Deve permitir o restore no nível de arquivos para o host de origem ou hosts distintos;

4.1.8.44 Deve suportar filtros de exclusão de arquivos como data de criação, data de alteração, tamanho e caminho. Deve permitir o uso de operadores lógicos como “E” e “OU”;

Proteção de Ambientes VMWARE

4.1.8.45 Possuir suporte a backup e restore de máquinas virtuais VMWare com as seguintes características:

4.1.8.46 Deve possuir a capacidade de realizar backup das máquinas virtuais Windows e Linux.

4.1.8.47 Suportar o mecanismo de proteção para máquinas virtuais sendo totalmente integrado diretamente ao ESXi, atendendo as seguintes características:

4.1.8.47.1 Para execução do backup não deverá necessitar de VMs e/ou servidores físicos apartados para execução da função de proxies/agents/data movers/media server.

4.1.8.47.2 Não deverá utilizar área temporária do cluster vmware para armazenamento do snapshot das máquinas virtuais. O snapshot deverá ser armazenado diretamente no appliance.

4.1.8.48 Caso a proponente não possua tal característica, será facultado a integração com o VADP, desde que, a proponente inclua infraestrutura/servidor adicional necessário em sua proposta, para executar a função de “proxies /data movers/media server” incluindo todo hardware e licenciamento necessário para seu perfeito funcionamento. O servidor deverá atender com as seguintes características mínimas ou mais recursos a depender das boas práticas do fabricante:

4.1.8.48.1 Deverá possuir licenciamento VMWARE para permitir virtualização dos proxies. Caso necessite de sistema operacional, o mesmo deverá estar licenciado e com suporte do fabricante.

4.1.8.48.2 Deverá possuir no mínimo 2 (dois) processadores para servidores corporativos das famílias Intel Xeon ou AMD EPYC, de quarta geração ou superior, sendo que cada processador deverá ter no mínimo 16 núcleos de processamento e frequência mínima de 2,00GHz. O processador deverá estar em linha de produção pelo fabricante do processador e a época de lançamento deve ser igual ou superior ao primeiro quadrimestre de 2025, não sendo aceitos processadores descontinuados.

4.1.8.48.3 Deverá possuir no mínimo 256GB (duzentos e cinquenta e seis Gigabytes) de memória RAM DDR4 ou superior, com tecnologia de correção ECC (Error Correcting Code), provisionados por módulos de mesmo tamanho e na velocidade máxima suportada pelo processador. A memória RAM deverá ser fornecida pelo FABRICANTE do equipamento, devendo ser compatível e homologada para o processador e para o modelo de servidor físico. Os módulos deverão ser distribuídos de forma a proporcionar maior desempenho.

4.1.8.48.4 Deverá possuir 2 (dois) discos SSD de no mínimo 240GB, conectados a uma controladora RAID configurada em RAID-1.

4.1.8.48.5 Deverá possuir capacidade para pelo menos 4 (quatro) discos de 2,5 polegadas hot-swap e hot-pluggable, permitindo a troca de disco sem a necessidade de abrir o gabinete, e sem a necessidade de desligar o servidor.

4.1.8.48.6 Deverá possuir módulo de gerenciamento, com suporte a gerenciamento remoto da solução e suporte a IPMI-over-LAN.

4.1.8.48.7 Deverá possuir no mínimo 04 (quatro) portas 25GbE (Vinte e Cinco Gigabit Ethernet);

4.1.8.49 Deverá permitir a recuperação de máquinas virtuais através de plugin integrado ao VMWare.

4.1.8.50 Deverá possuir funcionalidade nativa para descoberta automática das máquinas virtuais VMWare conforme são criadas no ambiente virtual para que através de filtros possam ser incluídas nas políticas/rotinas de backup, sem a utilização de scripts e/ ou composições feitas exclusivamente para atendimento a esse item.

4.1.8.51 Possuir funcionalidade de replicação dos backups de máquinas virtuais VMWARE para um armazenamento em nuvem pública para fins de disaster recovery, sem a necessidade de aquisição de softwares de terceiros. O licenciamento desta funcionalidade deverá ser igual a capacidade total solicitada neste edital. A área de armazenamento em nuvem pública não faz parte deste certame.

5.1.8.52 Permitir integração nativa através de API com vRealize Automation

4.1.8.53 Possuir suporte a backup e restore de máquinas virtuais VMware 6.5 ou superior.

4.1.8.54 Deve permitir que através de uma única rotina de Backup seja possível recuperar a imagem completa da máquina virtual Windows e Linux (VMDK), somente o VMDK desejado de forma seletiva e os arquivos de maneira granular sem a necessidade de scripts, ou área temporária.

4.1.8.55 Deve suportar o uso da funcionalidade CBT (Change Block Tracking) para as operações de backup e restore.

4.1.8.56 Deve permitir a identificação de aplicações Microsoft SQL que residem nas máquinas virtuais, através de integração VADP, permitindo o backup, recuperação integral ou granular.

4.1.8.57 Deverá permitir o “instant recovery”, ou seja, iniciar de maneira imediata a execução de base de dados SQL virtualizadas, diretamente a partir do seu repositório de backup.

4.1.8.58 Deverá permitir o “instant recovery”, ou seja, iniciar múltiplas máquinas virtuais de maneira imediata, diretamente a partir do seu repositório de backup.

4.1.8.59 Deve permitir a recuperação granular de arquivos (FLR) a partir do backup da imagem completa (VMDK).

4.1.8.60 Deve possuir a capacidade de balanceamento de carga automático dos backups.

4.1.8.61 Deve permitir restaurar e iniciar de maneira imediata a execução de múltiplas máquinas virtuais instantaneamente, diretamente a partir do seu repositório de backup.

4.1.8.62 Deve possuir capacidade de realizar backup de maneira off-host, sem a necessidade de instalação de agentes nas máquinas virtuais.

4.1.8.63 Deve possuir a capacidade de recuperação da imagem da máquina virtual, para máquinas que possuam discos VMFS ou RDM.

4.1.8.64 A solução deve disponibilizar recurso de busca e indexação dos dados de backup copiados, de forma a buscar de forma granular os arquivos protegidos nos servidores utilizando apenas o nome do arquivo desejado.

Proteção em ambientes MICROSOFT HYPER-V

4.1.8.65 Deve suportar o backup e a recuperação de máquinas virtuais;

4.1.8.66 O backup das máquinas virtuais pode utilizar o agente instalado em cada host Hyper-V, mas deve permitir realizar os backups sem a instalação de agentes nas mesmas;

4.1.8.67 Deve possuir a compatibilidade tanto com ambientes standalone como cluster, incluindo CSV com SMB;

4.1.8.68 Deve permitir o backup consistente de VMs com suporte a Resilient Change Tracking (RCT);

4.1.8.69 Deve permitir a recuperação tanto de VMs inteiras como de arquivos individuais;

4.1.8.70 Deve permitir a descoberta e proteção automática de novas VMs baseado em regras;

4.1.8.71 Deve suportar o VHDX e o VHD.

Proteção em ambientes SQL Server

4.1.8.72 Deve fazer a descoberta automática das bases de dados contidas em um servidor;

4.1.8.73 O agente deve implementar deduplicação na origem dos dados e permitir múltiplos streams de backups;

4.1.8.74 Deve permitir o backup full e incremental;

4.1.8.75 Deve fazer uso de VDI;

4.1.8.76 Deve permitir a cópia consistente de bases de dados a partir do backup tipo Image da VM em ambientes Vmware;

4.1.8.77 Deve permitir o backup e restore centralizado consistente de bases de dados com datapath direto para o repositório de dados;

4.1.8.78 Deve permitir o backup e restore descentralizado a partir do host, também chamado de Self Service; mantendo a consistência de catálogo da aplicação de backup;

4.1.8.79 Deve permitir o restore no nível de database ou de tabelas;

4.1.8.80 Deverá proteger servidores Microsoft SQL Standalone e em Cluster;

Proteção em ambientes Oracle

4.1.8.81 Deve fazer a descoberta automática das bases de dados contidas em um servidor;

4.1.8.82 O agente deve implementar deduplicação na origem dos dados;

4.1.8.83 Deve permitir o backup full, incremental e logs;

4.1.8.84 Deve fazer uso do RMAN;

4.1.8.85 Deve permitir o backup e restore centralizado consistente de bases de dados com datapath direto para o repositório de dados;

4.1.8.86 Deve permitir o backup e restore descentralizado a partir do host, também chamado de Self Service; mantendo a consistência de catálogo da aplicação de backup;

4.1.8.87 Deve permitir o restore no nível de database ou de tabelas;

4.1.8.88 Deverá suportar Oracle RAC;

Proteção em ambientes Exchange

4.1.8.89 O agente deve implementar deduplicação na origem dos dados;

4.1.8.90 Deve fazer uso de BBB;

4.1.8.91 Deve permitir o backup e restore centralizado consistente com datapath direto para o repositório de dados;

4.1.8.92 Deve permitir o backup e restore descentralizado a partir do host, também chamado de self service; mantendo a consistência de catálogo da aplicação de backup;

4.1.8.93 Deve suportar implementações Standalone, DAG & IP-Less DAG;

Proteção de ambientes Kubernetes

4.1.8.94 Deve possuir integração nativa com Kubernetes no nível de namespaces e PVCs, não sendo aceitos scripts ou backups no nível de sistema de arquivos para atendimento a esse item;

4.1.8.95 Deve suportar volumes contidos em armazenamento tipo CSI-based;

4.1.8.96 Deve ser compatível com Container Storage Interface (CSI) driver;

4.1.8.97 Deve suportar o backup de volumes persistentes com modo de volume "Filesystem";

4.1.8.98 Utilizar recursos de deduplicação na origem, transferindo apenas os blocos únicos durante o processo de backup do Kubernetes.

4.1.8.99 Deve realizar o backup completo do Namespace e seus objetos como: Pods, Secrets, Services, Deployments, Replica set, Certificates, ConfigMaps e Persistent Volumes.

4.1.8.100 Deve ser possível a visualização dos diversos clusters Kubernetes e seus componentes protegidos a partir da console de gerenciamento de backup;

4.1.8.101 Serão aceitas composições com softwares de terceiros para prover as funcionalidades solicitadas, desde que o nível de suporte atenda ao solicitado desde que centralizado;

4.1.8.102 Deve ser capaz de realizar a descoberta automática de namespaces dentro de um cluster;

4.1.8.103 Deve realizar a descoberta automática dos containers e seus volumes persistentes configurados.

4.1.8.104 Possuir políticas de backup dinâmicas onde através de filtros e regras um novo Namespace pode ser protegido em uma determinada política de maneira automática, sem intervenção do administrador.

4.1.8.105 Permitir o restore do Namespace nos seguintes formatos:

4.1.8.105.1 Restore para o Namespace original;

4.1.8.105.2 Restore para um Namespace existente;

4.1.8.105.3 Restore para um novo Namespace;

4.1.8.105.4 Restore do Namespace em um outro cluster Kubernetes diferente da origem;

4.1.8.106 Deve permitir o backup e restore centralizado consistente com datapath direto para o repositório de dados;

4.1.8.107 Deve permitir o backup e restore descentralizado a partir do host, também chamado de self service; mantendo a consistência de catálogo da aplicação de backup;

4.1.8.108 Suportar diferentes distribuições de Kubernetes em ambientes VMWare, Red Hat OpenShift, Rancher, Google Anthos, Microsoft Azure Kubernetes Service (AKS), Google Kubernetes Engine (GKE) e Amazon Elastic Kubernetes Service (EKS)

Proteção de file systems do Appliance Scale-Out NAS.

4.1.8.109 Deve suportar o backup e restore dos filesystems (shares) NFS ou CIFS

4.1.8.110 Deve suportar o restore dos arquivos;

4.1.9 APPLIANCE DE PROTEÇÃO E RECUPERAÇÃO DE DADOS

4.1.9.1 Appliance de Proteção e Recuperação de Dados com deduplicação e compressão para instalação em rack de 19" (dezenove polegadas) onde deverão ser fornecidos os respectivos kits de fixação;

4.1.9.2 Deverá obrigatoriamente fazer uso de sistemas inteligentes de armazenamento de backup em disco, baseado em Appliance, que se entende como um subsistema com o propósito específico de entrada dos dados de backup, deduplicação e replicação;

4.1.9.3 O Appliance deverá ser composto, de processamento e armazenamento integrado, dedicado única e exclusivamente, à execução das atividades de entrada, deduplicação e replicação dos dados enviados pelos servidores de backup;

4.1.9.4 O hardware do Appliance não poderá ser compartilhado com nenhum outro software;

4.1.9.5 Não será permitido Appliance virtual.

4.1.9.6 O Sistema Operacional do equipamento deverá ser licenciado e nativo do produto. Não serão aceitas as modalidades OEM de sistemas operacionais de propósito geral, tal como Windows ou Unix/Linux;

4.1.9.7 O Appliance deve ser novo, sem uso e constar da linha de produção do fabricante, não sendo aceito gateways e/ ou composições feitas exclusivamente para atendimento ao presente edital;

4.1.9.8 A deduplicação deve segmentar os dados em blocos de tamanho variável ajustado automaticamente pelo algoritmo do Appliance;

4.1.9.9 A deduplicação deverá ser global considerando todos os dados armazenados no equipamento em sua total capacidade disponível, ou seja, deverá comparar e identificar dados duplicados provenientes de diferentes servidores e protocolos de acesso de forma a atingir melhores taxas de deduplicação, mesmo que estejam em partições lógicas ou físicas diferentes do mesmo subsistema. Será facultada a utilização de soluções que não fazem uso da deduplicação global, desde que a área líquida solicitada seja acrescida em 50% (cinquenta por cento) de forma a compensar a menor eficiência deste tipo de tecnologia.

4.1.9.10 Possuir tecnologia de deduplicação de dados em linha (inline), ou seja, os dados de backup são deduplicados em CPU e memória antes mesmo de sua gravação em disco. Não serão aceitas soluções que realizem a deduplicação após a gravação do dado no disco (pós-processo) ou mesmo híbridas que realizem parte do processo antes e parte após a gravação dos dados no disco.

4.1.9.11 A solução deve fazer uso de recursos dedicados para realizar a compressão dos dados via hardware após a deduplicação dos dados, de forma que este processo de compressão não deve impactar o desempenho do equipamento. Será facultada a utilização de soluções que não fazem uso de compressão após a deduplicação, desde que a área líquida solicitada seja acrescida em 50% (cinquenta por cento) de forma a compensar a menor eficiência deste tipo de tecnologia.

4.1.9.12 O sistema inteligente de armazenamento de backup em disco deve permitir realizar a replicação otimizada dos dados (off-host) sem onerar a CPU dos servidores de backup;

4.1.9.13 O sistema inteligente de armazenamento de backup em disco deve permitir replicar os dados através de rede IP de forma criptografada;

4.1.9.14 Deve suportar replicação 1 para N (1 origem e várias destinos), N para 1 (várias origens e 1 destino) e cascata;

4.1.9.15 O sistema inteligente de armazenamento de backup em disco deverá ser capaz de suportar falhas de até dois discos, devendo ser fornecido com proteção RAID-6 ou similar;

4.1.9.16 O sistema inteligente de armazenamento de backup deve ser fornecido com no mínimo um disco "Hot-Spare" para cada RAID group ou gaveta de discos;

4.1.9.17 O(s) disco(s) de "hot spare" devem ser utilizados de forma global dentro do Appliance;

4.1.9.18 Deverá possuir mecanismos que não permitam a inconsistência dos dados mesmo em casos de interrupção abrupta ou desligamento acidental, por meio de memória não volátil dedicada a operações de escrita ou recurso similar.

4.1.9.19 Deverá possuir interface de administração GUI e CLI;

4.1.9.20 A solução ofertada deve suportar a integração comprovada por matriz de compatibilidade com o software Oracle RMAN e estar inscrita na lista de fabricantes homologados pelo Oracle Backup Solutions Program (BSP) através do site (<https://www.oracle.com/technetwork/database/features/availability/bsp-088814.html>), permitindo que o backup e o restore do banco de dados Oracle possam ser feitos diretamente para o Appliance, sem utilização de software adicional de backup. Esta funcionalidade deve ser suportada inclusive para equipamentos do tipo Oracle Exadata.

4.1.9.21 A solução deverá suportar a criptografia dos dados deduplicados sem necessidade de equipamento adicional;

4.1.9.22 A solução deverá suportar regras de quotas de capacidade por volume, limitando a sua capacidade para backup sem necessidade de software ou equipamento adicional;

4.1.9.23 Permitir o particionamento lógico da área de armazenamento (Multi-Tenant), sem prejuízo das características de deduplicação solicitadas neste certame;

- 4.1.9.24 A controladora deve possuir no mínimo 2 processadores multi-core Intel ou AMD;
- 4.1.9.25 Deve possuir ao menos 256GB de memória RAM. Não serão aceitas como memória a utilização de tecnologias Flash, SSD ou qualquer outra tecnologia de extensão de memória cache;
- 4.1.9.26 A solução deve fazer uso de discos do tipo SSD (Solid State Drive) para aceleração dos dados. Será facultada a oferta do dobro (2x) de memória cache solicitada neste certame para as soluções que não fazem uso de discos Flash ou SSD para aceleração, de forma a compensar a menor eficiência deste tipo de equipamento.
- 4.1.9.27 Deverá disponibilizar no mínimo 96TB úteis de armazenamento líquido disponíveis para gravação, considerando base 10 como referência de cálculo de capacidade, descontadas todas as perdas com redundâncias, paridades, spares de proteção do arranjo de discos, deduplicação de dados e qualquer outro mecanismo de redução de dados.
- 4.1.9.28 Deve permitir a expansão da área de armazenamento em, no mínimo, 256TB úteis, em um único pool (área) de armazenamento e deve ser atingida somente com a adição de gavetas de disco sem prejuízo das demais características solicitadas;
- 4.1.9.29 Deverá suportar as seguintes interfaces de interconexão com os servidores de backup: interfaces Fibre Channel (FC) 32Gb, interfaces 10GbE e 25Gb Ethernet;
- 4.1.9.30 O equipamento deve estar licenciado para permitir acesso através de: CIFS, NFS, NDMP, VTL (Virtual Tape Library) e OST;
- 4.1.9.31 Deverá ser fornecido com no mínimo 08 portas Ethernet 10/25Gbps ótico padrão SFP+/SFP28;
- 4.1.9.32 Deverá possuir performance de ingestão de no mínimo 66TB/hora de dados transferidos;
- 4.1.9.33 Deve suportar no mínimo 270 jobs de gravação simultânea.
- 4.1.9.34 Deve ser compatível com os protocolos de rede IPv4 e IPv6;
- 4.1.9.35 Deverá ter suporte ao protocolo de monitoramento SNMP v2 e v3;
- 4.1.9.36 Deve possuir ventiladores e fontes redundantes possibilitando a substituição sem a necessidade de parada do sistema.
- 4.1.9.37 Cada fonte de alimentação deverá vir acompanhada de um cabo de alimentação C13/C14.
- 4.1.9.38 A solução deve possuir no próprio hardware do equipamento função de “call-home” ou email para notificar de forma automática quaisquer problemas para a central do fabricante.
- 4.1.9.39 Todos os serviços relacionados a instalação física e configuração do Appliance no ambiente da CONTRATANTE devem estar inclusos;
- 4.1.9.40 O equipamento deve suportar nativamente enviar de forma desduplicada e criptografada os dados de backup para um armazenamento em nuvem pública ou privada utilizando-se de políticas internas de movimentação baseadas no tempo de acesso dos dados. Esta funcionalidade deverá estar licenciada permitindo o uso do dobro de capacidade útil solicitada neste certame;
- 4.1.9.40.1 Devera suportar AWS (S3 Standard, S3 IA e Glacier), Azure (Cool e HotBlob) e Google Nearline storage;
- 4.1.9.41 Deverá possuir os seguintes recursos de integridade e segurança cibernética:
- 4.1.9.41.1 O processo de exclusão dos dados armazenados (data shredding) deve seguir os padrões de segurança estabelecidos no National Institute of Systems and Technology (NIST) SP800-88.
- 4.1.9.41.2 O equipamento deve fazer uso de API para permitir que os backups sejam acessados e enviados para o repositório de backup sem que o volume esteja montado no servidor de backup, eliminando qualquer risco de propagação Ransomware e acesso aos dados de backups armazenados.

4.1.9.41.3 A solução deverá possuir sistema de proteção interno utilizando snapshots internos que permitam melhorar a segurança dos dados e índices e permitir a recuperação para um momento anterior;

4.1.9.41.4 Deverá utilizar padrão de criptografia AES-256 para replicação dados em trânsito (in-flight) e em repouso (at-rest). Seguindo, no mínimo, as regras estabelecidas para o nível de segurança do padrão FIPS 140-2.

4.1.9.41.5 Deve possuir mecanismo inteligente que verifique continuamente de forma automática a integridade lógica dos dados, “ponteiros” e índices armazenados (fim-a-fim) no hardware com correção automática das falhas encontradas, de forma a garantir a consistência de todo o conteúdo em sua total capacidade, sem a utilização de scripts e/ ou composições feitas exclusivamente para atendimento a esse item.

4.1.9.41.6 Possuir recurso de dupla autenticação (2FA – Two Factor Authentication) para executar atividades administrativas de exclusão.

4.1.9.41.7 Deverá possuir recurso de imutabilidade de dados utilizando WORM (Write Once Read Many) de proteção contra alteração/regravação e exclusão dos dados armazenados, em conformidade com SEC 17a-4(f), permitindo somente uma única escrita e múltiplas leituras, garantindo integridade e autenticidade. A solução não deverá permitir que usuários, inclusive com privilégios de administrador, consigam alterar ou apagar dados protegidos, até que o tempo de retenção configurado tenha expirado.

4.1.9.41.8 O recurso de imutabilidade WORM (Write Once Read Many) deve incluir proteção ao controle de horário do subsistema (System Clock Hardening Protection), impedindo que se adiante a data ou horário do subsistema;

4.1.9.41.9 As rotinas internas de manutenção dos dados de backup armazenados tais como: Processo de limpeza (Garbage Collector ou housekeeping) e Validação de integridade (data integrity), devem ser executados em paralelo com as rotinas de backup e recuperação, ou seja, a solução ofertada não deve exigir parada ou interrupção (blackout window) das atividades de backup/restore para tarefas internas do equipamento.

4.1.9.41.10 Deverá bloquear a conta por no mínimo 15 minutos após três tentativas de login incorretas

4.1.9.41.11 Deverá desabilitar o login root para SSH

4.1.9.41.12 Deverá permitir a implementação da função de segurança RBAC;

4.2 CONDIÇÕES DE ENTREGA, GARANTIA, MANUTENÇÃO E ASSISTÊNCIA TÉCNICA

Condições de Entrega dos Bens

4.2.1. A entrega dos bens deverá ocorrer em conformidade com as especificações técnicas estabelecidas neste Termo de Referência, no local indicado pela CONTRATANTE, devidamente acondicionados, lacrados e acompanhados da documentação técnica pertinente.

4.2.2. Os equipamentos deverão ser novos, de primeiro uso, e fornecidos em linha de produção ativa do fabricante, não sendo admitidos produtos descontinuados, reconicionados ou fora de linha.

4.2.3. A CONTRATADA deverá realizar, quando aplicável:

- I – transporte, seguro e descarregamento dos equipamentos;
- II – instalação física e lógica dos equipamentos no ambiente da CONTRATANTE;
- III – integração com a infraestrutura existente;
- IV – testes operacionais iniciais para validação do funcionamento.

4.2.4. O recebimento ocorrerá conforme a demanda do órgão de acordo com fase de implantação do Data Center, ocorrerá em duas etapas:

- I – Recebimento Provisório, para verificação quantitativa e inicial;

II – Recebimento Definitivo, após validação técnica e funcional, atestando conformidade com os requisitos estabelecidos e o funcionamento da Solução TIC.

Condições de Garantia

4.2.5. Os bens deverão possuir garantia contratual mínima de 60 (sessenta) meses, ou superior, quando ofertada pelo fabricante, contada a partir do primeiro dia útil subsequente ao recebimento definitivo.

4.2.6. A garantia deverá contemplar, no mínimo:

- I – substituição de peças defeituosas;
- II – mão de obra especializada;
- III – atualização de firmware e software embarcado, quando aplicável;
- IV – suporte técnico remoto e/ou presencial.

4.2.7. A garantia deverá ser prestada pelo fabricante ou por rede autorizada, com cobertura integral para todos os componentes da solução.

4.2.8. Durante o período de garantia, não poderá haver qualquer ônus adicional para a CONTRATANTE.

Manutenção

4.2.9. A CONTRATADA deverá assegurar a manutenção corretiva dos equipamentos durante todo o período de garantia.

4.2.10. A manutenção corretiva compreende:

- I – diagnóstico de falhas;
- II – reparo ou substituição de componentes;
- III – restauração plena da capacidade operacional dos equipamentos.

4.2.11. Quando aplicável, deverá ser assegurada também a manutenção preventiva, conforme recomendações do fabricante.

Assistência Técnica

4.2.12. A CONTRATADA deverá disponibilizar serviço de assistência técnica com as seguintes características mínimas:

- I – Central de atendimento (Service Desk) disponível em horário comercial ou regime 24x7, conforme criticidade da solução;
- II – canais de atendimento eletrônico e telefônico;
- III – registro, acompanhamento e rastreabilidade de chamados técnicos.

4.2.13. Os níveis de serviço (SLA) deverão observar, no mínimo:

- I – prazo máximo para início de atendimento: até 2 horas após abertura do chamado;
- II – prazo máximo para solução: até 12 horas ou 1 dia, conforme criticidade;
- III – substituição temporária de equipamento (backup), quando necessário à continuidade do serviço.

4.2.14. A assistência técnica deverá ser prestada por profissionais qualificados e certificados, quando exigido pelo fabricante.

4.2.15. Obrigações Adicionais da Contratada

4.2.15.1 A CONTRATADA deverá:

- I – garantir disponibilidade de peças de reposição durante todo o período de garantia;
- II – manter base de suporte técnico ativa no território nacional;
- III – fornecer documentação técnica completa dos equipamentos; comunicar previamente eventuais descontinuações tecnológicas.

4.3. PROCEDIMENTOS DE TESTES, INSPEÇÃO E ACEITAÇÃO DO OBJETO

Diretrizes Gerais

4.3.1. Os procedimentos de testes e inspeção têm por finalidade verificar a conformidade dos bens e serviços entregues com os requisitos técnicos, funcionais e de qualidade estabelecidos neste Termo de Referência, em consonância com a Instrução Normativa SGD/ME nº 94, de 23 de dezembro de 2022.

4.3.2. Os testes deverão observar critérios objetivos, mensuráveis e rastreáveis, assegurando transparência, controle e adequada evidência documental para fins de aceitação do objeto.

4.3.3. A CONTRATANTE poderá realizar testes em todos os itens fornecidos ou por amostragem, conforme critérios técnicos, devendo registrar formalmente os resultados obtidos.

Inspeção no Recebimento Provisório

4.3.4. No ato da entrega, será realizado o recebimento provisório, com verificação preliminar dos bens, contemplando:

- I – conferência quantitativa dos itens entregues;
- II – verificação da integridade física dos equipamentos;
- III – conferência de marca, modelo e especificações técnicas;
- IV – verificação da documentação técnica e licenças;
- V – conferência de acessórios e componentes obrigatórios.

4.3.5. Serão recusados, total ou parcialmente, os bens que apresentem:

- I – sinais de uso, avarias ou inconformidades físicas;
- II – divergência em relação às especificações técnicas;
- III – ausência de componentes essenciais.

Testes Técnicos e Funcionais

4.3.6. Após o recebimento provisório, será realizada a etapa de testes técnicos e funcionais, com vistas à validação dos bens entregues e ao fim da implantação a validação completa da solução.

4.3.7. Os testes deverão contemplar, no mínimo:

- I – verificação de inicialização e operação dos equipamentos;
- II – validação de desempenho conforme especificações;
- III – testes de integração com o ambiente da CONTRATANTE;
- IV – verificação de compatibilidade entre componentes;

V – testes de conectividade e comunicação de rede;

VI – validação de versões de firmware e software;

VII – testes de funcionamento sob carga, quando aplicável.

4.3.8. A CONTRATADA deverá prestar suporte técnico à execução dos testes, fornecendo documentação, orientações e, quando necessário, equipe especializada em toda as fases de implantação da solução.

4.3.9. Todos os testes deverão ser formalmente documentados, contendo:

I – identificação do item testado;

II – descrição do procedimento realizado;

III – resultado obtido;

IV – evidências técnicas (logs, relatórios ou registros).

Critérios de Aceitação e Recebimento Definitivo

4.3.10. O aceite do objeto estará condicionado ao atendimento integral das especificações e requisitos estabelecidos neste Termo de Referência.

4.3.11. O recebimento definitivo da Solução de TIC somente será realizado após a conclusão integral da implantação do projeto e a comprovação de que todos os seus componentes encontram-se instalados, integrados e em pleno funcionamento, observados os requisitos estabelecidos neste Termo de Referência.

4.3.12. As entregas parciais de equipamentos realizadas durante a execução contratual poderão ser objeto de recebimento provisório, para fins de conferência quantitativa e qualitativa, sem que isso caracterize o recebimento definitivo da Solução de TIC.

4.3.13. O recebimento definitivo somente será realizado após:

I – a conclusão satisfatória dos testes integrados da solução;

II – a validação técnica da implantação;

III – a comprovação de conformidade com todos os requisitos funcionais, técnicos e operacionais estabelecidos;

IV – a comprovação de que a Solução de TIC está operacional em ambiente de produção, com todos os equipamentos, softwares, licenças, configurações, integrações e funcionalidades previstos no escopo contratual devidamente implantados e funcionando de forma integrada.

4.3.14. A CONTRATANTE poderá rejeitar, total ou parcialmente, o objeto que:

I – apresente desempenho inferior ao especificado;

II – esteja em desacordo com as exigências técnicas;

III – não atenda aos critérios de qualidade definidos.

4.3.15. Em caso de rejeição:

I – a CONTRATADA deverá promover a substituição ou correção no prazo estabelecido;

II – não haverá ônus adicional para a Administração;

III – poderão ser aplicadas sanções contratuais, conforme previsto no instrumento convocatório.

4.3.16. O recebimento definitivo será formalizado mediante ateste da conformidade técnica e funcional do objeto, após a conclusão dos testes e validações.

4.3.17. O recebimento definitivo não exclui a responsabilidade da CONTRATADA por vícios ocultos ou defeitos identificados posteriormente.

Registro e Rastreabilidade

4.3.18. Todos os procedimentos de testes e inspeção deverão ser registrados e mantidos como evidência da execução contratual.

4.3.19. O fiscal técnico deverá registrar ocorrências, inconformidades e providências adotadas, assegurando rastreabilidade e transparência.

4.4. MODELO DE EXECUÇÃO DO OBJETO E REGIME DE FORNECIMENTO

Regime de Fornecimento

4.4.1. O objeto da presente contratação será executado sob o regime de fornecimento de bens de Tecnologia da Informação e Comunicação (TIC), compreendendo a disponibilização de infraestrutura tecnológica, bem como a sua instalação, bem como garantia técnica ao longo da vigência contratual.

4.4.2. O fornecimento dos bens ocorrerá de forma parcelado de acordo com o projeto de implantação, mediante emissão de Ordem de Fornecimento de Bens (OFB) pela CONTRATANTE.

Caracterização do Modelo de Execução

4.4.3 A solução a ser contratada possui natureza integrada e híbrida, contemplando:

- I – fornecimento de ativos de infraestrutura de TIC;
- II – prestação de serviços de instalação;
- III – prestação dos serviços de garantia e manutenção da solução;

4.4.4. A execução contratual abrange não apenas a entrega dos bens, mas a sua plena operacionalização em ambiente produtivo, incluindo atividades necessárias à manutenção do desempenho, disponibilidade da solução.

Justificativa Técnica do Regime Adotado

4.4.5. A adoção do regime de fornecimento associado à prestação de garantia e manutenção justifica-se tecnicamente em razão das seguintes circunstâncias do objeto:

- I – a solução contempla infraestrutura crítica de TIC, destinada a suportar sistemas institucionais essenciais, exigindo alta disponibilidade e operação contínua;
- II – há necessidade de manutenção permanente (corretiva, preventiva e evolutiva) para garantir a continuidade e o desempenho dos serviços;
- III – a operação da solução demanda suporte técnico especializado e gestão integrada, não sendo tecnicamente viável dissociar o fornecimento dos equipamentos dos serviços associados;
- IV – o modelo assegura padronização tecnológica, estabilidade operacional e mitigação de riscos de indisponibilidade;
- V – a solução possui ciclo de vida tecnológico de médio e longo prazo, exigindo acompanhamento contínuo para preservação de sua eficiência;
- VI – a contratação integrada promove ganhos de eficiência administrativa e economicidade, evitando a fragmentação contratual e reduzindo custos indiretos.

Fundamentação Normativa

4.4.6 O regime adotado está em conformidade com a Instrução Normativa SGD/ME nº 94, de 23 de dezembro de 2022, especialmente no que se refere:

- I – à definição de modelo de execução compatível com as características da solução de TIC;
- II – à necessidade de estabelecimento de requisitos técnicos necessários e suficientes;
- III – à gestão de riscos e à garantia da continuidade dos serviços;
- IV – à busca da solução mais vantajosa para a Administração ao longo do ciclo de vida do objeto.

Vantagens do Modelo Adotado

4.4.7 O modelo de fornecimento associado à prestação de serviços de garantia e manutenção:

- I – continuidade operacional de sistemas críticos;
- II – redução de riscos de falhas e indisponibilidade;
- III – previsibilidade e melhor gestão dos custos;
- IV – maior controle e governança sobre a infraestrutura de TIC;
- V – alinhamento com boas práticas de contratação de soluções tecnológicas integradas.

4.5 REQUISITOS DE INSTALAÇÃO E IMPLEMENTAÇÃO DOS PRODUTOS

4.5.1 A CONTRATADA deverá instalar e configurar a solução a ser fornecida com as seguintes atividades:

Planejamento

4.5.2 Deverá ser designado pela CONTRATADA um Gerente de Projeto remoto que vai conduzir o projeto ao longo do processo de implantação - que irá acompanhar o processo de entrega dos equipamentos ao local de instalação, em conjunto com o CONTRATANTE irá validar que o local está de acordo com as premissas para a implantação, atuará no planejamento, implantação, pós-implantação e transição ao processo de suporte.

4.5.3 Deverá ser discutido e elaborado, juntamente com equipe técnica do CONTRATANTE, um planejamento de todo o processo de instalação e configuração dos equipamentos. Neste planejamento deverão constar, pelo menos, um cronograma com as definições de datas e prazos para as atividades relacionadas à instalação e configuração dos equipamentos e uma matriz de responsabilidades para todas as equipes participantes do processo.

4.5.4 Deverão ser analisados os requisitos de disponibilidade técnica e de ambiente do local;

4.5.5 Deverão ser confirmadas as datas de análise de preparação e instalação, destacando as dependências da preparação completa do local pelo CONTRATANTE (incluindo circuitos elétricos e conectores das PDUs), realizada pelo próprio, e das datas de envio do produto para cumprir o cronograma de instalação planejado;

4.5.6 A CONTRATANTE deve fornecer um contato para permitir que os prazos e processos sejam concluídos dentro do cronograma.

4.5.7 A CONTRATADA deve realizar a programação de uma janela de suspensão temporária, no caso de upgrade off-line do hardware, juntamente com a CONTRATANTE.

Instalação e Configuração física

4.5.8 A instalação física deverá ser realizada pelo próprio FABRICANTE ou por empresa certificada pelo Fabricante dos equipamentos;

4.5.9 Realizar a Instalação do equipamento e Montagem do hardware relacionado (como trilhos, suportes e bandeja) no rack;

4.5.10 Montar o(s) equipamento(s) no rack; Instalar no rack as PDU(s), conforme for necessário para obter a configuração apropriada de energia do equipamento - Instalar e fazer o cabeamento de alimentação dos equipamentos;

4.5.11 Deverá conectar e identificar os cabos fornecidos para o Produto, sendo de responsabilidade do CONTRATANTE o fornecimento de etiquetas ou anilhas para a correta identificação;

4.5.12 Deverá efetuar a ligação do equipamento, fazer o boot inicial do sistema e verificar se há indicadores visíveis de falhas;

4.5.13 Realizará as devidas atualizações de drivers, firmware e BIOS, incluindo firmware de chassi, se aplicável de acordo com matriz elaborada para assegurar a compatibilidade adequada com ambiente da CONTRATANTE;

4.5.14 Deverá instalar e inicializar os módulos de gerenciamento do equipamento (CMC, IDRAC ou IKVM).

4.5.15 Deverá realizar a configuração de RAID de acordo com o planejamento realizado;

4.5.16 Deverá realizar a integração com os Switches Ethernet/SAN;

Instalação e Configuração do software de sistema

4.5.17 A configuração lógica do ambiente deverá ser realizada de forma presencial (on site);

4.5.18 Realizar as configurações do equipamento (topologia física, níveis de firmware, endereços IP, execução de diagnóstico)

4.5.19 Instalação, configuração e atualização para a última versão de software disponível do fabricante e de acordo com a matriz de Compatibilidade do Sistema Operacional dos Switches fornecidos para a solução;

4.5.20 Instalar e configurar o sistema operacional ou hipervisor.

4.5.21 Instalar e configurar software de gerenciamento.

4.5.22 Durante a implementação da solução, a CONTRATADA deverá realizar breve orientação sobre o produto e análise da documentação associada em todas as fases de implantação.

Teste, Validação do sistema e Suporte pós-implantação

4.5.23 Realizar a captura do status do equipamento no sistema e emitir um relatório de configuração.

4.5.24 Realizar testes dos componentes do servidor para validação da conectividade com a rede da CONTRATANTE (atribuição de endereço IP).

4.5.25 Executar testes de verificação básicos (ping, traceroute, exibir comandos).

4.5.26 Realizar teste de capacidade básica de failover da solução quando aplicável.

4.5.27 Validar a configuração com o design da solução.

4.5.28 Entregar documentação da implantação executada para a CONTRATANTE contendo, entre outras informações, as seguintes: Etiqueta(s) de serviço, BIOS, revisão do firmware de módulo e componente. A documentação deve ser entregue a CONTRATANTE em PDF ou Word. Obter a confirmação da CONTRATANTE quanto aos Serviços Executados.

4.5.29 Realizar assistência de configuração pelo período de até 30 dias após a implantação de cada ambiente e após a implantação de toda a solução.

4.6 GARANTIA E SUPORTE DOS PRODUTOS

Todos os produtos fornecidos pela Contratada deverão atender aos seguintes requisitos de garantia e suporte técnico:

Requisitos de manutenção

4.6.1 Os serviços de manutenção e garantia serão prestados de acordo com o item “GARANTIA E MANUTENÇÃO”, sendo que:

4.6.1.1 A CONTRATADA poderá efetuar um número ilimitado de chamados técnicos, durante o período da garantia, para correção de problemas relativos ao uso e aplicações dos equipamentos, software e suas funcionalidades.

4.6.1.2 A CONTRATADA deverá apresentar declaração de garantia, ofertada pelo fabricante dos equipamentos, de no mínimo 60

(sessenta) meses, contados a partir do primeiro dia útil após o aceite definitivo dos equipamentos

4.6.1.3 A declaração de garantia deverá conter no mínimo: número(s) de série e descrição dos equipamentos fornecidos, número de contrato, telefone e endereço do(s) responsáveis pela prestação dos serviços de garantia, manutenção e suporte técnico, condições de garantia e outras informações necessárias.

4.6.1.4 Durante o período de garantia o Fabricante se compromete a executar correções visando eliminar erros detectados nos produtos que impeçam seu pleno funcionamento de acordo com as especificações listadas neste documento.

4.6.1.5 A CONTRATADA deverá apresentar o certificado de garantia ou declaração emitida pelo fabricante dos equipamentos, no prazo de até 3 (três) dias corridos, a contar da entrega do equipamento (termo de recebimento provisório).

4.6.1.6 Os equipamentos deverão ser garantidos no Brasil, sem itens restritivos, tanto para o hardware como para o software.

4.6.1.7 Os atendimentos deverão ser prestados pelo próprio Fabricante ou por técnicos credenciados pelo fabricante para executar as atividades, devendo este ser demonstrado mediante documento de comprovação (declaração do fabricante).

4.6.1.8 Os serviços deverão ser executados sem impacto na utilização do ambiente de TI do CONTRATANTE, de forma que os subsistemas mais críticos deverão ser executados em horário noturno e/ou finais de semana.

4.6.1.9 Caso a CONTRATADA identifique a necessidade de substituição de equipamentos que apresentem defeitos ou falhas, os mesmos deverão ser substituídos por produtos de qualidade e características técnicas iguais ou superiores aos existentes, desde que compatíveis, com todas as configurações necessárias ao seu funcionamento

4.6.1.10 O Fabricante da solução irá fornecer as últimas versões dos softwares utilizados pelos equipamentos, contendo correções de bugs, atualizações ou novas funcionalidades suportadas pelo equipamento em questão, bem como as respectivas licenças de uso.

4.6.1.11 O Fabricante da solução deverá fornecer drivers e firmwares, incluindo atualizações de versões e pequenas atualizações de release e reparos de defeitos (bug fixing patches) por 60 (Sessenta) meses.

4.6.12. Para atendimento aos serviços em garantia aos produtos instalados, a contratada deverá oferecer atendimento através de Centro de Suporte Técnico do FABRICANTE da solução ofertada.

4.6.13 O Suporte Técnico deverá ser realizado no regime de 24 horas por dia, 7 dias por semana (24x7x365);

4.6.14 O Suporte Técnico deverá ser prestado na modalidade on-site quando for necessário realizar a substituição de peças defeituosas, na Sede do CONTRATANTE. O início do atendimento se dará a partir da comunicação do(s) defeitos (s) pelo CONTRATANTE, via serviço telefônico (0800) ou outro meio indicado pela contratada.

4.6.15 Os serviços de suporte técnico a hardware/software deverão incluir, dentre outros:

4.6.15.1 Orientações sobre uso, configuração e instalação do software ofertado;

4.6.15.2 Questões sobre compatibilidade e interoperabilidade do produto ofertado (hardware e software);

4.6.15.3 Interpretação da documentação do software ofertado;

4.6.15.4 Orientações para identificar a causa de uma falha de software;

4.6.15.5 Orientação quanto às melhores práticas para implementação do software adquirido;

4.6.15.6 Apoio na recuperação de ambientes em caso de panes ou perda de dados;

4.6.16 Apoio para execução de procedimentos de atualização para novas versões do software instalado.

Garantia e Manutenção

4.6.17 A solução como um todo deve ser ofertada em conjunto com tecnologias e ferramentas que permitam o monitoramento e diagnóstico remoto do ambiente em regime 24 (vinte e quatro) horas por dia, 07 (sete) dias por semana;

4.6.18 Os equipamentos deverão possuir, no mínimo, 60 (sessenta) meses de garantia e suporte técnico, prestados em regime 24 (vinte e quatro) horas por dia, 07 (sete) dias por semana com tempo de reparo do problema ou solução de contorno a partir de 04 (quatro) horas corridas após o atendimento inicial para os casos de alta criticidade;

4.6.19 Diagnóstico e suporte de problemas por telefone ou remoto via internet com suporte na língua nativa do instrumento contratual. Caso não seja possível resolver o problema remotamente, o serviço deverá ser prestado localmente (on-site).

4.6.20 O suporte deve ser provido pelo fabricante do produto em níveis de serviços reativos, como reparo do equipamento e substituição de peças no local (on-site) e níveis de serviços proativos, a fim de identificar e solucionar problemas de configuração, disponibilidade e segurança antes que a operação seja impactada;

4.6.21 O fabricante deverá fornecer relatórios de incidentes, regularmente, para ajudar a identificar tendências de problemas e evitar recorrências;

4.6.22 Durante o tempo de vigência dos serviços de garantia e suporte técnico do fabricante, os custos de deslocamento, troca de peças danificadas entre outros custos são de responsabilidade do fabricante, não gerando ônus ao CONTRATANTE;

Gerente de Suporte

4.6.23 O papel de Gerente do suporte, devidamente qualificado, deve estar disponível pelo menos no período entre 9 e 17h;

4.6.24 Coordenar a entrega de eventos de manutenção dos equipamentos de acordo com a janela de manutenção da CONTRATANTE;

4.6.25 Fornecimento de relatórios mensais com o resumo dos chamados abertos e fechados no mês; análise das versões dos firmwares instalados e em caso de estarem defasados, coordenar a atualização;

4.6.26 Deve possuir interlocução direta com o fabricante do hardware e do software utilizado pela CONTRATADA;

4.6.27 Deve possuir autorização para abrir chamado diretamente com o fabricante;

4.6.28 Deve possuir acesso direto ao sistema de chamados do fabricante para acompanhamento e escalonamento de prioridade

4.6.29 Deve possuir acesso ao sistema do fabricante para informar possíveis bugs e solicitação de novas funcionalidades (feature request)

4.6.30 Deve possuir interlocução direta com os engenheiros de backoffice do fabricante, para escalonamento e acompanhamento de chamados

4.6.31 Gerenciar atendimento de segundo nível para quando os problemas não forem resolvidos através do atendimento inicial;

4.6.32 Gerenciar situação crítica atuando como ponto de contato único para a comunicação relacionada a resolução de problemas;

Atividades de Garantia Preventiva e Corretiva de Software

- 4.6.33 Suporte preventivo e corretivo de programas específicos e sistemas operacionais incluindo diagnóstico e resolução de problemas, liberação de correções, novas versões e releases de software, orientações para instalações, configurações e esclarecimentos de dúvidas, entre outros.
- 4.6.34 Deverão ser fornecidas, sem ônus adicional, todas as atualizações, upgrades e correções de software durante o período de garantia e manutenção dos produtos.
- 4.6.35 Diagnóstico e suporte de problemas por telefone ou remoto via internet. Caso não seja possível resolver o problema remotamente, o serviço deverá ser prestado localmente (on-site).

Garantia de Qualidade e nível de Prestação da garantia

- 4.6.36 Caberá à CONTRATADA a responsabilidade de manter todos os itens objeto deste contrato com alta confiabilidade e disponibilidade, garantindo as atividades operacionais e administrativas com os seguintes critérios de qualidade e nível de serviço:
- 4.6.36.1 A tabela 1 abaixo resume os critérios para a manutenção preventiva e corretiva e de suporte de software descritos no item anterior:

Severidade	Prazo (Início do Atendimento)	Comunicação (Situação corrente e próximos passos)	Prazo para Reparos (Contorno ou definitiva)
Severidade 1: Crítica - Problema grave que impeça a utilização de um sistema como um todo ou parcialmente.	30 min. (24x7)	Em sequência, sem interrupção, a cada 1 (uma) hora, até que seja atingida uma solução definitiva.	Para eventos de Hardware: Em até 6 (seis) horas após a chegada do técnico ao site. O despacho do técnico a contar da data da constatação do erro de hardware não deverá exceder 2 (duas) horas de diagnóstico após o registro do evento por qualquer meio de aviso de incidente, alertas dos equipamentos ou constatação das equipes operacionais. Para eventos de Software: Em até 8 (oito) horas para problemas identificados na base de conhecimento e problemas do fabricante, com solução disponível, a contar do momento de constatação do erro de software que não deverá exceder 4 (quatro) horas de diagnóstico após o registro do evento por qualquer meio de aviso, seja um incidente, alertas do próprio equipamento ou constatação das equipes operacionais.
Severidade 2: Problema de alto impacto que prejudique seriamente a utilização dos sistemas sem, no entanto, impedir a	2 horas (24x7)	Em pausas, a cada 4 (quatro) horas, até que seja atingida uma solução	Para eventos de Hardware: Em até 8 (oito) horas após a chegada do técnico ao site. O despacho do técnico a contar da data da constatação do erro de hardware não deverá exceder 4 (quatro) horas de diagnóstico após o registro do evento por qualquer meio de aviso de incidente, alertas dos equipamentos ou constatação das equipes operacionais. Para eventos de Software: Em até 10 (dez) horas para problemas

realização de atividades essenciais do mesmo.		definitiva ou de contorno.	identificados na base de conhecimento e problemas do fabricante, com solução disponível, a contar do momento de constatação do erro de software que não deverá exceder 6 (seis) horas de diagnóstico após o registro do evento por qualquer meio de aviso, seja um incidente, alertas do próprio equipamento ou constatação das equipes operacionais.
Severidade 3: Problema de impacto médio que não impeça a realização de atividades essenciais dos sistemas.	3 horas (Horário comercial)	Em pausas, a cada 8 (oito) horas, até que seja atingida uma solução definitiva ou de contorno.	<p>Para eventos de Hardware: Em até 8 (oito) horas após a chegada do técnico ao site. O despacho do técnico a contar da data da constatação do erro de hardware não deverá exceder 48 (quarenta e oito) horas de diagnóstico após o registro do evento por qualquer meio de aviso de incidente, alertas dos equipamentos ou constatação das equipes operacionais.</p> <p>Para eventos de Software: Em até 90 (noventa) dias para problemas identificados na base de conhecimento e problemas do fabricante, com solução disponível, a contar do momento de constatação do erro de software que não deverá exceder 7 (sete) dias de diagnóstico após o registro do evento por qualquer meio de aviso, seja um incidente, alertas do próprio equipamento ou constatação das equipes operacionais</p>
<p>Severidade 4: Pouco ou nenhum impacto na utilização dos sistemas.</p> <p>Tipicamente, dúvidas de utilização, requisições de melhorias, solicitação de upgrades etc.</p>	8 horas (Horário comercial)	Em pausas, diariamente, até que seja atingida uma solução definitiva ou de contorno.	<p>Para eventos de Hardware: Em até 8 (oito) horas após a chegada do técnico ao site. O despacho do técnico a contar da data da constatação do erro de hardware não deverá exceder 5 (cinco) dias de diagnóstico após o registro do evento por qualquer meio de aviso de incidente, alertas dos equipamentos ou constatação das equipes operacionais.</p> <p>Para eventos de Software: Em até 150 (cento e cinquenta) dias para problemas identificados na base de conhecimento e problemas do fabricante, com solução disponível, a contar do momento de constatação do erro de software que não deverá exceder 15 (quinze) dias de diagnóstico após o registro do evento por qualquer meio de aviso, seja um incidente, alertas do próprio equipamento ou constatação das equipes operacionais.</p>

Requisito De Operação e Manutenção da Solução

4.6.37 Devido às características da solução, há necessidade de realização de manutenções (corretivas/preventivas/adaptativa/evolutiva) pela Contratada, baseando-se na GARANTIA e SUPORTE, visando à operação e disponibilidade da solução;

Requisitos de Capacitação

4.6.38 Não faz parte do escopo da contratação a realização de capacitação técnica na utilização dos recursos relacionados ao objeto da presente contratação;

4.6.39 Deverá ser realizada uma breve sessão de orientação sobre o produto e análise da documentação associada. Essa visão geral não visa substituir nenhum curso de treinamento oficial disponível para este produto.

4.6.40 Entregar documentação da implantação conforme executada. Essa documentação deve especificar os serviços realizados incluindo:

etiqueta(s) de serviço; BIOS, revisão do firmware de módulos e componentes;

4.6.41 Entregar documentação em PDF ou Word especificando os serviços realizados e assim receber o aceite da Contratante;

Requisitos Legais

4.6.42 O presente processo de contratação deve estar aderente à Constituição Federal, à Lei nº 14.133/2021, Instrução Normativa SEGES /ME nº 65, de 7 de julho de 2021, Lei nº 13.709, de 14 de agosto de 2018 (Lei Geral de Proteção de Dados Pessoais – LGPD) e a outras legislações aplicáveis;

4.6.43 Decreto Nº 7.174, de 12 de maio de 2010 - Regulamenta a contratação de bens e serviços de informática e automação pela administração pública federal, direta ou indireta, pelas fundações instituídas ou mantidas pelo Poder Público e pelas demais organizações sob o controle direto ou indireto da União;

4.6.44 Decreto nº 7.845, de 14 de novembro de 2012 – regulamenta procedimentos para credenciamento de segurança e tratamento de informação classificada em qualquer grau de sigilo, e dispõe sobre o Núcleo de Segurança e Credenciamento;

4.6.45 Lei Nº 11.077, de 30 de dezembro de 2004 - Altera a Lei no 8.248, de 23 de outubro de 1991, a Lei no 8.387, de 30 de dezembro de 1991, e a Lei no 10.176, de 11 de janeiro de 2001, dispondo sobre a capacitação e competitividade do setor de informática e automação e dá outras providências;

4.6.46 A solução a ser contratada também deverá estar alinhada às normas de segurança ABNT 27001 e 27002, bem como às diretrizes do INC em relação ao uso de recursos de Tecnologia da Informação.

4.6.47 Instrução Normativa nº 94/2022, da Secretaria de Governo Digital do Ministério Economia - Dispõe sobre o processo de contratação de soluções de Tecnologia da Informação e Comunicação - TIC pelos órgãos e entidades integrantes do Sistema de Administração dos Recursos de Tecnologia da Informação - SISP, do Poder Executivo Federal;

4.6.48 Instrução Normativa SEGES/ME Nº 98/2022, que estabelece regras e diretrizes para o procedimento de contratação de serviços sob o regime de execução indireta de que dispõe a Lei nº 14.133, de 1º de abril de 2021, no âmbito da Administração Pública federal direta, autárquica e fundacional;

4.6.49 Lei 12.846/2013-Lei anticorrupção;

4.6.50 Decreto nº 11.878, de 9 de janeiro de 2024 (Normas para o funcionamento do Sistema de Cadastramento Unificado de Fornecedores - SICAF);

4.6.51 Instrução Normativa SEGES/ME nº 5/2017 (Atualizada), que dispõe sobre as regras e diretrizes do procedimento de contratação de serviços sob o regime de execução indireta no âmbito da Administração Pública federal direta, autárquica e fundacional;

4.6.52 Instrução Normativa nº 65, de 07 de julho de 2021, da Secretaria Especial de Desburocratização, Gestão e Governo Digital do Ministério da Economia;

Requisitos Temporais

4.6.53 A Entrega dos equipamentos deverá ser efetivada no prazo máximo de 120 (cento e vinte) dias corridos, a contar da demanda exercida pelo Instituto Nacional de Cardiologia.

4.6.54 A implementação completa da solução ocorrerá cumprindo o Cronograma estabelecido pela Área Requisitante.

Requisitos de Segurança e Privacidade

4.6.55 A Contratada deverá observar integralmente os requisitos de Segurança da Informação Privacidade descritas neste Termo de referência.

4.6.56 Os serviços contratados deverão ser prestados consoante as leis, normas e diretrizes vigentes no âmbito da Administração Pública Federal relacionadas à Segurança da Informação e Comunicações (SIC); em especial atenção ao Decreto nº 9.637, de 26 de dezembro de 2018, à Instrução Normativa GSI/PR nº 01, de 13 de junho de 2008 (e suas normas complementares).

4.6.57 A CONTRATADA deverá atender a Lei nº 13.709, de 14 de agosto de 2018 Lei Geral de Proteção de Dados Pessoais – LGPD, dispõe sobre o tratamento de dados pessoais, inclusive nos meios digitais, por pessoa natural ou por pessoa jurídica de direito público, ou privado, visando proteger os direitos fundamentais de liberdade e de privacidade e o livre desenvolvimento da personalidade da pessoa natural.

4.6.58 A CONTRATADA deverá comprometer-se, por si e por seus funcionários, em documento formal, a aceitar e aplicar rigorosamente todas as normas e procedimentos de segurança implementados no ambiente de Tecnologia da Informação do INC inclusive com a assinatura de Termo de Responsabilidade e Manutenção de Sigilo.

4.6.59 A CONTRATADA deverá comunicar ao INC, com a antecedência mínima necessária, qualquer ocorrência de transferência, remanejamento ou demissão de funcionários envolvidos diretamente na execução do Contrato, para que seja providenciada a revogação de todos os privilégios de acesso aos sistemas, informações e recursos do INC que porventura sejam colocados à disposição para realização dos serviços contratados.

4.6.60 A CONTRATADA deve garantir os controles criptográficos para armazenamento, tráfego e tratamento da informação;

Requisito de Vistoria

4.6.61 Não há necessidade de realização de avaliação prévia do local de execução dos serviços.

Sustentabilidade

4.6.62 Além dos critérios de sustentabilidade eventualmente inseridos na descrição do objeto, devem ser atendidos os seguintes se baseiam no Guia Nacional de Contratações Sustentáveis e no Plano de Logística requisitos, que se baseiam no Sustentável (PLS), do Ministério da Saúde.

Conformidade com Normas Técnicas e Ambientais

4.6.62.1. Os equipamentos de Tecnologia da Informação e Comunicação objeto da presente contratação, compreendendo servidores, deverão atender, sempre que aplicável, às normas técnicas de segurança, eficiência switches e appliances de rede energética e compatibilidade eletromagnética estabelecidas por entidades de normalização reconhecidas.

4.6.62.2. Para fins de atendimento a tais requisitos, os equipamentos deverão estar em conformidade com normas técnicas emitidas pela Associação Brasileira de Normas Técnicas ou por normas técnicas internacionais equivalentes, quando aplicáveis, bem como possuir certificações emitidas por organismos acreditados pelo Instituto Nacional de Metrologia, Qualidade e Tecnologia - INMETRO.

Requisitos de Segurança e Compatibilidade Eletromagnética

4.6.62.3. Os equipamentos ofertados deverão atender às normas técnicas aplicáveis relativas à segurança elétrica e à compatibilidade eletromagnética, de forma a garantir o adequado funcionamento em ambientes de infraestrutura de Tecnologia da Informação e Comunicação, evitando interferências eletromagnéticas e riscos à integridade das instalações e dos usuários.

A comprovação poderá ocorrer por meio de:

- Certificação emitida por organismos acreditados pelo Inmetro;
- Relatórios de ensaios ou certificações emitidos por laboratórios reconhecidos; ou
- Documentação técnica oficial do fabricante que demonstre a conformidade com normas técnicas equivalentes.

Eficiência Energética e Sustentabilidade Ambiental

4.6.62.4. Visando promover a adoção de práticas de Tecnologia da Informação Verde (Green IT) e a redução do impacto ambiental associado à operação de equipamentos de TI em ambientes de Data Center, os equipamentos deverão observar requisitos relacionados à eficiência energética e ao consumo racional de energia.

Nesse sentido, os equipamentos deverão, sempre que aplicável:

- Atender às normas técnicas ou certificações relacionadas à eficiência energética;
- Possuir recursos de gerenciamento e monitoramento de consumo energético;
- Observar diretrizes de redução de substâncias potencialmente nocivas ao meio ambiente, conforme normas ambientais vigentes.

Logística Reversa e Destinação Ambientalmente Adequada

4.6.62.5. Em observância aos princípios da responsabilidade compartilhada pelo ciclo de vida dos produtos, previstos na Lei nº 12.305 /2010, o fornecedor deverá adotar práticas que favoreçam a destinação ambientalmente adequada de equipamentos eletroeletrônicos ao final de seu ciclo de vida. Quando aplicável, o fornecedor deverá:

- Comprovar a existência de política ou programa de logística reversa para equipamentos eletroeletrônicos;
- Disponibilizar orientações técnicas ou procedimentos para o descarte ambientalmente adequado dos equipamentos e de seus componentes;
- Colaborar, quando solicitado pela Administração, com programas de recolhimento, reaproveitamento ou reciclagem de equipamentos eletroeletrônicos.

Embalagens Sustentáveis

4.6.62.6. As embalagens utilizadas para o acondicionamento e transporte dos equipamentos deverão observar práticas que reduzam o impacto ambiental, devendo, sempre que possível:

- Ser constituídas por materiais recicláveis ou reutilizáveis;
- Priorizar o uso de materiais reciclados ou provenientes de fontes sustentáveis;
- Reduzir a utilização de materiais plásticos descartáveis ou de difícil reciclagem.
- Sempre que aplicável, recomenda-se que as embalagens permitam a adequada reciclagem ou reaproveitamento após a entrega dos equipamentos.

Aceitação de Normas ou Certificações Equivalentes

4.6.62.7. Serão aceitas normas técnicas internacionais ou certificações equivalentes às normas da ABNT, desde que emitidas por organismos de avaliação da conformidade reconhecidos ou acreditados por entidades competentes, desde que garantam nível de segurança, desempenho e eficiência energética equivalente ou superior ao previsto nas normas nacionais aplicáveis.

Comprovação de Conformidade

4.6.62.8. A comprovação do atendimento aos requisitos estabelecidos nesta seção poderá ser realizada mediante a apresentação de:

- Certificados emitidos por organismos acreditados pelo Inmetro;
- Relatórios de ensaios laboratoriais reconhecidos;
- Documentação técnica oficial do fabricante; ou
- Declaração formal do fabricante ou de seu representante autorizado, acompanhada da documentação comprobatória pertinente.

4.6.62.9. Matriz de Sustentabilidade

Critério	Aplicação
Eficiência energética	Servidores, switches e outros componentes tais como: fontes de alimentação, processadores, memória RAM, armazenamento, placas de rede, sistemas de refrigeração, GPUs, placas-mãe, equipamentos de rede, infraestrutura elétrica do Data Center e afins.
Redução de substâncias tóxicas	Todos os equipamentos
Certificação ambiental	Quando aplicável
Durabilidade e modularidade	Servidores
Logística reversa	Todos os equipamentos
Embalagem sustentável	Todos os equipamentos

Indicação de marcas ou modelos (Art. 41, inciso I, da Lei nº 14.133, de 2021):

4.6.63 Na presente aquisição os itens listados no objeto devem obedecer fielmente ao descritivo e seus detalhes não havendo o que se condicionar a específica marca ou modelo aos referidos itens.

Da exigência de revendedor autorizado

4.6.64 Em caso de fornecedor revendedor ou distribuidor, a licitante deverá comprovar que possui autorização para revender os produtos objetos deste edital. A exigência será constada através de consulta ao site do fabricante dos produtos informados em sua proposta após a etapa de lances.

Subcontratação

4.6.65 Não é admitida a subcontratação do objeto contratual, bem como dos componentes pertencentes a Solução objetivadas.

Da verificação de amostra do objeto

4.6.66 Poderá ser solicitada à primeira classificada, sob pena de desclassificação, a apresentação de catálogo, folder e/ou ficha técnica relativa ao material ofertado indicando as características técnicas solicitadas na contratação, para fins de avaliação minuciosa de compatibilidade e adequação às especificações do objeto.

4.6.67 Caso o catálogo, folder e/ou ficha técnica não seja(m) suficientemente claro(s) poderá ser solicitada, sob pena de desclassificação, amostra dos itens, que deverá(ão) ser entregue(s) no prazo máximo e improrrogável de até 10 (dez) dias úteis, a contar da data da convocação para avaliação técnica de compatibilidade e adequação às especificações do objeto;

4.6.68 Se solicitadas as amostras, estas deverão ser entregues devidamente identificadas no local e horário indicado na seção pertinente deste documento, na pessoa do fiscal/comissão de recebimento ou de seu substituto legal;

4.6.69 Caso o catálogo, folder e/ou ficha técnica ou a(s) amostra(s) da melhor proposta seja(m) reprovada(s), será convocada a autora da segunda melhor proposta e, assim, sucessivamente;

4.6.70 As amostras aprovadas permanecerão em poder deste Instituto até a entrega definitiva do objeto contratado, com vistas à avaliação da conformidade entre a amostra aprovada e o material efetivamente entregue, não serão devolvidas, tampouco subtraídas quando da entrega definitiva do objeto;

4.6.71 As amostras reprovadas estarão passíveis de destruição parcial ou total caso não sejam recolhidas, a expensas da empresa, no prazo de 10 (dez) dias úteis;

4.6.72 Vencido o prazo de entrega das amostras, não será permitido fazer ajustes ou modificações no produto apresentado para fins de adequá-lo à especificação constante deste instrumento.

4.6.73 Será realizada verificação de amostra do objeto para averiguar se os equipamentos da Solução de TIC apresentada pela Licitante detêm os requisitos mínimos necessários para realização dos serviços a serem contratados, de acordo com as funcionalidades, procedimentos e critérios objetivos descritos deste Termo de Referência.

4.6.74 A previsão de exigência de apresentação de catálogo, ficha técnica e, subsidiariamente, de amostra física dos itens ofertados, conforme estabelecido no item 4.13 deste Termo de Referência, justifica-se na necessidade de assegurar a adequada verificação da conformidade técnica da solução de TIC proposta, em consonância com as diretrizes da Instrução Normativa SGD/ME nº 94, de 23 de dezembro de 2022.

4.6.75 Considerando a complexidade e criticidade da solução a ser contratada, que envolve infraestrutura de datacenter composta por equipamentos de alto desempenho, armazenamento, rede e serviços associados, a simples análise documental pode não ser suficiente para comprovar, de forma inequívoca, a aderência integral aos requisitos técnicos especificados.

4.6.76 Nesse contexto, o próprio item 4.13 prevê que a avaliação inicial será realizada por meio de documentação técnica (catálogo, folder ou ficha técnica), sendo a exigência de amostra adotada apenas de forma subsidiária, quando tais documentos não forem suficientemente claros ou detalhados para aferição da compatibilidade do objeto.

4.6.77 A exigência de amostra, portanto, atende aos seguintes objetivos técnicos:

I – Mitigação de riscos de aquisição inadequada, permitindo verificar, de forma prática, a compatibilidade entre o produto ofertado e os requisitos técnicos exigidos;

II – Validação da aderência funcional e operacional, assegurando que a solução de TIC apresentada possui os requisitos mínimos necessários à execução dos serviços pretendidos ;

III – Redução de assimetria de informação entre licitantes e Administração, evitando que propostas sejam avaliadas com base apenas em descrições genéricas ou incompletas;

IV – Garantia da qualidade e desempenho da solução, especialmente relevante diante da criticidade do ambiente tecnológico a ser suportado (infraestrutura de saúde com alta exigência de disponibilidade e confiabilidade);

V – Suporte à atuação da equipe de fiscalização técnica, permitindo avaliação empírica e objetiva da solução ofertada antes da contratação.

4.6.78 Adicionalmente, a modelagem adotada no item 4.13 observa os princípios da proporcionalidade e da competitividade, uma vez que:

I – prioriza a análise documental, exigindo amostra apenas quando necessário;

II – limita a exigência à licitante melhor classificada, evitando ônus excessivo aos demais participantes;

III – estabelece prazo razoável para apresentação;

IV - prevê critérios objetivos de avaliação e possibilidade de convocação sucessiva em caso de reprovação.

4.6.79 Destaca-se ainda que a retenção da amostra aprovada até a entrega definitiva visa garantir a verificação de conformidade entre o material entregue e aquele previamente validado, reforçando o controle de qualidade da execução contratual

Requisitos de Negócio

4.6.80 A presente aquisição deve-se mostrar viável a atender as necessidades tecnológicas do Instituto Nacional de Cardiologia.

Principais Necessidades de Negócio

4.6.81 Atualização Tecnológica: A infraestrutura de TI obsoleta do INC não consegue mais acompanhar as necessidades atuais. Uma solução atualizada é necessária para revitalizar o sistema, incorporando tecnologias modernas que impulsionem o desempenho, a segurança e a escalabilidade.

4.6.82 Desempenho Aprimorado: A natureza sensível ao tempo das operações cardíacas requer um ambiente de TI que ofereça desempenho consistente e rápido. A solução proposta deve fornecer poder de processamento e armazenamento necessários para análises médicas avançadas.

4.6.83 Disponibilidade Contínua: A área médica não pode tolerar interrupções. A solução deve ser projetada para alta disponibilidade.

4.6.84 Segurança dos Dados: Dados médicos são altamente sensíveis. A solução proposta deve incluir recursos de segurança robustos, como criptografia e controle de acesso, para proteger informações confidenciais e garantir conformidade com regulamentações de privacidade.

4.6.85 Suporte Especializado: A transição para uma nova infraestrutura exige suporte técnico especializado. A empresa fornecedora da solução deve oferecer assistência competente para garantir uma implementação tranquila e manutenção contínua.

Informações Relevantes para o Dimensionamento da Proposta

4.6.86 A demanda do órgão tem como base as seguintes características:

Custo Total de Propriedade (TCO): A Solução proposta representa um investimento menor, e manutenção simplificada.

Otimização de Recursos: A integração de computação, armazenamento e virtualização na Solução proposta reduz o excesso de provisionamento, permitindo a alocação precisa de recursos de acordo com as necessidades reais. Isso evita gastos desnecessários em hardware subutilizado, maximizando o valor do investimento.

Manutenção e Suporte Simplificados: A gestão centralizada da Solução simplifica as tarefas de manutenção e suporte. A equipe de TI do INC gastará menos tempo na solução de problemas complexos, reduzindo custos associados a interrupções operacionais e a contratação de suporte externo.

Redução de Riscos Financeiros: A Solução proposta oferece redundância e tolerância a falhas, minimizando o risco de interrupções de serviço. Isso evita custos financeiros associados a paralisações operacionais, perda de dados ou recuperação de desastres.

Requisitos da Arquitetura Tecnológica

4.6.87 Conforme o item 4.1 deste TR.

Requisitos de Experiência Profissional

4.6.88 Não serão exigidos requisitos de experiência profissional para a presente contratação.

Requisitos de Formação da Equipe

4.6.89 Não serão exigidos requisitos de formação da equipe para a presente contratação.

Requisitos de Metodologia de Trabalho

4.6.90 O fornecimento dos equipamentos está condicionado ao recebimento pelo Contratado de Ordem de fornecimento de Bens (OFB) emitida pela Contratante.

4.6.91 A OFB indicará o tipo de equipamento, a quantidade e a localidade na qual os equipamentos deverão ser entregues.

4.6.92 O Contratado deve fornecer meios para contato e registro de ocorrências da seguinte forma: com funcionamento 24 horas por dia e 7 dias por semana de maneira eletrônica e 8 horas por dia e 5 dias por semana por via telefônica.

4.6.93 O andamento do fornecimento dos equipamentos deve ser acompanhado pelo Contratado, que dará ciência de eventuais acontecimentos à Contratante.

Da exigência de carta de solidariedade

4.6.94 Em caso de fornecedor revendedor ou distribuidor, será exigida carta de solidariedade emitida pelo fabricante, que assegure a execução do contrato.

Requisitos de Manutenção

4.6.95 Devido às características da solução, há necessidade de realização de manutenções corretivas/preventivas /adaptativa/evolutiva pela Contratada, visando à manutenção da disponibilidade da solução;

Da Aplicação da Margem de Preferência

4.6.96 Não será aplicada margem de preferência na presente contratação.

Requisitos de Garantia, Manutenção e Assistência Técnica

4.6.97 O prazo de garantia contratual dos bens, complementar à garantia legal, será de, no mínimo, 60 (sessenta) meses, ou pelo prazo fornecido pelo fabricante, se superior, contado a partir do primeiro dia útil subsequente à data do recebimento definitivo do objeto.

4.6.97.1. Justifica-se o prazo de garantia contratual descrito acima pela necessidade de assegurar a continuidade operacional, a confiabilidade e a sustentabilidade da infraestrutura de TIC em consonância com as diretrizes estabelecidas pela Instrução Normativa SGD/ME nº 94, de 23 de dezembro de 2022, conforme seguintes aspectos descritos abaixo:

4.6.97.1.1. a natureza dos bens a serem adquiridos, caracterizados como ativos críticos de TIC, demanda elevado nível de disponibilidade, desempenho e resiliência, sendo diretamente responsáveis pelo suporte aos processos institucionais e à prestação de serviços públicos digitais.

4.6.97.1.2. sob a perspectiva técnica, equipamentos de TIC possuem depreciação funcional e obsolescência tecnológica progressivas, sendo que os primeiros anos de operação concentram maior probabilidade de falhas decorrentes de defeitos de fabricação, vícios ocultos ou incompatibilidades sistêmicas. Assim, a exigência de garantia estendida por período mínimo de 60 meses alinha-se às melhores práticas de mercado para ambientes corporativos e datacenters.

4.6.98 Caso o prazo da garantia oferecida pelo fabricante seja inferior ao estabelecido nesta cláusula, o fornecedor deverá complementar a garantia do bem ofertado pelo período restante.

4.6.99 A garantia será prestada com vistas a manter os equipamentos fornecidos em perfeitas condições de uso, sem qualquer ônus ou custo adicional para o Contratante.

4.29. A garantia abrange a realização da manutenção corretiva dos bens pelo próprio Contratado, ou, se for o caso, por meio de assistência técnica autorizada, de acordo com as normas técnicas específicas.

4.6.100 Entende-se por manutenção corretiva aquela destinada a corrigir os defeitos apresentados pelos bens, compreendendo a substituição de peças, a realização de ajustes, reparos e correções necessárias.

4.6.101 As peças que apresentarem vício ou defeito no período de vigência da garantia deverão ser substituídas por outras novas, de primeiro uso, e originais, que apresentem padrões de qualidade e desempenho iguais ou superiores aos das peças utilizadas na fabricação do equipamento.

4.6.102 Uma vez notificado, o Contratado realizará a reparação ou substituição dos bens que apresentarem vício ou defeito no prazo de até 5 (cinco) dias úteis, contados a partir da data de retirada do equipamento das dependências da Administração pelo Contratado ou pela assistência técnica autorizada.

4.6.103 O prazo indicado no subitem anterior, durante seu transcurso, poderá ser prorrogado uma única vez, por igual período, mediante solicitação escrita e justificada do Contratado, aceita pelo Contratante.

4.6.104 Na hipótese do subitem acima, o Contratado deverá disponibilizar equipamento equivalente, de especificação igual ou superior ao anteriormente fornecido, para utilização em caráter provisório pelo Contratante, de modo a garantir a continuidade dos trabalhos administrativos durante a execução dos reparos.

4.6.105 Decorrido o prazo para reparos e substituições sem o atendimento da solicitação do Contratante ou a apresentação de justificativas pelo Contratado, fica o Contratante autorizado a contratar empresa diversa para executar os reparos, ajustes ou a substituição do bem ou de seus componentes, bem como a exigir do Contratado o reembolso pelos custos respectivos, sem que tal fato acarrete a perda da garantia dos equipamentos.

4.6.106 O custo referente ao transporte dos equipamentos cobertos pela garantia será de responsabilidade do Contratado.

4.6.107 A garantia legal ou contratual do objeto tem prazo de vigência próprio e desvinculado daquele fixado no contrato, permitindo eventual aplicação de penalidades em caso de descumprimento de alguma de suas condições, mesmo depois de expirada a vigência contratual.

Requisitos Sociais, Ambientais e Culturais

4.6.108 Os equipamentos devem estar aderentes às seguintes diretrizes sociais, ambientais e culturais:

- **Logística Reversa e Resíduos:** Responsabilidade da contratada pela logística reversa de itens como SSDs, baterias e embalagens, com destinação final ambientalmente adequada, em conformidade com a Política Nacional de Resíduos Sólidos (Lei nº 12.305/2010) e Decreto nº 10.936/2022.
- **Eficiência Energética:** Os equipamentos devem apresentar baixo consumo de energia.
- **Materiais Sustentáveis:** Prioridade para o fornecimento de bens que sejam, no todo ou em parte, compostos por materiais recicláveis, atóxicos e biodegradáveis.
- **Normas Técnicas:** Aderência às normas de eficiência energética e compatibilidade eletromagnética, como a Portaria nº 170/2012 do INMETRO.

4.6.109 Requisitos Sociais e Culturais:

- **Conduta Profissional:** Os colaboradores da contratada devem agir com ética, urbanidade, cortesia e sem qualquer espécie de preconceito (raça, sexo, idade, religião, etc.) no trato com os usuários do serviço público.
- **Manual e Suporte:** O objeto deve vir acompanhado de manual do usuário, com versão em português e informações claras sobre assistência técnica.
- **Acessibilidade:** Conformidade com as resoluções que visam a inclusão e acessibilidade, como Resolução CNJ nº 400/2021.
- **Lei nº 14.133/2021 (Nova Lei de Licitações):** Estabelece que os critérios de sustentabilidade são obrigatórios para a Administração Pública, visando a melhoria do desempenho ambiental e social.

Essas diretrizes visam garantir que a aquisição não seja apenas vantajosa economicamente, mas também socialmente inclusiva e ambientalmente responsável.

Requisitos de Projeto e de Implementação

4.6.110 Revisão e Qualidade: A empresa contratada deve certificar-se de que os equipamentos estão em perfeito funcionamento, pois serão revisados pela equipe de recebimento quanto aos requisitos de configurações mínimas e de funcionamento para o recebimento definitivo.

4.6.111 Conformidade: Fornecer os equipamentos conforme especificações do Termo de Referência e do Instrumento Convocatório, com os recursos necessários ao funcionamento.

4.6.112 Instalação/Automação: Adotar os mecanismos de automação e de implantação contínua disponibilizada pela CONTRATANTE, quando aplicável.

4.6.113 Conformidade Física: A instalação física deve ocorrer em rack padrão disponibilizado pela CONTRATANTE.

4.6.114 Testes: Energização e testes iniciais de funcionamento.

Outros requisitos comuns descritos nos resultados de pesquisa incluem:

- **Segurança (Security by design):** Utilizar o conceito de *security by design* em todo o ciclo de vida da entrega de soluções.
- **Interrupções:** A implantação não deverá interferir na rede em funcionamento, sendo que, em caso de necessidade, as interrupções devem ser autorizadas e agendadas.
- **Documentação:** A solução deverá ser entregue com toda a documentação técnica, em formato eletrônico, incluindo manuais do usuário.

Requisitos de Implantação

4.6.115 Os equipamentos deverão observar integralmente os requisitos de implantação, instalação e fornecimento descritos a seguir:

- **Conformidade Integral:** Não é aceitável cumprimento parcial. Todos os itens de implantação, instalação e fornecimento mencionados a seguir devem ser obedecidos.
- **Implantação:** Requisitos de local, fundações, infraestrutura prévia, layout ou preparação do ambiente.
- **Instalação:** Procedimentos técnicos de montagem, conexão, fixação e configuração.
- **Fornecimento:** Especificações do produto, componentes inclusos, documentação técnica, manuais e certificados.

Garantia da contratação

4.6.116 Será exigida a garantia da contratação de que tratam os arts. 96 e seguintes da Lei nº 14.133, de 2021, com validade durante a execução do contrato e 90 (noventa) dias após término da vigência contratual, podendo o Contratado optar pela caução em dinheiro ou em títulos da dívida pública, seguro-garantia, fiança bancária ou título de capitalização, em valor correspondente a 10% (dez por cento) do valor total da contratação.

4.6.117 Em caso de opção pelo seguro-garantia, a parte adjudicatária deverá apresentá-la, no máximo, até a data de assinatura do contrato.

4.6.117.1. A apólice de seguro-garantia permanecerá em vigor mesmo que o Contratado não pague o prêmio nas datas convencionadas.

4.6.117.2. Caso o adjudicatário não apresente a apólice de seguro de garantia antes da assinatura do contrato, ocorrerá a preclusão do direito de escolha dessa modalidade de garantia.

4.6.117.3. A apólice de seguro-garantia deverá acompanhar as modificações referentes à vigência do contrato principal mediante a emissão do respectivo endosso pela seguradora.

4.6.117.4. Será permitida a substituição da apólice de seguro-garantia na data de renovação ou de aniversário, desde que mantidas as condições e coberturas da apólice vigente e nenhum período fique descoberto, ressalvados os períodos de suspensão contratual.

4.6.117.5. Caso o adjudicatário não opte pelo seguro-garantia ou não apresente a apólice de seguro de garantia antes da assinatura do contrato, deverá apresentar, no prazo máximo de 10 (dez) dias úteis, prorrogáveis por igual período, a critério do Contratante, contado da assinatura do contrato, comprovante de prestação de garantia nas modalidades de caução em dinheiro ou títulos da dívida pública, fiança bancária ou títulos de capitalização.

4.6.118 Caso seja a garantia em dinheiro a modalidade de garantia escolhida pelo Contratado, deverá ser efetuada em favor do Contratante, em conta específica na Caixa Econômica Federal, com correção monetária.

4.6.119 Caso a opção seja por utilizar títulos da dívida pública, estes devem ter sido emitidos sob a forma escritural, mediante registro em sistema centralizado de liquidação e de custódia autorizado pelo Banco Central do Brasil, e avaliados pelos seus valores econômicos, conforme definido pelo Ministério competente.

4.6.120 No caso de garantia na modalidade de fiança bancária, deverá ser emitida por banco ou instituição financeira devidamente autorizada a operar no País pelo Banco Central do Brasil, e deverá constar expressa renúncia do fiador aos benefícios do artigo 827 do Código Civil.

4.6.121 Na hipótese de opção pelo título de capitalização, a garantia deverá ser custeada por pagamento único, com resgate pelo valor total, sob a modalidade de instrumento de garantia, emitido por sociedades de capitalização regulamente constituídas e autorizadas pelo Governo Federal.

4.6.121.1. O título de capitalização deverá ser apresentado ao Contratante juntamente com as condições gerais e o número do processo administrativo sob o qual o plano de capitalização foi aprovado pela Susep (art. 8º, III, da Circular SUSEP nº 656, de 11 de março de 2022).

4.6.122. A garantia assegurará, qualquer que seja a modalidade escolhida, sob pena de não aceitação, o pagamento de:

4.6.122.1. prejuízos advindos do não cumprimento do objeto do contrato e do não adimplemento das demais obrigações nele previstas; e

4.6.122.2. multas moratórias e punitivas aplicadas pela Administração ao Contratado.

4.6.123 No caso de alteração do valor do contrato, ou prorrogação de sua vigência, a garantia deverá ser ajustada ou renovada, no prazo máximo de 10 (dez) dias úteis, prorrogáveis por igual período, contado da data de assinatura do termo aditivo ou da emissão do apostilamento, seguindo os mesmos parâmetros utilizados quando da contratação.

4.6.124 Na hipótese de suspensão do contrato por ordem ou inadimplemento da Administração, o Contratado ficará desobrigado de renovar a garantia ou de endossar a apólice de seguro até a ordem de reinício da execução ou o adimplemento pela Administração.

4.6.125 Se o valor da garantia for utilizado total ou parcialmente em pagamento de qualquer obrigação, o Contratado obriga-se a fazer a respectiva reposição no prazo máximo de 10 (dez) dias úteis, prorrogáveis por igual período, a critério do Contratante, contados da data em que for notificada

4.6.126 O Contratante executará a garantia na forma prevista na legislação que rege a matéria.

4.6.126.1. O emitente da garantia ofertada pelo Contratado deverá ser notificado pelo Contratante quanto ao início de processo administrativo para apuração de descumprimento de cláusulas contratuais.

4.6.126.2. Caso se trate da modalidade seguro-garantia, ocorrido o sinistro durante a vigência da apólice, sua caracterização e comunicação poderão ocorrer fora desta vigência, não caracterizando fato que justifique a negativa do sinistro, desde que respeitados os prazos prescricionais aplicados ao contrato de seguro, nos termos do art. 20 da Circular Susep nº 662, de 11 de abril de 2022.

4.6.127. Extinguir-se-á a garantia com a restituição da carta fiança, autorização para a liberação de importâncias depositadas em dinheiro a título de garantia ou anuência ao resgate do título de capitalização, acompanhada de declaração do Contratante, mediante termo circunstanciado, de que o Contratado cumpriu todas as cláusulas do contrato.

4.6.127.1. A extinção da garantia na modalidade seguro-garantia observará a regulamentação da Susep.

4.6.127.2. A Administração deverá apurar se há alguma pendência contratual antes do término da vigência da apólice.

4.6.128. A garantia somente será liberada ou restituída após a fiel execução do contrato ou após a sua extinção por culpa exclusiva da Administração e, quando em dinheiro, será atualizada monetariamente.

4.6.129. O Contratado autoriza o Contratante a reter, a qualquer tempo, a garantia, na forma prevista neste Termo de Referência.

4.6.130. O garantidor não é parte para figurar em processo administrativo instaurado pelo Contratante com o objetivo de apurar prejuízos e/ou aplicar sanções ao Contratado.

4.6.131. A garantia de execução é independente de eventual garantia do produto ou serviço prevista neste Termo de Referência.

4.6.132 O contrato, em caso que se fizer necessário, oferecerá maior detalhamento das regras que serão aplicadas em relação à garantia da contratação.

Informações relevantes para o dimensionamento E/OU apresentação da proposta

4.6.133 A demanda do órgão é fundamentada em:

- **Quantitativos Estimados:** Descrição detalhada dos volumes, unidades e itens necessários, baseados em histórico de consumo ou estudos técnicos.
- **Perfis de Demanda:** Especificação de perfis de usuário, tipos de materiais, ou complexidade dos serviços (ex: níveis de serviço - SLA).
- **Local e Prazo de Execução:** Endereços onde o serviço será prestado ou bens entregues, e o cronograma estimado (início/fim).
- **Requisitos Técnicos Mínimos:** Padrões de qualidade, normas técnicas (ABNT) e certificações exigidas para os produtos/serviços

Reserva de cotas para microempresas e empresas de pequeno porte:

4.6.134 Inviabilidade Técnica ou Prejuízo ao Conjunto: A lei exige a reserva quando o objeto é divisível. Se o objeto for indivisível (ex: uma máquina que precisa ser comprada inteira de um único fornecedor para funcionar), a cota não se aplica.

4.6.135 No Caso dessa aquisição a solução necessária é indivisível por isso retiramos a cota para microempresas e empresas de pequeno porte.

5. PAPÉIS E RESPONSABILIDADES

5.1. São obrigações da CONTRATANTE:

5.1.1. nomear Gestor e Fiscais Técnico, Administrativo e Requisitante do contrato para acompanhar e fiscalizar a execução dos contratos;

5.1.2. encaminhar formalmente a demanda por meio de Ordem de Serviço ou de Fornecimento de Bens, de acordo com os critérios estabelecidos no Termo de Referência;

5.1.3. receber o objeto fornecido pelo Contratado que esteja em conformidade com a proposta aceita, conforme inspeções realizadas;

5.1.4. aplicar à contratada as sanções administrativas regulamentares e contratuais cabíveis, comunicando ao órgão gerenciador da Ata de Registro de Preços, quando aplicável;

5.1.5. liquidar o empenho e efetuar o pagamento à contratada, dentro dos prazos preestabelecidos em contrato;

5.1.6. comunicar à contratada todas e quaisquer ocorrências relacionadas com o fornecimento da solução de TIC;

5.1.7. definir produtividade ou capacidade mínima de fornecimento da solução de TIC por parte do Contratado, com base em pesquisas de mercado, quando aplicável; e

5.1.8. prever que os direitos de propriedade intelectual e direitos autorais da solução de TIC sobre os diversos artefatos e produtos cuja criação ou alteração seja objeto da relação contratual pertençam à Administração, incluindo a documentação, o código-fonte de aplicações, os modelos de dados e as bases de dados, justificando os casos em que isso não ocorrer.

5.2. São obrigações do CONTRATADO:

5.2.1. indicar formalmente preposto apto a representá-la junto à Contratante, que deverá responder pela fiel execução do contrato;

5.2.2. atender prontamente quaisquer orientações e exigências da Equipe de Fiscalização do Contrato, inerentes à execução do objeto contratual;

5.2.3. reparar quaisquer danos diretamente causados à Contratante ou a terceiros por culpa ou dolo de seus representantes legais, prepostos ou empregados, em decorrência da relação contratual, não excluindo ou reduzindo a responsabilidade da fiscalização ou o acompanhamento da execução do contrato pela Contratante;

5.2.4. propiciar todos os meios necessários à fiscalização do contrato pela Contratante, cujo representante terá poderes para sustar o fornecimento, total ou parcial, em qualquer tempo, desde que motivadas as causas e justificativas desta decisão;

5.2.5. manter, durante toda a execução do contrato, as mesmas condições da habilitação;

5.2.6. quando especificada, manter, durante a execução do contrato, equipe técnica composta por profissionais devidamente habilitados, treinados e qualificados para fornecimento da solução de TIC;

5.2.7. quando especificado, manter a produtividade ou a capacidade mínima de fornecimento da solução de TIC durante a execução do contrato;

5.2.8. ceder os direitos de propriedade intelectual e direitos autorais da solução de TIC sobre os diversos artefatos e produtos produzidos em decorrência da relação contratual, incluindo a documentação, os modelos de dados e as bases de dados à Administração; e

5.2.9. fazer a transição contratual, com transferência de conhecimento, tecnologia e técnicas empregadas, sem perda de informações, podendo exigir, inclusive, a capacitação dos técnicos do contratante ou da nova empresa que continuará a execução do contrato, quando for o caso.

5.3 São obrigações do órgão gerenciador do registro de preços:

- Efetuar o registro do licitante fornecedor e firmar a correspondente Ata de Registro de Preços;
- Os procedimentos para emissão das solicitações de fornecimento;
- O controle dos quantitativos registrados, solicitados, entregues e remanescentes;
- A definição dos prazos de entrega após cada solicitação;
- O acompanhamento da capacidade de fornecimento do contratado;
- Os mecanismos de comunicação entre o órgão gerenciador, os órgãos participantes e o fornecedor;
- Os procedimentos para reprogramação de entregas em situações excepcionais devidamente justificadas;
- O acompanhamento do cumprimento das garantias e demais obrigações contratuais.
- As regras para a substituição da solução registrada na Ata de Registro de Preços, garantida a verificação de Amostra do Objeto, observado o disposto no inciso III, alínea "c", item 2 deste artigo, em função de fatores supervenientes que tornem necessária e imperativa a substituição da solução tecnológica.

6. MODELO DE EXECUÇÃO DO CONTRATO

Rotinas de Execução

Do Encaminhamento Formal de Demandas

- 6.1. O gestor do contrato emitirá a Ordem de fornecimento de bens (OFB) para a entrega dos bens desejados.
- 6.2. O Contratado deverá fornecer equipamentos com as mesmas configurações e quantidades definidas na OFB.

Forma de execução e acompanhamento do contrato

Condições de Entrega

- 6.3 Os componentes pertencentes à Solução serão entregues diante da demanda executada pela Área Técnica requisitante conforme a Ordem de Fornecimento de Bens ou Nota de Empenho, em remessa única, de acordo com os empenhos.
- 6.4 Caso não seja possível a entrega até a data estabelecida até 120 dias após solicitação da Área Técnica Requisitante, a fornecedora deverá comunicar as razões respectivas com pelo menos 10 dias de antecedência para que qualquer pleito de prorrogação de prazo seja analisado, ressalvadas situações de caso fortuito e força maior.
- 6.5 Os bens deverão ser entregues no seguinte endereço: Rua das Laranjeiras, nº 374, Anexo, 3º andar – Área de TI.
- 6.6 O local de instalação dos equipamentos é acessível apenas por escadas, sem acesso direto por elevador.

Da Substituição do Termo de Contrato pela Nota Empenho

- 6.7 Após a adjudicação e homologação do certame, será formalizada a Ata de Registro de Preços e, quando cabível, o respectivo instrumento contratual.
- 6.8 Os equipamentos serão solicitados de forma parcelada, conforme a necessidade da Administração, mediante emissão de Nota de Empenho ou outro instrumento hábil de contratação, observadas as condições registradas na Ata e os quantitativos efetivamente demandados.
- 6.9 A contratada se vincula à sua proposta e às previsões contidas no aviso de dispensa de licitação, no Termo de Referência e seus anexos;
- 6.10 O prazo de vigência da contratação é de 12 meses;
- 6.11 Na hipótese de a descrição do objeto indicado na Nota de Empenho não contemplar de forma plena o detalhamento do objeto, prevalecerá àquela expressa no Termo de Referência;
- 6.12 A contratada reconhece que as hipóteses de rescisão são aquelas previstas nos artigos 137 e 138 da Lei nº 14.133/21 e reconhece os direitos da Administração previstos nos artigos 137 a 139 da mesma Lei.
- 6.13 A recusa injustificada do adjudicatário em aceitar a Nota de Empenho ou assinatura do Contrato no prazo estabelecido pela Administração caracterizará o descumprimento total da obrigação assumida e o sujeitará às penalidades legalmente estabelecidas e à imediata perda da garantia de proposta em favor do órgão (Art. 90, §5º da Lei nº 14.133/2021);

Mecanismos Formais de Comunicação

- 6.14 São definidos como mecanismos formais de Comunicação, entre a Contratante e o Contratado, os seguintes:

- Ordem de Fornecimento de Bens;
- Ata de Reunião;
- Ofício;

- Sistema de abertura de chamados;
- E-mails e Cartas;
- Protocolo de atendimento.

Formas de Pagamento

6.15 Os critérios de medição e pagamento serão tratados em tópico próprio do Modelo de Gestão do Contrato.

Manutenção de Sigilo e Normas de Segurança

6.16 O Contratado deverá manter sigilo absoluto sobre quaisquer dados e informações contidos em quaisquer documentos e mídias, incluindo os equipamentos e seus meios de armazenamento, de que venha a ter conhecimento durante a execução do contrato, não podendo, sob qualquer pretexto, divulgar, reproduzir ou utilizar, sob pena de lei, independentemente da classificação de sigilo conferida pelo Contratante a tais documentos.

6.17 O Termo de Compromisso e Manutenção de Sigilo, contendo declaração de manutenção de sigilo e respeito às normas de segurança vigentes na entidade, a ser assinado pelo representante legal do Contratado, e Termo de Ciência, a ser assinado por todos os empregados do Contratado diretamente envolvidos na contratação.

Procedimentos de transição e finalização do contrato

6.18. Não serão necessários procedimentos de transição e finalização do contrato devido às características do objeto.

Formas de transferência de conhecimento

6.19. Não será necessária transferência de conhecimento devido às características do objeto.

Quantidade mínima de bens ou serviços para comparação e controle

6.20. Cada OFB conterá a quantidade a ser fornecida, incluindo a sua localização e o prazo, conforme definições deste TR.

7. MODELO DE GESTÃO DO CONTRATO

7.1. O contrato deverá ser executado fielmente pelas partes, de acordo com as cláusulas avençadas e as normas da Lei nº 14.133, de 2021, e cada parte responderá pelas consequências de sua inexecução total ou parcial.

7.2. Em caso de impedimento, ordem de paralisação ou suspensão do contrato, o cronograma de execução será prorrogado automaticamente pelo tempo correspondente, anotadas tais circunstâncias mediante simples apostila.

7.3. As comunicações entre o órgão ou entidade e o Contratado devem ser realizadas por escrito sempre que o ato exigir tal formalidade, admitindo-se o uso de mensagem eletrônica para esse fim.

7.4. O órgão ou entidade poderá convocar representante da empresa para adoção de providências que devam ser cumpridas de imediato.

Reunião Inicial

7.5 A Reunião Inicial será caracterizada como Obrigatória;

7.6. Após a assinatura do Contrato e a nomeação do Gestor e Fiscais do Contrato, será realizada a Reunião Inicial de alinhamento com o objetivo de nivelar os entendimentos acerca das condições estabelecidas no Contrato, Edital e seus anexos, e esclarecer possíveis dúvidas acerca da execução do contrato.

7.7. A reunião será realizada em conformidade com o previsto no inciso I do Art. 31 da IN SGD/ME nº 94, de 2022, e ocorrerá em até 5 (cinco) dias úteis da assinatura do Contrato, podendo ser prorrogada a critério da Contratante.

7.8. A pauta desta reunião observará, pelo menos:

7.8.1. Presença do representante legal da contratada, que apresentará o seu preposto;

7.8.2. Entrega, por parte da Contratada, do Termo de Compromisso e dos Termos de Ciência;

7.8.3. esclarecimentos relativos a questões operacionais, administrativas e de gestão do contrato;

7.8.4. A Carta de apresentação do Preposto deverá conter no mínimo o nome completo e CPF do funcionário da empresa designado para acompanhar a execução do contrato e atuar como interlocutor principal junto à Contratante, incumbido de receber, diligenciar, encaminhar e responder as principais questões técnicas, legais e administrativas referentes ao andamento contratual;

7.8.5. Apresentação das declarações/certificados do fabricante, comprovando que o produto ofertado possui a garantia solicitada neste termo de referência.

Fiscalização

7.9. A execução do contrato deverá ser acompanhada e fiscalizada pelo(s) fiscal(is) do contrato, ou pelos respectivos substitutos, nos termos do art. 33 da IN SGD nº 94, de 2022, observando-se, em especial, as rotinas a seguir.

Fiscalização Técnica

7.10. O fiscal técnico do contrato, além de exercer as atribuições previstas no art. 33, II, da IN SGD nº 94, de 2022, acompanhará a execução do contrato, para que sejam cumpridas todas as condições estabelecidas no contrato, de modo a assegurar os melhores resultados para a Administração.

7.11. O fiscal técnico do contrato anotará no histórico de gerenciamento do contrato todas as ocorrências relacionadas à execução do contrato, com a descrição do que for necessário para a regularização das faltas ou dos defeitos observados.

7.12. Identificada qualquer inexecução ou irregularidade, o fiscal técnico do contrato emitirá notificações para a correção da execução do contrato, determinando prazo para a correção.

7.13. O fiscal técnico do contrato informará ao gestor do contrato, em tempo hábil, a situação que demandar decisão ou adoção de medidas que ultrapassem sua competência, para que adote as medidas necessárias e saneadoras, se for o caso.

7.14. No caso de ocorrências que possam inviabilizar a execução do contrato nas datas aprazadas, o fiscal técnico do contrato comunicará o fato imediatamente ao gestor do contrato.

7.15. O fiscal técnico do contrato comunicará ao gestor do contrato, em tempo hábil, o término do contrato sob sua responsabilidade, com vistas à renovação tempestiva ou à prorrogação contratual.

Fiscalização Administrativa

7.16. O fiscal administrativo do contrato, além de exercer as atribuições previstas no art. 33, IV, da IN SGD nº 94, de 2022, verificará a manutenção das condições de habilitação da contratada, acompanhará o empenho, o pagamento, as garantias, as glosas e a formalização de apostilamento e termos aditivos, solicitando quaisquer documentos comprobatórios pertinentes, caso necessário.

7.17. Caso ocorra descumprimento das obrigações contratuais, o fiscal administrativo do contrato atuará tempestivamente na solução do problema, reportando ao gestor do contrato para que tome as providências cabíveis, quando ultrapassar a sua competência.

7.18. A fiscalização de que trata esta cláusula não exclui nem reduz a responsabilidade do Contratado, inclusive perante terceiros, por qualquer irregularidade, ainda que resultante de imperfeições técnicas, vícios redibitórios, ou emprego de material inadequado ou de qualidade inferior e, na ocorrência desta, não implica corresponsabilidade da Contratante ou de seus agentes, gestores e fiscais, de conformidade.

Gestor do Contrato

7.19. Cabe ao gestor do contrato, além de exercer as atribuições previstas no art. 33, I, da IN SGD nº 94, de 2022:

7.19.1. Coordenar a atualização do processo de acompanhamento e fiscalização do contrato contendo todos os registros formais da execução no histórico de gerenciamento do contrato, a exemplo da ordem de serviço, do registro de ocorrências, das alterações e das prorrogações contratuais, elaborando relatório com vistas à verificação da necessidade de adequações do contrato para fins de atendimento da finalidade da administração.

7.19.2. Acompanhar os registros realizados pelos fiscais do contrato, de todas as ocorrências relacionadas à execução do contrato e as medidas adotadas, informando, se for o caso, à autoridade superior àquelas que ultrapassarem a sua competência.

7.19.3. Acompanhar a manutenção das condições de habilitação da contratada, para fins de empenho de despesa e pagamento, e anotar os problemas que obstem o fluxo normal da liquidação e do pagamento da despesa no relatório de riscos eventuais.

7.19.4. Emitir documento comprobatório da avaliação realizada pelos fiscais técnico, administrativo e setorial quanto ao cumprimento de obrigações assumidas pelo Contratado, com menção ao seu desempenho na execução contratual, baseado nos indicadores objetivamente definidos e aferidos, e a eventuais penalidades aplicadas, devendo constar do cadastro de atesto de cumprimento de obrigações.

7.19.5. Tomar providências para a formalização de processo administrativo de responsabilização para fins de aplicação de sanções, a ser conduzido pela comissão de que trata o art. 158 da Lei nº 14.133, de 2021, ou pelo agente ou pelo setor com competência para tal, conforme o caso.

7.19.6. Elaborar relatório final com informações sobre a consecução dos objetivos que tenham justificado a contratação e eventuais condutas a serem adotadas para o aprimoramento das atividades da Administração.

7.19.7. Enviar a documentação pertinente ao setor de contratos para a formalização dos procedimentos de liquidação e pagamento, no valor dimensionado pela fiscalização e gestão nos termos do contrato.

7.20. O fiscal técnico do contrato comunicará ao gestor do contrato, em tempo hábil, o término do contrato sob sua responsabilidade, com vistas à tempestiva renovação ou prorrogação contratual.

Critérios de Aceitação

7.21. A avaliação da qualidade dos produtos entregues, para fins de aceitação, consiste na verificação dos critérios relacionados a seguir:

7.22. Todos os equipamentos fornecidos deverão ser novos (incluindo todas as peças e componentes presentes nos produtos), de primeiro uso (sem sinais de utilização anterior), não reconicionados e em fase de comercialização normal através dos canais de venda do fabricante no Brasil (não serão aceitos produtos end-of-life).

7.23. Todos os componentes do(s) equipamento(s) e respectivas funcionalidades deverão ser compatíveis entre si, sem a utilização de adaptadores, frisagens, pinturas, usinagens em geral, furações, emprego de adesivos, fitas adesivas ou quaisquer outros procedimentos não previstos nas especificações técnicas ou, ainda, com emprego de materiais inadequados ou que visem adaptar forçadamente o produto ou suas partes que sejam fisicamente ou logicamente incompatíveis.

7.24. Todos os componentes internos do(s) equipamento(s) deverá(ão) estar instalado(s) de forma organizada e livres de pressões ocasionados por outros componentes ou cabos, que possam causar desconexões, instabilidade, ou funcionamento inadequado.

7.25. O número de série de cada equipamento deve ser obrigatório e único, afixado em local visível, na parte externa do gabinete e na embalagem que o contém. Esse número deverá ser identificado pelo fabricante, como válido para o produto entregue e para as condições do mercado brasileiro no que se refere à garantia e assistência técnica no Brasil.

7.26. Serão recusados os produtos que possuam componentes ou acessórios com sinais claros de oxidação, danos físicos, sujeira, riscos ou outro sinal de desgaste, mesmo sendo o componente ou acessório considerado como novos pelo fornecedor dos produtos.

7.27. Os produtos, considerando a marca e modelo apresentados na licitação, não poderão estar fora de linha comercial, considerando a data de LICITAÇÃO (abertura das propostas). Os produtos devem ser fornecidos completos e prontos para a utilização, com todos os acessórios, componentes, cabos etc.

7.28. Todas as licenças, referentes aos softwares e drivers solicitados, devem estar registrados para utilização do Contratante, em modo definitivo (licenças perpétuas), legalizado, não sendo admitidas versões “shareware” ou “trial”. O modelo do produto ofertado pelo licitante deverá estar em fase de produção pelo fabricante (no Brasil ou no exterior), sem previsão de encerramento de produção, até a data de entrega da proposta.

7.29. A Contratante poderá optar por avaliar a qualidade de todos os equipamentos fornecidos ou uma amostra dos equipamentos, atentando para a inclusão nos autos do processo administrativo de todos os documentos que evidenciem a realização dos testes de aceitação em cada equipamento selecionado, para posterior rastreabilidade.

7.30. Só haverá o recebimento definitivo, após a análise da qualidade dos bens e/ou serviços, em face da aplicação dos critérios de aceitação, resguardando-se ao Contratante o direito de não receber o OBJETO cuja qualidade seja comprovadamente baixa ou em desacordo com as especificações definidas neste Termo de Referência – situação em que poderão ser aplicadas à CONTRATADA as penalidades previstas em lei, neste Termo de Referência e no CONTRATO. Quando for o caso, a empresa será convocada a refazer todos os serviços rejeitados, sem custo adicional.

Níveis Mínimos de Serviço Exigidos

7.31. Os níveis mínimos de serviço são indicadores mensuráveis estabelecidos pelo Contratante para aferir objetivamente os resultados pretendidos com a contratação. São considerados para a presente contratação os seguintes indicadores:

IAE – INDICADOR DE ATRASO NO FORNECIMENTO DO EQUIPAMENTO		
Tópico	Descrição	
Finalidade	Medir o tempo de atraso na entrega dos produtos e serviços constantes na Ordem de Fornecimento de Bens.	
Meta a cumprir	IAE < = 0	A meta definida visa garantir a entrega dos produtos e serviços constantes nas Ordens de Fornecimento de Bens dentro do prazo previsto.
Instrumento de medição	OFB, Termo de Recebimento Provisório (TRP)	
Forma de acompanhamento	A avaliação será feita conforme linha de base do cronograma registrada na OFB. Será subtraída a data de entrega dos produtos da OFB (desde que o fiscal técnico reconheça aquela data, com registro em Termo de Recebimento Provisório) pela data de início da execução da OFB.	
Periodicidade	Para cada Ordem de Fornecimento de Bens encerrada e com Termo de Recebimento Definitivo.	

Mecanismo de Cálculo (métrica)	<p><u>IAE = TEX – TEST</u></p> <p>Onde:</p> <p>IAE – Indicador de Atraso de Entrega da OFB;</p> <p>TEX – Tempo de Execução – corresponde ao período de execução da OFB, da sua data de início até a data de entrega dos produtos da OFB.</p> <p>A data de início será aquela constante na OFB; caso não esteja explícita, será o primeiro dia útil após a emissão da OFB.</p> <p>A data de entrega da OFB deverá ser aquela reconhecida pelo fiscal técnico, conforme critérios constantes neste Termo de Referência. Para os casos em que o fiscal técnico rejeita a entrega, o prazo de execução da OFB continua a correr, findando-se apenas quanto o Contratado entrega os produtos da OFB e haja aceitação por parte do fiscal técnico.</p> <p>TEST – Tempo Estimado para a execução da OFB – constante na OFB, conforme estipulado no Termo de Referência.</p>
Observações	<p>Obs1: Serão utilizados dias corridos na medição.</p> <p>Obs2: Os dias com expediente parcial no órgão/entidade serão considerados como dias corridos no cômputo do indicador.</p>
Início de Vigência	A partir da emissão da OFB.
Faixas de ajuste no pagamento e Sanções	<p>Para valores do indicador IAE:</p> <p>Menor ou igual a 0 – Pagamento integral da OFB;</p> <p>De 1 a 60 - aplicar-se-á glosa de 0,1666% por dia de atraso sobre o valor da OFB ou fração em atraso.</p> <p>Acima de 60 - aplicar-se-á glosa de 10% bem como multa de 2% sobre o valor OFB ou fração em atraso.</p>

Para valores do indicador

IAE: Menor ou igual a 0 – Pagamento integral da OFB;

Faixas de ajuste no pagamento e Sanções

De 1 a 60 - aplicar-se-á glosa de 0,1666% por dia de atraso sobre o valor da OFB ou fração em atraso.

Acima de 60 - aplicar-se-á glosa de 10% bem como multa de 2% sobre o valor OFB ou fração em atraso.

8. INFRAÇÕES E SANÇÕES ADMINISTRATIVAS E PROCEDIMENTOS PARA RETENÇÃO OU GLOSA NOS PAGAMENTOS

8.1. Nos casos de inadimplemento na execução do objeto, as ocorrências serão registradas pela Contratante, conforme a tabela abaixo:

Id	Ocorrência	Glosa / Sanção
1	Não prestar os esclarecimentos imediatamente, referente à execução do contrato, salvo quando implicarem em indagações de caráter técnico, hipótese em que serão respondidos no prazo máximo de (2) dois dias úteis.	Multa de 2 (dois) % sobre o valor total do Contrato por dia útil de atraso em prestar as informações por escrito, ou por outro meio quando autorizado pela Contratante, até o limite de 10 (dez) dias úteis.
		Após o limite de 10 (dez) dias úteis, aplicar-se-á multa de 10 (dez) % do valor total do Contrato.
2	Não atender ao indicador de nível de serviço IAE (Indicador de Atraso de Entrega de OS)	Glosa de 2 (dois) % sobre o valor da OS para valores do indicador IAE de 0,11 a 0,20.
		Glosa de 4 (quatro) % sobre o valor da OS para valores do indicador IAE de 0,21 a 0,30.
		Glosa de 6 (seis) % sobre o valor da OS para valores do indicador IAE de 0,31 a 0,50.
		Glosa de 8 (oito) % sobre o valor da OS para valores do indicador IAE de 0,51 a 1,00.
		Multa de 10 (dez) % sobre o valor do Contrato e Glosa de 5 (cinco) % sobre o valor da OS, para valores do indicador IAE maiores que 1,00.
N	Não cumprir qualquer outra obrigação contratual não citada nesta tabela.	Advertência. Em caso de reincidência ou configurado prejuízo aos resultados pretendidos com a contratação, aplica-se multa de 5 (cinco) % do valor total do Contrato.

8.2. Nos termos do art. 19, inciso III da Instrução Normativa SGD/ME nº 94, de 2022, será efetuada a retenção ou glosa no pagamento, proporcional à irregularidade verificada, sem prejuízo das sanções cabíveis, nos casos em que o Contratado:

8.2.1. não atingir os valores mínimos aceitáveis fixados nos critérios de aceitação, não produzir os resultados ou deixar de executar as atividades contratadas; ou

8.2.2. deixar de utilizar materiais e recursos humanos exigidos para fornecimento da solução de TIC, ou utilizá-los com qualidade ou quantidade inferior à demandada;

8.3. Comete infração administrativa, nos termos da Lei nº 14.133, de 2021, o Contratado que:

a) der causa à inexecução parcial do contrato;

b) der causa à inexecução parcial do contrato que cause grave dano à Administração ou ao funcionamento dos serviços públicos ou ao interesse coletivo;

c) der causa à inexecução total do contrato;

- d) ensejar o retardamento da execução ou da entrega do objeto da contratação sem motivo justificado;
- e) apresentar documentação falsa ou prestar declaração falsa durante a execução do contrato;
- f) praticar ato fraudulento na execução do contrato;
- g) comportar-se de modo inidôneo ou cometer fraude de qualquer natureza;
- h) praticar ato lesivo previsto no art. 5º da Lei nº 12.846, de 1º de agosto de 2013.

8.4. Serão aplicadas ao Contratado que incorrer nas infrações acima descritas as seguintes sanções:

8.4.1 Advertência, quando o Contratado der causa à inexecução parcial do contrato, sempre que não se justificar a imposição de penalidade mais grave;

8.4.2. Impedimento de licitar e contratar, quando praticadas as condutas descritas nas alíneas “b”, “c” e “d” do subitem acima, sempre que não se justificar a imposição de penalidade mais grave;

8.4.3. Declaração de inidoneidade para licitar e contratar, quando praticadas as condutas descritas nas alíneas “e”, “f”, “g” e “h” do subitem acima, bem como nas alíneas “b”, “c” e “d”, que justifiquem a imposição de penalidade mais grave.

8.4.4. Multa:

8.4.4.1. Moratória, para as infrações descritas no item “d”, de **1% (um por cento)** por dia de atraso injustificado sobre o valor da parcela inadimplida, até o limite de **10(dez)** dias

8.4.4.2. Moratória de 0,07% (sete centésimos por cento) por dia de atraso injustificado sobre o valor total do contrato, até o máximo de 2% (dois por cento), pela inobservância do prazo fixado para apresentação, suplementação ou reposição da garantia;

8.4.4.2.1. O atraso superior a 25 (vinte e cinco) dias para apresentação, suplementação ou reposição da garantia autoriza a Administração a promover a extinção do contrato por descumprimento ou cumprimento irregular de suas cláusulas, conforme dispõe o inciso I do art. 137 da Lei n. 14.133, de 2021.

8.4.4.3. Compensatória, para as infrações descritas acima alíneas “e” a “h” de **1% (um por cento)** a **5% (cinco por cento)** do valor da contratação.

8.4.4.4. Compensatória, para a inexecução total do contrato prevista acima na alínea “c”, de **10% (dez por cento)** a **20% (vinte por cento)** do valor da contratação.

8.4.4.5. Compensatória, para a infração descrita acima na alínea “b”, de **5% (cinco por cento)** a **10% (dez por cento)** do valor da contratação.

8.4.4.6. Compensatória, em substituição à multa moratória para a infração descrita acima na alínea “d”, de **5% (cinco por cento)** a **10% (dez por cento)** do valor da contratação.

8.4.4.7. Compensatória, para a infração descrita acima na alínea “a”, de **5% (cinco por cento)** a **10% (dez por cento)** do valor da contratação, ressalvadas as seguintes infrações também enquadráveis nessa alínea:

8.4.4.7.1. INDICAR ITENS ESPECÍFICOS DE INEXECUÇÃO PARCIAL QUE JUSTIFIQUEM PENALIDADE DIVERSA;

8.5. A aplicação das sanções previstas neste Termo de Referência não exclui, em hipótese alguma, a obrigação de reparação integral do dano causado ao Contratante.

8.6. Todas as sanções previstas neste Termo de Referência poderão ser aplicadas cumulativamente com a multa.

8.7. Antes da aplicação da multa será facultada a defesa do interessado no prazo de 15 (quinze) dias úteis, contado da data de sua intimação.

8.8. Se a multa aplicada e as indenizações cabíveis forem superiores ao valor do pagamento eventualmente devido pelo Contratante ao Contratado, além da perda desse valor, a diferença será descontada da garantia prestada ou será cobrada judicialmente.

8.9. A multa poderá ser recolhida administrativamente no prazo máximo de 30 (trinta) dias, a contar da data do recebimento da comunicação enviada pela autoridade competente.

8.10. A aplicação das sanções realizar-se-á em processo administrativo que assegure o contraditório e a ampla defesa ao Contratado, observando-se o procedimento previsto no caput e parágrafos do art. 158 da Lei nº 14.133, de 2021, para as penalidades de impedimento de licitar e contratar e de declaração de inidoneidade para licitar ou contratar.

8.10.1. Para a garantia da ampla defesa e contraditório, as notificações serão enviadas eletronicamente para os endereços de e-mail informados na proposta comercial, bem como os cadastrados pela empresa no SICAF.

8.10.2. Os endereços de e-mail informados na proposta comercial e/ou cadastrados no SICAF serão considerados de uso contínuo da empresa, não cabendo alegação de desconhecimento das comunicações a eles comprovadamente enviadas.

8.11. Na aplicação das sanções serão considerados:

8.11.1. a natureza e a gravidade da infração cometida;

8.11.2. as peculiaridades do caso concreto;

8.11.3. as circunstâncias agravantes ou atenuantes;

8.11.4. os danos que dela provierem para o Contratante; e

8.11.5. a implantação ou o aperfeiçoamento de programa de integridade, conforme normas e orientações dos órgãos de controle.

8.12. Os atos previstos como infrações administrativas na Lei nº 14.133, de 2021, ou em outras leis de licitações e contratos da Administração Pública que também sejam tipificados como atos lesivos na Lei nº 12.846, de 2013, serão apurados e julgados conjuntamente, nos mesmos autos, observados o rito procedimental e autoridade competente definidos na referida Lei.

8.13. A personalidade jurídica do Contratado poderá ser desconsiderada sempre que utilizada com abuso do direito para facilitar, encobrir ou dissimular a prática dos atos ilícitos previstos neste Termo de Referência ou para provocar confusão patrimonial, e, nesse caso, todos os efeitos das sanções aplicadas à pessoa jurídica serão estendidos aos seus administradores e sócios com poderes de administração, à pessoa jurídica sucessora ou à empresa do mesmo ramo com relação de coligação ou controle, de fato ou de direito, com o Contratado, observados, em todos os casos, o contraditório, a ampla defesa e a obrigatoriedade de análise jurídica prévia.

8.14. O Contratante deverá, no prazo máximo de 15 (quinze) dias úteis, contado da data de aplicação da sanção, informar e manter atualizados os dados relativos às sanções por ela aplicadas, para fins de publicidade no Cadastro Nacional de Empresas Inidôneas e Suspensas (CEIS) e no Cadastro Nacional de Empresas Punidas (CNEP), instituídos no âmbito do Poder Executivo Federal.

8.14.1. As penalidades serão obrigatoriamente registradas no SICAF.

8.15. As sanções de impedimento de licitar e contratar e declaração de inidoneidade para licitar ou contratar são passíveis de reabilitação na forma do art. 163 da Lei nº 14.133, de 2021.

8.16. Os débitos do Contratado para com a Administração Contratante, resultantes de multa administrativa e/ou indenizações, não inscritos em dívida ativa, poderão ser compensados, total ou parcialmente, com os créditos devidos pelo referido órgão decorrentes deste mesmo contrato ou de outros contratos administrativos que o Contratado possua com o mesmo órgão ora Contratante, na forma da Instrução Normativa SEGES/ME nº 26, de 13 de abril de 2022.

9. CRITÉRIOS DE MEDIÇÃO E DE PAGAMENTO

9.1. Recebimento do Objeto

9.1.1. Os bens serão recebidos provisoriamente, de forma sumária, no ato da entrega, juntamente com a Nota Fiscal ou instrumento de cobrança equivalente, pelo responsável pelo acompanhamento e fiscalização do contrato, para efeito de posterior verificação de sua conformidade com as especificações constantes neste Termo de Referência e na proposta da CONTRATADA.

9.1.2. O recebimento provisório não implica aceitação definitiva do objeto, constituindo etapa preliminar para verificação técnica.

9.2. Critérios de Medição

9.2.1. A medição da execução contratual será realizada com base em **critérios objetivos, mensuráveis e previamente definidos**, vinculados:

- II – à conformidade técnica dos bens e serviços;
- II – ao cumprimento dos prazos de fornecimento e implantação;
- III – à efetiva disponibilização operacional da solução;
- IV – ao cumprimento dos níveis mínimos de serviço;

9.2.2. Para fins de medição, serão considerados os seguintes indicadores:

- I – disponibilidade da solução;
- II – cumprimento dos prazos de entrega e instalação;
- III – conformidade nos testes de aceitação.
- IV – tempo de resposta e solução de incidentes;

9.2.3. A medição será realizada, mediante relatório de desempenho elaborado pela CONTRATADA e validado pela fiscalização do contrato.

9.3. Rejeição e Correção

9.3.1. Os bens poderão ser rejeitados, no todo ou em parte, inclusive antes do recebimento provisório, quando em desacordo com as especificações, devendo ser substituídos no prazo de até 15 (quinze) dias, às expensas da CONTRATADA, sem prejuízo da aplicação de penalidades.

9.3.2. A rejeição implicará a não medição da parcela correspondente até sua regularização.

9.4. Recebimento Definitivo

9.4.1. O recebimento definitivo ocorrerá no prazo de até 10 (dez) dias úteis, contados da apresentação da Nota Fiscal, após:

- I – verificação da conformidade técnica do objeto;
- II – aprovação nos testes definidos no item 4.3;
- III – validação dos indicadores de desempenho;
- IV – inexistência de inconformidades críticas.

9.4.2. O recebimento definitivo constitui condição para reconhecimento da execução para fins de pagamento.

9.5. Medição por Desempenho

9.5.1. O valor a ser pago será calculado com base na entrega dos bens pela CONTRATADA, em conformidade com os níveis mínimos de serviço estabelecidos no item 7.31.

9.5.2. O não atendimento aos níveis mínimos de serviço e especificações dos bens implicará aplicação automática de glosas, conforme item 7.31.

9.5.3. A medição considerará exclusivamente os bens efetivamente entregues, inspecionados e aceitos pela Administração.

9.6. Liquidação da Despesa

9.6.1. Recebida a Nota Fiscal, iniciar-se-á o prazo de até 10 (dez) dias úteis para fins de liquidação, após a validação da medição e do desempenho contratual.

9.6.2. A liquidação ficará condicionada à:

- I – comprovação da execução do objeto;
- II – validação dos indicadores de desempenho;
- III – verificação da regularidade fiscal da CONTRATADA;
- IV – inexistência de pendências técnicas.

9.6.3. Havendo inconsistências, o prazo ficará suspenso até a regularização, sem ônus para a Administração.

9.7. Pagamento

9.7.1. O pagamento será realizado com base na medição do desempenho, observando:

- I – os equipamentos forma efetivamente entregues;
- II – o cumprimento dos níveis mínimos de serviço;
- III – a aplicação de eventuais glosas e penalidades.

9.7.2. O pagamento estará diretamente vinculado ao desempenho da CONTRATADA, podendo sofrer reduções proporcionais em caso de descumprimento dos SLAs.

9.7.3. Em caso de execução parcial, o pagamento será proporcional à parcela efetivamente executada e aceita.

9.8. Regularidade Fiscal e Condições para Pagamento

9.8.1. O pagamento ficará condicionado à comprovação da regularidade fiscal, mediante consulta ao SICAF ou documentação equivalente.

9.8.2. A irregularidade fiscal não impede o pagamento pelos serviços efetivamente prestados, mas poderá ensejar medidas administrativas cabíveis.

9.9. Disposições Gerais

9.9.1. O recebimento provisório ou definitivo não exclui a responsabilidade da CONTRATADA quanto à qualidade, segurança e desempenho do objeto.

9.9.2. As atividades de instalação e configuração são condição indispensável para fins de aceitação e medição.

Prazo de pagamento

9.19. O pagamento será efetuado no prazo de até 10 (dez) dias úteis contados da finalização da liquidação da despesa, conforme seção anterior, nos termos da Instrução Normativa SEGES/ME nº 77, de 2022.

9.20. No caso de atraso pelo Contratante, os valores devidos ao Contratado serão atualizados monetariamente entre o termo final do prazo de pagamento até a data de sua efetiva realização, mediante aplicação do índice IPCA (Índice de Preços ao Consumidor Amplo) de correção monetária.

Forma de pagamento

9.21. O pagamento será realizado por meio de ordem bancária, para crédito em banco, agência e conta corrente indicados pelo Contratado.

9.22. Será considerada data do pagamento o dia em que constar como emitida a ordem bancária para pagamento.

9.23. Quando do pagamento, será efetuada a retenção tributária prevista na legislação aplicável.

9.24. Independentemente do percentual de tributo inserido na planilha, quando houver, serão retidos na fonte, quando da realização do pagamento, os percentuais estabelecidos na legislação vigente.

9.25. O Contratado regularmente optante pelo Simples Nacional, nos termos da Lei Complementar nº 123, de 2006, não sofrerá a retenção tributária quanto aos impostos e contribuições abrangidos por aquele regime. No entanto, o pagamento ficará condicionado à apresentação de comprovação, por meio de documento oficial, de que faz jus ao tratamento tributário favorecido previsto na referida Lei Complementar.

Antecipação de pagamento

9.26. A presente contratação não se aplicará antecipação de pagamento (parcial/total).

Cessão de Crédito

9.27. As cessões de crédito dependerão de prévia aprovação do Contratante.

9.27.1. A eficácia da cessão de crédito, em relação à Administração, está condicionada à celebração de termo aditivo ao contrato administrativo.

9.27.2. Sem prejuízo do regular atendimento da obrigação contratual de cumprimento de todas as condições de habilitação por parte do Contratado (cedente), a celebração do aditamento de cessão de crédito e a realização dos pagamentos respectivos também se condicionam à regularidade fiscal e trabalhista do cessionário, bem como à certificação de que o cessionário não se encontra impedido de licitar e contratar com o Poder Público, conforme a legislação em vigor, ou de receber benefícios ou incentivos fiscais ou creditícios, direta ou indiretamente, conforme o art. 12 da Lei nº 8.429, de 1992, nos termos do Parecer JL-01, de 18 de maio de 2020.

9.27.3. O crédito a ser pago à cessionária é exatamente aquele que seria destinado à cedente (Contratado) pela execução do objeto contratual, restando absolutamente incólumes todas as defesas e exceções ao pagamento e todas as demais cláusulas exorbitantes ao direito comum aplicáveis no regime jurídico de direito público incidente sobre os contratos administrativos, incluindo a possibilidade de pagamento em conta vinculada ou de pagamento pela efetiva comprovação do fato gerador, quando for o caso, e o desconto de multas, glosas e prejuízos causados à Administração.

9.27.4. A cessão de crédito não afetará a execução do objeto contratado, que continuará sob a integral responsabilidade do Contratado.

9.28. O disposto nesta seção não afeta as operações de crédito de que trata a Instrução Normativa SEGES/MGI nº 82, de 21 de fevereiro de 2025, as quais ficam por esta regidas.

Reajuste

9.29. Os preços inicialmente contratados são fixos e irredutíveis no prazo de um ano contado da data limite para a apresentação das propostas.

9.30. Após o interregno de um ano, e independentemente de pedido do contratado, os preços iniciais serão reajustados, mediante a aplicação, pelo contratante, do Índice de Custos de Tecnologia da Informação - ICTI, mantido pela Fundação Instituto de Pesquisa Econômica Aplicada - IPEA, exclusivamente para as obrigações iniciadas e concluídas após a ocorrência da anualidade.

9.31. Nos reajustes subsequentes ao primeiro, o interregno mínimo de um ano será contado a partir dos efeitos financeiros do último reajuste.

9.32. No caso de atraso ou não divulgação do(s) índice (s) de reajustamento, o Contratante pagará ao Contratado a importância calculada pela última variação conhecida, liquidando a diferença correspondente tão logo seja(m) divulgado(s) o(s) índice(s) definitivo(s).

9.33. Nas aferições finais, o(s) índice(s) utilizado(s) para reajuste será(ão), obrigatoriamente, o(s) definitivo(s).

9.34. Caso o(s) índice(s) estabelecido(s) para reajustamento venha(m) a ser extinto(s) ou de qualquer forma não possa(m) mais ser utilizado(s), será(ão) adotado(s), em substituição, o(s) que vier(em) a ser determinado(s) pela legislação então em vigor.

9.35. Na ausência de previsão legal quanto ao índice substituto, as partes elegerão novo índice oficial, para reajustamento do preço do valor remanescente, por meio de termo aditivo.

9.36. O reajuste será realizado por apostilamento.

10. FORMA E CRITÉRIOS DE SELEÇÃO DO FORNECEDOR E FORMA DE FORNECIMENTO

Forma de seleção e critério de julgamento da proposta

10.1. O critério de julgamento da proposta é o menor preço global. As regras de desempate entre propostas são as discriminadas no edital.

Forma de fornecimento

10.2. O fornecimento do objeto será integral e as entregas de acordo com o cronograma físico financeiro.

Critérios de aceitabilidade de preços

10.3 Em se tratando de contratação para registro de preços, caso adotado o critério de julgamento de menor preço ou de maior desconto por grupo de itens, o critério de aceitabilidade de preços unitários máximos será:

10.4 Valores unitários: conforme planilha de composição de preços anexa ao edital OU tabela constante no item 1.5 deste Termo de Referência

Exigências de habilitação

10.5. As exigências de habilitação estabelecidas neste Termo de Referência têm por finalidade assegurar que a futura contratada detenha capacidade jurídica, técnica, operacional e econômico-financeira compatível com a complexidade do objeto, em conformidade com a Lei nº 14.133/2021 e com as diretrizes da Instrução Normativa SGD/ME nº 94 /2022.

10.6. Considerando que a contratação envolve solução integrada de infraestrutura de Tecnologia da Informação e Comunicação (TIC), com fornecimento de bens e prestação de serviços, as exigências de habilitação foram definidas com base nos princípios da proporcionalidade, razoabilidade, competitividade e vinculação ao objeto, limitando-se ao estritamente necessário para garantir a adequada execução contratual. Para fins de habilitação, deverá o interessado comprovar os seguintes requisitos:

Habilitação jurídica

10.6.1. pessoa física: cédula de identidade (RG) ou documento equivalente que, por força de lei, tenha validade para fins de identificação em todo o território nacional.

10.6.2. Empresário individual: inscrição no Registro Público de Empresas Mercantis, a cargo da Junta Comercial da respectiva sede;

10.6.3. Microempreendedor Individual - MEI: Certificado da Condição de Microempreendedor Individual - CCMEI, cuja aceitação ficará condicionada à verificação da autenticidade no sítio <https://www.gov.br/empresas-e-negocios/pt-br/empreendedor>;

10.6.4. sociedade empresária, sociedade limitada unipessoal – SLU ou sociedade identificada como empresa individual de responsabilidade limitada - EIRELI: inscrição do ato constitutivo, estatuto ou contrato social no Registro Público de Empresas Mercantis, a cargo da Junta Comercial da respectiva sede, acompanhada de documento comprobatório de seus administradores.

10.6.5. sociedade empresária estrangeira: portaria de autorização de funcionamento no Brasil, publicada no Diário Oficial da União e arquivada na Junta Comercial da unidade federativa onde se localizar a filial, agência, sucursal ou estabelecimento, a qual será considerada como sua sede, conforme Instrução Normativa DREI/ME n.º 77, de 18 de março de 2020;

10.6.6. sociedade simples: inscrição do ato constitutivo no Registro Civil de Pessoas Jurídicas do local de sua sede, acompanhada de documento comprobatório de seus administradores;

10.6.7. filial, sucursal ou agência de sociedade simples ou empresária: inscrição do ato constitutivo da filial, sucursal ou agência da sociedade simples ou empresária, respectivamente, no Registro Civil das Pessoas Jurídicas ou no Registro Público de Empresas Mercantis onde opera, com averbação no Registro onde tem sede a matriz;

10.6.8. sociedade cooperativa: ata de fundação e estatuto social, com a ata da assembleia que o aprovou, devidamente arquivado na Junta Comercial ou inscrito no Registro Civil das Pessoas Jurídicas da respectiva sede, além do registro de que trata o art. 107 da Lei nº 5.764, de 16 de dezembro 1971.

10.6.9. Os documentos apresentados deverão estar acompanhados de todas as alterações ou da consolidação respectiva.

Habilitação fiscal, social e trabalhista

10.6.10. Prova de inscrição no Cadastro Nacional de Pessoas Jurídicas ou no Cadastro de Pessoas Físicas, conforme o caso;

10.6.11. Prova de regularidade fiscal perante a Fazenda Nacional, mediante apresentação de certidão expedida conjuntamente pela Secretaria da Receita Federal do Brasil (RFB) e pela Procuradoria-Geral da Fazenda Nacional (PGFN), referente a todos os créditos tributários federais e à Dívida Ativa da União (DAU) por elas administrados, inclusive aqueles relativos à Seguridade Social, nos termos da Portaria Conjunta nº 1.751, de 02 de outubro de 2014, do Secretário da Receita Federal do Brasil e da Procuradora-Geral da Fazenda Nacional;

10.6.12. Prova de regularidade com o Fundo de Garantia do Tempo de Serviço (FGTS);

10.6.13. Prova de inexistência de débitos inadimplidos perante a Justiça do Trabalho, mediante a apresentação de certidão negativa ou positiva com efeito de negativa, nos termos do Título VII-A da Consolidação das Leis do Trabalho, aprovada pelo Decreto-Lei nº 5.452, de 1º de maio de 1943;

10.6.14. Prova de inscrição no cadastro de contribuintes Estadual ou Distrital relativo ao domicílio ou sede do fornecedor, pertinente ao seu ramo de atividade e compatível com o objeto contratual;

10.6.15. Prova de regularidade com a Fazenda Estadual ou Distrital do domicílio ou sede do fornecedor, relativa à atividade em cujo exercício contrata ou concorre;

10.6.16. Caso o fornecedor seja considerado isento dos tributos relacionados ao objeto contratual, deverá comprovar tal condição mediante a apresentação de declaração da Fazenda respectiva do seu domicílio ou sede, ou outra equivalente, na forma da lei.

10.6.17. O fornecedor enquadrado como microempreendedor individual que pretenda auferir os benefícios do tratamento diferenciado previstos na Lei Complementar n. 123, de 2006, estará dispensado da prova de inscrição nos cadastros de contribuintes estadual e municipal.

Qualificação Econômico-Financeira

10.6.18. certidão negativa de insolvência civil expedida pelo distribuidor do domicílio ou sede do interessado, caso se trate de pessoa física, desde que admitida a sua participação na licitação/contratação, ou de sociedade simples;

10.6.19. certidão negativa de falência expedida pelo distribuidor da sede do fornecedor;

10.6.20. balanço patrimonial, demonstração de resultado de exercício e demais demonstrações contábeis dos dois últimos exercícios sociais, já exigíveis e apresentados na forma da lei, comprovando, índices de Liquidez Geral (LG), Liquidez Corrente (LC), e Solvência Geral (SG) superiores a 1 (um), obtidos por meio da aplicação das seguintes fórmulas:

LG =

Ativo Circulante + Realizável a Longo Prazo

Passivo Circulante + Passivo Não Circulante

SG =

Ativo Total

Passivo Circulante + Passivo Não Circulante

LC =

Ativo Circulante

Passivo Circulante

10.6.21. Caso a empresa interessada apresente resultado inferior ou igual a 1 (um) em qualquer dos índices de Liquidez Geral (LG), Solvência Geral (SG) e Liquidez Corrente (LC), será exigido para fins de habilitação capital mínimo de 3% (três por cento) do valor total estimado da contratação

10.6.22. Os indicadores fixados acima deverão ser atingidos em cada um dos dois últimos exercícios sociais, sob pena de inabilitação;

10.6.23. Os documentos referidos acima limitar-se-ão ao último exercício no caso de a pessoa jurídica ter sido constituída há menos de 2 (dois) anos;

10.6.24. Os documentos referidos acima deverão ser exigidos com base no limite definido pela Receita Federal do Brasil para transmissão da Escrituração Contábil Digital - ECD ao Sped.

10.6.25. As empresas criadas no exercício financeiro da licitação/contratação deverão atender a todas as exigências da habilitação e poderão substituir os demonstrativos contábeis pelo balanço de abertura.

10.6.26. O atendimento dos índices econômicos previstos neste item deverá ser atestado mediante declaração assinada por profissional habilitado da área contábil, apresentada pelo fornecedor.

Qualificação Técnica

10.6.27. Comprovação de aptidão para fornecimento de bens similares de complexidade tecnológica e operacional equivalente à 50% (cinquenta por cento) do objeto desta contratação, ou com o item pertinente, por meio da apresentação de certidões ou atestados, por pessoas jurídicas de direito público ou privado, ou regularmente emitido (s) pelo conselho profissional competente, quando for o caso.

10.6.28. Para fins da comprovação de que trata este subitem, os atestados deverão dizer respeito a contratos executados com as seguintes características mínimas:

- 10.6.28.1. Fornecimento com instalação e implantação de Servidores
- 10.6.28.2. Fornecimento com instalação e implantação de equipamentos e solução de backup.

10.6.28.3. Fornecimento de equipamentos e serviços relacionados a equipamentos de armazenamento de dados

10.6.28.4. Será admitida, para fins de comprovação de quantitativo mínimo, a apresentação e o somatório de diferentes atestados executados de forma concomitante.

10.6.29. Os atestados de capacidade técnica poderão ser apresentados em nome da matriz ou da filial do fornecedor.

10.6.30 . O fornecedor disponibilizará todas as informações necessárias à comprovação da legitimidade dos atestados, apresentando, quando solicitado pela Administração, cópia do contrato que deu suporte à contratação, endereço atual da Contratante e local em que foi executado o objeto contratado, dentre outros documentos.

10.6.31. Caso admitida a participação de cooperativas, será exigida a seguinte documentação complementar:

10.6.31.1. A relação dos cooperados que atendem aos requisitos técnicos exigidos para a contratação e que executarão o contrato, com as respectivas atas de inscrição e a comprovação de que estão domiciliados na localidade da sede da cooperativa, respeitado o disposto nos arts. 4º, inciso XI, 21, inciso I e 42, §§2º a 6º da Lei n. 5.764, de 1971;

10.6.31.2. A declaração de regularidade de situação do contribuinte individual – DRSCI, para cada um dos cooperados indicados;

10.6.31.3. A comprovação do capital social proporcional ao número de cooperados necessários à prestação do serviço; 10.33.4. O registro previsto na Lei n. 5.764, de 1971, art. 107;

10.6.31.4. A comprovação de integração das respectivas quotas-partes por parte dos cooperados que executarão o contrato; e

10.6.31.5. Os seguintes documentos para a comprovação da regularidade jurídica da cooperativa:

- ata de fundação;
- estatuto social com a ata da assembleia que o aprovou;
- regimento dos fundos instituídos pelos cooperados, com a ata da assembleia;
- editais de convocação das três últimas assembleias gerais extraordinárias;
- três registros de presença dos cooperados que executarão o contrato em assembleias gerais ou nas reuniões seccionais e ata da sessão que os cooperados autorizaram a cooperativa a contratar o objeto da licitação;
- última auditoria contábil-financeira da cooperativa, conforme dispõe o art. 112 da Lei n.5.764, de 1971, ou uma declaração, sob as penas da lei, de que tal auditoria não foi exigida pelo órgão fiscalizador;

Disposições gerais sobre habilitação

10.6.32 Quando permitida a participação de empresas estrangeiras que não funcionem no País, as exigências de habilitação serão atendidas mediante documentos equivalentes, inicialmente apresentados em tradução livre.

10.6.33 Na hipótese de o fornecedor ser empresa estrangeira que não funcione no País, para assinatura do contrato ou da ata de registro de preços ou do aceite do instrumento equivalente, os documentos exigidos para a habilitação serão traduzidos por tradutor juramentado no País e apostilados nos termos do disposto no Decreto nº 8.660, de 29 de janeiro de 2016, ou de outro que venha a substituí-lo, ou consularizados pelos respectivos consulados ou embaixadas.

10.6.34 Não serão aceitos documentos de habilitação com indicação de CNPJ/CPF diferentes, salvo aqueles legalmente permitidos.

10.6.35 Se o fornecedor for a matriz, todos os documentos deverão estar em nome da matriz, e se o fornecedor for a filial, todos os documentos deverão estar em nome da filial, exceto para atestados de capacidade técnica, e no caso daqueles documentos que, pela própria natureza, comprovadamente, forem emitidos somente em nome da matriz.

10.6.36 Serão aceitos registros de CNPJ de fornecedor matriz e filial com diferenças de números de documentos pertinentes ao CND e ao CRF/FGTS, quando for comprovada a centralização do recolhimento dessas contribuições.

11. ESTIMATIVAS DO VALOR DA CONTRATAÇÃO

[Conteúdo Sigiloso | Justificativa: 11.1. O custo estimado da contratação possui caráter sigiloso e será tornado público apenas e imediatamente após o julgamento das propostas. 11.1.1. Quando as propostas permanecerem com preços acima do orçamento estimado, o custo estimado da contratação será tornado público após a fase de lances. 11.1.2 O orçamento estimado é definido como preço máximo a ser contratado por essa Administração. 11.2. A estimativa de custo levou em consideração o risco envolvido na contratação e sua alocação entre Contratante e Contratado, conforme especificado na matriz de risco constante do Contrato.]

Valor R\$: [REDACTED]

11.1 A estimativa do custo total da contratação foi elaborada com base nas definições da Instrução Normativa SEGES /ME nº 65, de 7 de julho de 2021, e nas disposições aplicáveis às soluções de Tecnologia da Informação e Comunicação contidas na Instrução Normativa SGD/ME nº 94, de 23 de dezembro de 2022.
11.2 O orçamento estimado é definido como preço máximo a ser contratado por essa Administração.
11.3 A estimativa de custo levou em consideração o risco envolvido na contratação e sua alocação entre Contratante e Contratado, conforme especificado na matriz de risco constante do Contrato.

Registro de Preços.

11.4 Os preços registrados poderão ser alterados ou atualizados em decorrência de eventual redução dos preços praticados no mercado ou de fato que eleve o custo dos bens, das obras ou dos serviços registrados, nas seguintes situações:

11.4.1 Em caso de força maior, caso fortuito ou fato do príncipe ou em decorrência de fatos imprevisíveis ou previsíveis de consequências incalculáveis, que inviabilizem a execução da ata tal como pactuada, nos termos do disposto na alínea “d” do inciso II do caput do art. 124 da Lei nº 14.133, de 2021;

11.4.2 Em caso de criação, alteração ou extinção de quaisquer tributos ou encargos legais ou superveniência de disposições legais, com comprovada repercussão sobre os preços registrados;

11.4.3 Serão reajustados os preços registrados, respeitada a contagem da anualidade e o índice previsto para a contratação; ou

11.4.4 Poderão ser repactuados, a pedido do interessado, conforme critérios definidos para a contratação.

12. ADEQUAÇÃO ORÇAMENTÁRIA

12.1 As despesas decorrentes da presente contratação correrão à conta de recursos específicos consignados no Orçamento Geral da União.

12.2. A indicação da dotação orçamentária fica postergada para o momento da assinatura do contrato ou instrumento equivalente.

13. DISPOSIÇÕES FINAIS

[Conteúdo Sigiloso | Justificativa: 11.1. O custo estimado da contratação possui caráter sigiloso e será tornado público apenas e imediatamente após o julgamento das propostas. 11.1.1. Quando as propostas permanecerem com preços acima do orçamento estimado, o custo estimado da contratação será tornado público após a fase de lances. 11.1.2 O orçamento estimado é definido como preço máximo a ser contratado por essa Administração. 11.2. A estimativa de custo levou em consideração o risco envolvido na contratação e sua alocação entre Contratante e Contratado, conforme especificado na matriz de risco constante do Contrato.]

13.1.As informações contidas neste Termo de Referência não são classificadas como sigilosas exceto o custo estimado da contratação, que possui caráter sigiloso até o julgamento das propostas.

13.2 As definições dos Ambientes de Implantação do Data Center são aquelas descritas no Anexo II deste Termo de Referência.

Cronograma Físico Financeiro

Fase de Implantação do Data Center	Período (Meses)	Evento de Medição / Marco de Entrega (Milestone)	Critério de Aceite Técnico (Fiscalização)	Peso %
Fase 1: Planejamento e Design	Mês 1	Entrega do Plano de Migração, Matriz de Riscos e Topologia Lógica da Nova Rede homologados.	Aprovação formal pela Equipe de Planejamento da Contratação (TIC).	0%
Fase 2: Entrega Física (Hardware) - Ambiente de Produção	Mês 2	Recebimento dos itens 1 a 5 (ambiente de produção) dos equipamentos no Datacenter (Servidores, Storages, Switches, Licenças).	Conferência de <i>Part Numbers</i> , números de série e Termo de Recebimento Provisório dos bens.	69%
Fase 3: <i>Instalação e Configuração, Migração de Dados e Cargas - Ambiente de Produção</i>	Mês 3	Montagem física nos racks dos itens 1 a 5(ambiente de produção) (<i>Rack & Stack</i>), cabeamento estruturado ativo e configuração dos Sistemas Operacionais /Hypervisors. Migração de Máquinas Virtuais (VMs), bases de dados e volumes de armazenamento do ambiente antigo para o novo.	Validação de conectividade física, inventário lógico e testes de gerência. Janelas de manutenção concluídas com sucesso e validação de funcionamento pelos donos dos sistemas.	1%
Fase 4: <i>Entrega Física (Hardware) - Ambiente PACS e Backup da Produção</i>	Mês 4	Recebimento dos itens 6 a 9 (PACS e BACKUP) dos equipamentos no Datacenter (Servidores, Storages, Switches, Licenças).	Conferência de <i>Part Numbers</i> , números de série e Termo de Recebimento Provisório dos bens.	29%
Fase 5: <i>Instalação e Configuração, Migração de Dados e Cargas - Ambiente PACS e Backup da Produção</i>	Mês 5	Montagem física nos racks dos itens 6 a 9(PACS e BACKUP) (<i>Rack & Stack</i>), cabeamento estruturado ativo e configuração dos Sistemas	Validação de conectividade física, inventário lógico e testes de gerência. Janelas de manutenção concluídas com sucesso e validação de funcionamento pelos donos dos sistemas.	1%
Fase 6:		Acompanhamento do novo ambiente em produção,	Relatório de conformidade, entrega de certificados de	

Operação Assistida e Decommissioning	Mês 6	treinamento da equipe interna, desligamento e sanitização dos equipamentos antigos.	destruição segura de dados (LGPD) e Termo de Recebimento Definitivo.	0%
--------------------------------------	-------	---	---	----

Integrante Requisitante	Integrante Técnico	Integrante Administrativo
Daniel Dias Soares	Geraldo Gabriel Crelier dos Santos	Renata Emanuelle Vasconcellos Anhon
Agente Administrativo	Auxiliar Operacional de Serviços Diversos	Auxiliar Operacional de Serviços Diversos
1742407	1531384	1530673

Autoridade Máxima da Área de TIC
Daniel Dias Soares
Agente Administrativo
1742407

Rio de Janeiro, 25 de Maio de 2026.

Aprovo,

Autoridade Competente
Aurora Felice Castro Issa
Diretora
Matrícula 2188092

14. Responsáveis

Todas as assinaturas eletrônicas seguem o horário oficial de Brasília e fundamentam-se no §3º do Art. 4º do [Decreto nº 10.543, de 13 de novembro de 2020](#).

RENATA EMANUELLE VASCONCELLOS ANHON
Integrante Administrativo



Assinou eletronicamente em 12/06/2026 às 16:21:03.

GERALDO GABRIEL CRELIER DOS SANTOS

Integrante Técnico



Assinou eletronicamente em 12/06/2026 às 16:25:06.

DANIEL DIAS SOARES

Integrante Requisitante



Assinou eletronicamente em 12/06/2026 às 16:20:35.

Lista de Anexos

Atenção: Apenas arquivos nos formatos ".pdf", ".txt", ".jpg", ".jpeg", ".gif" e ".png" enumerados abaixo são anexados diretamente a este documento.

- Anexo I - TERMO DE COMPROMISSO DE MANUTENCAO DE SIGILO E CONFIDENCIALIDADE(2026).pdf (433.21 KB)
- Anexo II - Definicao dos Ambientes de Implantacao do Data Center.pdf (192.51 KB)



Ministério da Saúde
Secretaria de Atenção Especializada à Saúde
Instituto Nacional de Cardiologia
Serviço de Apoio a Gestão da Integridade

TERMO DE COMPROMISSO DE MANUTENÇÃO DE SIGILO E CONFIDENCIALIDADE	
IDENTIFICAÇÃO	
Contrato INC nº	
Objeto:	
Fiscal do Contrato:	Matrícula:
Contratante:	
Contratada:	CNPJ:
Preposto da Contratada:	CPF:

TERMO DE COMPROMISSO
<p>Na qualidade de REPRESENTANTE LEGAL da empresa acima identificada e ora CONTRATADA, ACEITO as regras, condições e obrigações constantes deste TERMO DE COMPROMISSO DE MANUTENÇÃO DE SIGILO E CONFIDENCIALIDADE, que tem por objetivo prover a necessária e adequada proteção às informações restritas de propriedade exclusiva do Ministério da Saúde.</p> <p>1. A CONTRATADA compromete-se a não reproduzir e/ou dar conhecimento a terceiros, sem anuência formal e expressa do Instituto Nacional de Cardiologia - INC, das informações reveladas em razão da execução das atividades previstas no contrato.</p> <p>2. A CONTRATADA reconhece que, em razão da prestação de serviços ao INC, tem acesso a informações restritas, que pertencem ao INC.</p> <p>3. Considera-se INFORMAÇÃO RESTRITA toda e qualquer informação à qual a CONTRATADA venha a ter acesso durante ou em razão da execução do contrato celebrado, diretamente ou através de seus empregados, prepostos ou prestadores de serviço, seja a informação apresentada de forma escrita ou oral, ou observada de qualquer outro modo, tangível ou intangível, incluindo, mas não se limitando técnicas, projetos, especificações, desenhos, cópias, diagramas, fórmulas, modelos, amostras, fluxogramas, croquis, fotografias, plantas, programas de computador, discos, disquetes, pen drives, memórias de resultado, flash cards, fitas, contratos, planos de negócios, processos, projetos, conceitos de produto, especificações, amostras de ideia, clientes, nomes de revendedores e/ou distribuidores, preços e custos, definições e informações mercadológicas, invenções e ideias, outras informações técnicas, financeiras ou comerciais, entre outras obtidas em razão da execução das atividades previstas no contrato.</p>

4. Em caso de dúvida acerca da natureza confidencial de determinada informação, a CONTRATADA deverá mantê-la sob sigilo até que a dúvida seja expressamente esclarecida pelo INC, e em hipótese alguma a ausência de manifestação expressa do INC poderá ser interpretada como liberação de quaisquer dos compromissos ora assumidos.

5. A CONTRATADA tem ciência de que as informações reveladas devem ficar limitadas ao conhecimento dos diretores, consultores, prestadores de serviços, colaboradores e/ou prepostos que estejam diretamente envolvidos nas discussões, análises, reuniões e demais atividades relativas à prestação de serviços ao INC, devendo cientificá-los da existência deste TERMO DE COMPROMISSO e da natureza confidencial das informações reveladas, e devendo ainda a CONTRATADA manter ou firmar acordos por escrito com seus diretores, consultores, prestadores de serviços, colaboradores e/ou prepostos, a fim de garantir o cumprimento de todas as disposições do presente Termo, podendo ser utilizado o modelo fornecido pelo INC.

6. A quebra de sigilo das informações reveladas, sem autorização expressa do INC, sujeitará a CONTRATADA ao pagamento ou recomposição de todas as perdas e danos sofridos pelo INC, inclusive os de ordem moral, bem como as responsabilidades civil e criminal respectivas, apuradas em processo judicial ou administrativo, podendo, inclusive, acarretar a rescisão do contrato firmado entre as partes, sem ônus para o INC.

7. A CONTRATADA obriga-se, perante o INC, a informar imediatamente qualquer violação das regras estabelecidas neste TERMO DE COMPROMISSO, da qual tenha tomado conhecimento ou que tenha ocorrido por sua ação ou omissão, independentemente da existência de dolo.

8. A CONTRATADA compromete-se, ao término do contrato, a devolver imediatamente ao INC todo e qualquer material de propriedade deste, inclusive registros de documentos de qualquer natureza que tenham sido criados, usados ou mantidos sob seu controle ou posse, bem como de seus empregados, prepostos ou prestadores de serviço, assumindo o compromisso de não utilizar qualquer informação considerada confidencial a que teve acesso em decorrência do vínculo contratual com o INC.

9. A CONTRATADA, na prestação de serviços do INC, compromete-se a cumprir o que está disposto nos seguintes normativos:

(i) Portaria Ministério da Saúde nº 271 de 27 de Janeiro de 2017 que dispõe sobre a Política de Segurança da Informação (PSI) no âmbito do Ministério da Saúde (MS) e seus Núcleos Estaduais.

(ii) Lei nº 13.709/2018 que institui a Política Geral de Privacidade e Proteção de Dados Pessoais, no âmbito do Ministério da Saúde (MS) e seus Núcleos Estaduais; e

10. O presente TERMO DE COMPROMISSO tem natureza irrevogável e irretratável, permanecendo em vigor a partir da data da assinatura do contrato entre o INC e a CONTRATADA.

11. Por estar de acordo, a CONTRATADA, por meio de seu representante, firma o presente TERMO DE COMPROMISSO DE MANUTENÇÃO DE SIGILO E CONFIDENCIALIDADE.

Rio de Janeiro, ____ de _____ de 2026, ou data da assinatura eletrônica.

CONTRATADA

Anexo II - Definição dos Ambientes de Implantação do Data Center

A aquisição da solução de Data Center On-Premise tem como objetivo atender às demandas do Instituto Nacional de Cardiologia, bem como promover a modernização de sua infraestrutura tecnológica. Nesse contexto, a solução de TIC para Data Center On-Premise será implementada com foco em três áreas principais:

1- Ambiente de Produção:

O ambiente de produção tem a função de hospedar, executar e sustentar todas as aplicações e dados críticos da organização com alta performance, conectividade e capacidade de armazenamento, servir como a plataforma principal de execução dos sistemas corporativos críticos da organização, onde todos os serviços de TI realmente “rodam” no dia a dia. Este ambiente é composto pelos seguintes itens:

- *Servidor Rack Tipo 1U – 2 Procs. / 256 GB RAM ;*
- *Servidor Rack Tipo 1U – 2 Procs. / 1.536 GB RAM;*
- *Switch L3 com 48 Portas Fixas 1/10/25GbE e 6 Portas 100GbE;*
- *Infraestrutura de Armazenamento de Dados.*

2- Ambiente PACS:

Ele funciona como o repositório central de imagens médicas do instituto, capaz de:

- Armazenar grandes volumes de exames de imagem;
- Garantir acesso rápido por médicos e sistemas clínicos;
- Escalar conforme crescimento do instituto;
- Proteger dados sensíveis de pacientes;
- Sustentar operação contínua de diagnóstico por imagem;

Este ambiente é composto pelo seguinte item: *Appliance Scale -Out NAS para Armazenamento de Dados*

3- Ambiente de Backup:

Trata-se de uma plataforma corporativa de proteção de dados com alta disponibilidade, deduplicação, replicação e recuperação de desastres (DR).

A função do ambiente de backup é proteger, armazenar e possibilitar a recuperação de dados e sistemas críticos de forma segura, automatizada e resiliente, em diferentes camadas de infraestrutura (física, virtual e aplicações). Este ambiente é composto pelos seguintes itens:

- *Servidor Rack Tipo 1U – 2 Procs / 256 GB RAM;*
- *Software de Proteção e Recuperação de Dados;*
- *Appliance de Proteção e Recuperação de Dados*