ANEXO I

TERMO DE REFERÊNCIA

Contratante: Fundação de Apoio ao Desenvolvimento da Computação Científica - FACC
Beneficiário: Fundação Biblioteca Nacional

1. OBJETO

1.1. O presente Termo de Referência tem por objeto à **Aquisição de Solução de Infraestrutura Hiperconvergente (HCI), com fornecimento de serviço de instalação e configuração, suporte, manutenção especializada e garantia de toda a solução pelo período de 60 meses e repasse de conhecimento,** conforme condições, quantidades e exigências estabelecidas neste instrumento.

2. JUSTIFICATIVA

A Fundação Biblioteca Nacional, fundação pública vinculada ao Ministério da Cultura, é o órgão responsável pela execução da política de captação, guarda, preservação e difusão da produção bibliográfica e documental do país, é a mais antiga instituição cultural do Estado brasileiro. Apontada pela Unesco como a oitava maior instituição do gênero no mundo, a Biblioteca Nacional, instituição precípua à memória nacional, guarda a mais abastada coleção bibliográfica da América Latina.

O acervo institucional tem aproximadamente nove milhões de itens e permanece em constante crescimento e atualização, incorporando materiais editados em quaisquer suportes e formatos, inclusive os digitais (cerca de 3 milhões), cuja captação e armazenamento mobilizam tecnologias especializadas.

De forma mais específica, em resposta às exigências impostas pelas demandas da sociedade contemporânea e diante da importância do conjunto bibliográfico e documental sob sua guarda, a Fundação Biblioteca Nacional busca permanentemente investir no aprimoramento dos mecanismos de segurança, preservação e difusão do patrimônio cultural: visa sua permanência através das gerações por meio da pesquisa e produção de conhecimento sobre o acervo e suas práticas; e da adoção de novas tecnologias que garantam ao cidadão o pleno direito de acesso ao conhecimento.

Através do portal da Biblioteca Nacional Digital (BNDigital) é possível acessar as imagens dos documentos

do acervo digitalizado, além de exposições virtuais, dossiês e artigos. A digitalização do acervo, convertendo-o em arquivos digitais de qualidade, tem como objetivo preservá-lo por longo prazo e compor a Biblioteca Nacional Digital.

O acesso ao conteúdo digital da FBN, pela BNDigital, atingiu em 2020 (no auge da pandemia) a marca dos 110 milhões de acessos. Em 2022 a média mensal de acessos superou os 7 milhões de acessos/mês. Até setembro /2022, a instituição atendeu mais de 70 mil pessoas; em seu canal do YouTube foram quase 30 mil visualizações das diversas atrações transmitidas. O passeio virtual pelo edifício principal, publicado em 15 de agosto/2022, atingiu em menos de um mês mais de 100 mil acessos. Inaugurada em 2006, a Biblioteca Nacional Digital é hoje uma referência no país e no exterior.

Marco no processo de digitalização e desburocratização, no âmbito do Plano de Transformação Digital do Governo Federal, foi lançada plataforma para o registo e averbação de obras do Escritório de Direitos Autorais (setor da FBN para registro autoral), o EDA. Em 03 de outubro de 2022 foi implantado o Balcão Virtual do EDA, que permite aos usuários o acesso eletrônico ao serviço prestado.

O uso da tecnologia da informação, tornou-se uma ferramenta fundamental para a execução dos serviços nas esferas públicas e privadas. Principalmente no que tange a qualidade dos serviços disponibilizados pela FBN de forma online e pela crescente dependência tecnológica em diversas áreas da Fundação.

O caráter essencial destes serviços, que pode ser comprovado pela hipótese de sua eventual paralisação, assegura a continuidade das atividades e realização dos trabalhos da área fim e meio, evitando impactos severos como a indisponibilidade de recursos: acesso à rede institucional, serviço de internet, correio eletrônico, backup, impressão, dentre outros. A continuidade dos serviços institucionais é um dos atributos principais a ser levado em conta pelos gestores, tendo em vista que a interrupção da prestação dos serviços públicos causaria transtornos aos cidadãos.

É primordial manter o atual estágio de maturidade dos serviços que, para assegurar um ambiente apto e produtivo de TIC, evoluiu através das diversas medidas que foram tomadas, a partir de experiências anteriores, com o objetivo de eliminar ou reduzir problemas causados por eventuais falhas no ambiente computacional, como por exemplo: os serviços mais críticos passaram a ser apoiados em equipamentos redundantes e o monitoramento de equipamentos, circuitos de comunicação e aplicações foram implantados com procedimentos e especificidades mais rigorosas de configuração.

Atualmente, a FBN enfrenta o desafio de contar com equipamentos de TI desgastados, obsoletos e sem garantia. Esses equipamentos apresentam riscos significativos para a continuidade operacional e a segurança das informações. A ausência de garantia implica que, em caso de falha, a manutenção ou substituição dos dispositivos seja onerosa, o que pode resultar em interrupções nas operações dos usuários e custos imprevistos.

Diante do cenário exposto, é crucial destacar a imperatividade e a relevância dos desafios inerentes à infraestrutura de TIC enfrentados pelo FBN. A utilização dos atuais equipamentos não apenas coloca a instituição em uma posição delicada, mas também a expõe a riscos substanciais tanto em termos operacionais quanto de segurança da informação.

Dessa forma, é imperativo que a FBN adote medidas proativas para lidar com essas vulnerabilidades, incluindo a busca por soluções de infraestrutura de TIC mais sustentáveis e controláveis, visando assegurar a estabilidade operacional e a integridade dos dados institucionais.

Nesse contexto, é altamente aconselhável a aquisição de uma solução abrangente que englobe computação, rede e virtualização. Essa recomendação é fundamentada na crescente complexidade dos ativos lógicos da FBN, atualmente hospedados no datacenter próprio. A adoção dessa solução apresenta-se como uma medida estratégica que pode contribuir de maneira substancial para o aprimoramento da infraestrutura de Tecnologia da Informação e Comunicação da FBN.

O cenário atual destaca a necessidade de lidar com os ativos físicos e lógicos da FBN, que estão alojados no datacenter da FBN. A integração de uma solução de computação, rede e virtualização, representa uma abordagem abrangente para gerenciar essa complexidade crescente de maneira eficaz. Essa solução proposta não apenas centraliza a gestão desses ativos, mas também simplifica os processos operacionais associados, promovendo uma administração mais eficiente e eficaz dos recursos de TIC.

Ao optar por essa solução, espera-se uma melhoria significativa na agilidade, flexibilidade, segurança e escalabilidade da infraestrutura de TIC da FBN. A integração desses elementos em uma única plataforma coesa não apenas modernizará a infraestrutura existente, mas também permitirá uma adaptação mais rápida e eficiente às demandas em constante mudança. Essa abordagem integrada não só aprimora o desempenho dos aplicativos e sistemas, mas também proporciona uma base sólida para a inovação

tecnológica contínua.

Portanto, a contratação desta solução abrangente é recomendada como uma estratégia essencial para enfrentar os desafios atuais e futuros relacionados à gestão dos ativos, contribuindo significativamente para a melhoria da infraestrutura de TIC, essa decisão visa a otimização dos recursos e a promoção de práticas mais eficazes no âmbito tecnológico da Fundação.

A visão técnica mostra que os componentes e serviços associados à solução a ser adquirida configuram um conjunto indissociável, composto pela interligação dos serviços que funcionam harmonicamente razão pela qual qualquer inconformidade de um desses serviços poderá fragilizar ou até inviabilizar o funcionamento adequado da solução, com o consequente impacto sobre a segurança dos equipamentos, mídias e dados de alta criticidade da instituição.

Sendo assim, a adjudicação do certame para um único vencedor, visa além dos aspectos já mencionados, resguardar a efetividade do processo de aquisição bem como garantir a continuidade do provimento de infraestrutura tecnológica para o cumprimento do papel institucional da FBN.

3. DESCRIÇÃO DO OBJETO E QUANTIDADE

LOTE	ITEM	OBJETO	QTD	MÉTRICA	Valor Unitário	Valor Total
1	1	Hardware para Infraestrutura Hiperconvergente (HCI), incluindo, suporte técnico "onsite" dentro da garantia de 60 meses.	4	Und.	R$ 250.000,00	R$ 1.000.000,00
	2	Software para HCI com subscrição e suporte 24x7 durante 60 meses, por núcleo de processamento (core).	192	Core	R$ 15.000,00	R$ 2.880.000,00
	3	Software para armazenamento de arquivos e objetos, com subscrição e suporte 24x7 durante 60 meses, por terabyte de dados.	1	Und.	R$ 30.000,00	R$ 30.000,00
	4	Switches TOR 48 portas, incluindo, serviço de implantação, configuração, repasse de conhecimento, suporte técnico "onsite" dentro da garantia de 60 meses.	2	Und.	R$ 150.000,00	R$ 300.000,00

	5	Implantação, configuração repasse de conhecimento	1	Und.	R$ 40.000,00	R$ 40.000,00
VALOR TOTAL ESTIMADO						**R$ 4.250.000,00**
Valor Total: Quatro milhões, duzentos e cinquenta mil reais.						

Tabela 01

4. CARACTERÍSTICAS, DETALHAMENTO E ESPECIFICAÇÕES TÉCNICAS DOS ITENS

4.1	**ESPECIFICAÇÕES TÉCNICAS DA SOLUÇÃO DE TIC**
4.1.1	Apresentar a composição de cada item do escopo de fornecimento, contendo marca, modelo, códigos, descritivo dos códigos, unidade, quantidades do conjunto, tudo com o objetivo de se identificar claramente quais os produtos e serviços estão sendo ofertados;
4.1.2	Apresentar documentação técnica (manuais e/ou catálogos do fabricante, em mídia eletrônica ou URL) comprovando o pleno atendimento a todos os requisitos técnicos, por meio de apresentação de uma planilha ponto a ponto com indicação de nome do documento e página que comprova o atendimento.
4.1.3	O proponente deve apresentar carta oficial de revenda autorizada pelo fabricante do equipamento ofertado para o certame em questão;
4.1.4	Não será aceita comprovação por carta do fabricante ou distribuidor ou da licitante;
4.2	**REQUISITOS DE INFRAESTRUTURA:**
4.2.1	A solução deverá prover uma infraestrutura hiperconvergente de alta disponibilidade. Não serão aceitas soluções ou funcionalidades implementadas via software ainda em fase de desenvolvimento, ou seja, aquelas que ainda não foram homologadas pelo fabricante para ambiente de produção.
4.2.2	**Cada equipamento da solução deverá ser fornecido com todos os componentes, incluindo appliances, licenças e subscrições, módulos, acessórios, conectores, cabos e adaptadores, bem como qualquer outro elemento de hardware ou software adicionais, de forma a atender plenamente os seguintes requisitos:**
4.2.2.1	Capacidade de processamento, memória RAM e conectividade de rede;
4.2.2.2	Funcionalidades de hipervisor para virtualização de computação;
4.2.2.3	Funcionalidades de virtualização da camada de redes da solução (SDN);
4.2.2.4	Funcionalidades de gerenciamento da solução;
4.2.2.5	A solução deve fornecer um dashboard centralizado para monitoramento em tempo real de vulnerabilidades e riscos, permitindo a visibilidade abrangente do ambiente. Ela deve permitir a identificação e priorização de ativos críticos, além de realizar análises contínuas de configurações e permissões. A solução também deve gerar relatórios detalhados sobre a postura de segurança do ambiente e fornecer recomendações de mitigação.
4.2.2.6	Funcionalidades de proteção de dados (backup) da solução;
4.2.2.7	Tanto o hardware quanto o software dessa solução deverão suportar pelo menos os seguintes Hipervisores:
4.2.2.8	Microsoft Hyper-V; VMware ESXi;
4.2.2.9	Hipervisor baseado em KVM, desde que distribuído e suportado pelo fabricante da solução hiperconvergente.

4.2.2.10	A solução deve ser fornecida devidamente licenciada, inclusive com qualquer dos Hipervisores listados acima e para o a volumetria total de ativos monitorados, com atualização por um período de, no mínimo, 5 (cinco) anos, subscrição e suporte 24x7 com início do atendimento em até uma hora.
4.2.2.11	A utilização de memória RAM, dedicada ao funcionamento do controlador virtual de armazenamento, não deve exceder 64GB, para a especificação de hardware exigida neste documento.
4.2.2.12	A solução deverá suportar a implementação de “one node cluster”, ou seja, um cluster composto por apenas um nó.
4.2.2.13	Deverá suportar nativamente funções como:
4.2.2.13.1	**Live Migration (vMotion)** - Permitir operações de migração da máquina virtual para outro nó ou cluster com a máquina em operação, independentemente da quantidade de nós, sem que isto gere quaisquer problemas de performance às aplicações;
4.2.2.13.2	**High Availability** - Permitir operações de alta disponibilidade automatizada, nas quais ocorra falha de um nó ou armazenamento, as máquinas virtuais que dependam desse recurso deverão ser automaticamente iniciadas em outro nó. Ou seja, deverá garantir a continuidade dos serviços, mesmo em caso de falha dos equipamentos da solução, e prover recursos de recuperação contra desastres;
4.2.2.14	A Autoridade Nacional de Proteção de Dados (ANPD) é um órgão da administração pública direta federal do Brasil que faz parte da Presidência da República e possui atribuições relacionadas a proteção de dados pessoais e da privacidade e, sobretudo, deve realizar a fiscalização do cumprimento da Lei nº 13.709/2018, conhecida como Lei Geral de Proteção de Dados Pessoais (LGPD). A ANPD reconhece esquemas internacionais de certificação de privacidade como capacitadores de transferência internacional, uma vez que eles exigem que as organizações certificadas implementem uma série de medidas de proteção de dados de alto padrão. Neste sentido, a solução ofertada deverá contemplar ferramentas e permitir o emprego de configurações aderentes aos seguintes esquemas internacionais:
4.2.2.15	Common Criteria: estes critérios foram produzidos predominantemente para que as empresas que vendem produtos de informática para o mercado governamental (principalmente para uso de Defesa ou Inteligência) precisassem apenas avaliá-los em relação a um conjunto de padrões. Deverá ser comprovada a certificação Common Criteria EAL2+ do hipervisor e do sistema de armazenamento definido por software;
4.2.2.16	As publicações especiais do Instituto Nacional de Padrões e Tecnologia (NIST) para controles de segurança e privacidade (SP) para sistemas e organizações federais de informação (NIST SP 800.53);
4.2.2.17	O Guia de Implementação Técnica de Segurança (STIG) da Agência de Sistemas de Informação do Departamento de Defesa dos EUA (DISA);

4.2.2.18	Tanto para cluster com dados, como para cluster vazio, a solução deverá permitir configurar criptografia de dados durante a ingestão (inline) ou após a gravação na camada de armazenamento (data-at-rest encryption) com gerenciador de chaves (KMS), local ou externo (sem ponto único de falha em ambos os cenários), que suporte a troca da chave mestre de criptografia em períodos arbitrários para aumento de segurança, para que os dados sejam inacessíveis em caso de roubo de um disco ou equipamento. A solução deverá garantir que os dados nos drives sejam seguramente destruídos. Caso a solução dependa exclusivamente de um serviço externo para gerenciamento de chaves criptográficas, este deverá ser fornecido sem ponto único de falha juntamente com a solução. Caso esta funcionalidade requeira licenciamento de software ou componentes de hardware adicionais, estes deverão ser fornecidos com a solução garantindo a redundância entre os sites.
4.2.2.19	A CONTRATADA deverá considerar serviços profissionais do fabricante da solução para empregar configurações de segurança a fim de estabelecer conformidade com o Guia de Implementações Técnicas de Segurança (STIG). Deverá prever também todas as atualizações e correções conforme previsto nos alertas do Centro de Prevenção, Tratamento e Resposta a Incidentes Cibernéticos de Governo (CTIR.Gov) para a camada de virtualização de infraestrutura. Não serão aceitas configurações de contorno para vulnerabilidades conhecidas no momento da implementação.
4.2.2.20	Após o emprego destas configurações a solução deverá dispor de uma estrutura para automação do gerenciamento de configuração de segurança para garantir que os serviços sejam constantemente inspecionados quanto à variação da política de segurança:
4.2.2.21	Tanto para o hipervisor ofertado como para o sistema de armazenamento definido por software, a solução deverá permitir estabelecer um modelo padrão com todas as configurações empregadas no cluster de modo que a solução possa corrigir automaticamente qualquer desvio da configuração de segurança do sistema operacional e do hipervisor para permanecer em conformidade. Se algum componente for considerado não compatível, o componente deverá ser restaurado às configurações de segurança suportadas sem nenhuma intervenção do administrador.
4.2.2.22	As regras STIG deverão ser capazes de proteger o carregador de inicialização (boot loader), pacotes, sistema de arquivos, controle de serviço e inicialização, propriedade de arquivos, ativos de TI, autenticação, kernel e log.
4.2.2.23	A solução deverá estabelecer um ambiente avançado de detecção de intrusões (AIDE) gerando uma base de dados contendo todos os arquivos de configuração. O sistema deverá permitir a verificação da integridade dos arquivos e diretórios por meio de comparação com snapshot capturado da base de dados. No caso de alterações inesperadas, a solução deverá gerar um relatório para revisão. Para o caso de alterações válidas, o administrador poderá atualizar a base de dados.
4.2.2.24	Caso a solução não disponha de tal funcionalidade, deverá ser ofertada ferramenta para gestão de configurações baseadas no conceito de Configuration Management Database (CMDB) em que são guardadas todas as informações importantes sobre itens de configuração (ICs) utilizados pela CONTRATANTE. A ferramenta deverá estar licenciada para toda a capacidade do cluster sem restrições de uso e seguindo o mesmo nível de atendimento do suporte, sendo também necessário o treinamento da equipe técnica da CONTRATANTE para gestão da solução ofertada.

4.2.2.25	A solução deverá dispor de funcionalidades relativas à visibilidade de vulnerabilidades dos ativos de TI que serão considerados e implementados no hipervisor, para identificação de riscos e ameaças externas ou internas.
4.2.2.26	O fabricante da solução deverá publicar avisos de segurança com informações detalhadas sobre atualizações, correções de segurança, descrição das vulnerabilidades e as versões de software impactadas.
4.2.2.27	A solução deverá permitir estabelecer regras de autenticação, tais como:
4.2.2.28	proibir o login direto como usuário root, bloquear contas do sistema que não sejam root, impor detalhes de manutenção de senha, configurar cautelosamente o acesso via SSH, ativar o bloqueio de tela.
4.2.2.29	A solução também deverá suportar a configuração de diferentes métodos de autenticação à interface de gerenciamento centralizado:
4.2.2.30	autenticação através de usuário local,
4.2.2.31	Active Directory com possibilidade de autenticação de usuários com Common Access Card (CAC), permitindo a autenticação e controle de acesso através da combinação de dispositivos de segurança física e senhas de acesso,
4.2.2.32	Security Assertion Markup Language (SAML) através de um provedor externo de identidade.
4.2.2.33	Deverão estar disponíveis os seguintes tipos de usuários e suas respectivas funções:
4.2.2.34	Administrador do Cluster - Pode realizar todas as operações disponíveis, exceto criar ou modificar os usuários;
4.2.2.35	Administrador de Usuários - Pode realizar todas as operações disponíveis.
4.2.2.36	Com o objetivo de proporcionar maior segurança, o sistema operacional também deverá oferecer uma funcionalidade de impedir o acesso ao terminal de linha de comando;
4.2.2.37	A console Web deve suportar o acesso via HTTPS utilizando certificados.
4.2.2.38	A solução deve disponibilizar acesso ao sistema operacional da solução através do protocolo padrão SSH (Secure Shell);
4.2.2.39	A interface de administração WEB e SSH deverá ser configurada em alta-disponibilidade e sem ponto único de falha, garantindo que mesmo em caso de falha ou indisponibilidade de equipamento, a interface de administração continue disponível;
4.2.2.40	Com a finalidade de automatizar os processos de implementação, manutenção e gerenciamento do cluster, o sistema operacional em execução na solução hiperconvergente deverá oferecer REST APIs.
4.2.2.41	O gerenciador do cluster deverá enviar periodicamente informações e estatisticas automaticamente para o suporte do fabricante, funcionalidade conhecida como call-home. Este recurso tem por objetivo aplicar análises avançadas para otimizar a implementação da solução ou atuar proativamente na identificação de problemas. Deverá ser permitido desabilitar este recurso a qualquer momento através da interface WEB.
4.2.2.42	A console de administração gráfica deverá disponibilizar, quando necessário, o acesso remoto do time de suporte do fabricante. Tal funcionalidade deverá estabelecer um túnel SSH reverso aos servidores do fabricante com o objetivo de permitir ao suporte, executar manutenções no software dos controladores de armazenamento virtuais. O administrador do sistema poderá habilitar ou desabilitar o acesso a qualquer momento.
4.2.2.43	A solução deverá possuir ferramenta de checagem interna integrada a console de gerenciamento, buscando por problemas de saúde no cluster proativamente.

4.2.2.44	Deverá fazer monitoração automática e periódica da solução, com o envio de notificações preventivamente em caso de falhas, notificando o suporte da CONTRATADA a tomar medidas preventivas e acordadas com o CONTRATANTE a fim de evitar tempo de inatividade e impactos na produção;
4.2.2.45	Conforme disposto no item I do artigo 15 da lei 8.666, de 21 de junho de 1993 (I – Atender ao princípio de padronização, que imponha compatibilidade técnica e de desempenho, observadas, quando for o caso, as condições de manutenção, assistência técnica e garantia oferecidas), tanto os hardwares quanto os softwares desta solução deverão ser do mesmo fabricante ou com suporte unificado para hardware e software pelo fabricante da solução.
4.2.2.46	Todos os componentes de software da solução deverão ser devidamente licenciados e suportados por pelo menos 5 (cinco) anos.
4.2.2.47	A solução deverá possuir suporte com 0800 no Brasil e atendimento em português do Brasil salvo em caso de necessidade de escalonamento de chamados;
4.2.2.48	Caso a solução tenha algum componente em SaaS, deverá cumprir integralmente as diretrizes estabelecidas na Instrução Normativa Nº 5, de 30 de agosto de 2021, garantindo que, se baseada em nuvem, todos os dados e metadados sejam armazenados exclusivamente em território brasileiro; deve assegurar a segurança e privacidade dos dados em conformidade com a Lei Geral de Proteção de Dados Pessoais (LGPD); e deve implementar um plano robusto de recuperação de desastres que detalhe procedimentos para a recuperação e restauração completa da plataforma, infraestrutura, aplicações e dados após quaisquer incidentes de perda de dados.
4.2.2.49	É de responsabilidade do fornecedor garantir a compatibilidade técnica entre todos os componentes da solução durante toda a vigência do contrato;
4.3	**CARACTERISTICAS DO OBJETO**
4.3.1	**ITEM 01 - HARDWARE PARA INFRAESTRUTURA HIPERCONVERGENTE (HCI): CARACTERÍSTICAS GERAIS DE CADA NODE:**
4.3.1.1	Deverá possuir no máximo 2Us (Unidades de Rack) para montagem em rack padrão de 19 polegadas, acompanhado de todos os acessórios para perfeita fixação;
4.3.1.2	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;
4.3.1.3	Deverá permitir, sem a necessidade de ferramentas, ao menos para instalação/desinstalação de fontes de alimentação e discos;
4.3.1.4	Deverá possuir sistema de ventilação redundante (N+1) para que a CPU suporte a configuração máxima e dentro dos limites de temperatura adequados para o perfeito funcionamento do equipamento.
4.3.1.5	Os equipamentos devem possuir LED indicador de status que permita monitorar as condições de funcionamento do equipamento;
4.3.1.6	**Segue especificação para cada Node;**
4.3.1.6.1	**Fontes de Alimentação:**
4.3.1.6.1.1	Deverá ser equipado de no mínimo de 2 (duas) fontes, suportando o funcionamento do equipamento na configuração ofertada mesmo em caso de falha de uma das fontes;
4.3.1.6.1.2	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;

4.3.1.6.1.3	Cada fonte de alimentação deve possuir potência suficiente para suportar os appliances/nós em sua configuração máxima;
4.3.1.6.1.4	As fontes devem possuir tensão de entrada de 100VAC a 240VAC a 60Hz, com ajuste automático de tensão;
4.3.1.6.1.5	Deverá acompanhar cabo de alimentação para cada fonte de alimentação fornecida padrão C14.
4.3.1.6.1.6	A ventilação deve ser adequada para a refrigeração do sistema interno do equipamento na sua configuração máxima, e dentro dos limites de temperatura indicados pelo fabricante para correta operação do equipamento;
4.3.1.6.1.7	O fluxo de ar deverá ser da parte frontal para a parte traseira do equipamento.
4.3.1.6.2	**Rede:**
4.3.1.6.2.1	No mínimo, 2 (duas) interfaces Ethernet com banda de, no mínimo, 10/25 Gbps por interface, incluindo cabos DAC de 3m;
4.3.1.6.2.2	Possuir no mínimo 1 (uma) porta 1GbE para ser utilizada como interface de gerenciamento outof- band.
4.3.1.6.2.3	O modelo da interface de rede ofertado deverá estar certificado/homologado para o hipervisor ofertado.
4.3.1.6.3	**Processamento:**
4.3.1.6.3.1	Deverá possuir, no mínimo, 2 (dois) processadores, cada um contendo, 24 (vinte e quatro) Núcleos de processamento, em arquitetura x86_64, de última ou penúltima geração disponível para o equipamento operando a uma frequência base mínima de 2.0GHz; Memória cache de pelo menos 45 MB.
4.3.1.6.3.2	Compatibilidade com a tecnologia de virtualização Intel VT-x ou equivalente da AMD.
4.3.1.6.4	**Memória RAM:**
4.3.1.6.4.1	Deverá possuir, no mínimo, 384GB (Trezentos e oitenta e quatro) de memória utilizando módulos tipo DDR5 4800MHz RDIMM (Registered DIMM) ou LRDIMM (Load Reduced DIMM).
4.3.1.6.5	**Armazenamento:**
4.3.1.6.5.1	Cada equipamento deverá prover pelo menos 6TiB (um tebibytes – base 2) de capacidade de armazenamento útil, livre e disponível para as aplicações, já descontadas todas as perdas com formatação, configuração de RAID (quando aplicável) em nível para prover o melhor desempenho para o SDS, fator de replicação (dado original e uma réplica em equipamentos distintos no mesmo cluster e no mesmo site), alta-disponibilidade (HA), área de manobra (slack space) máxima e, também quando aplicável, grupos de discos em número máximo conforme estabelecido nos manuais do fabricante da solução de armazenamento definida por software, para reduzir impacto durante operações de reconstrução e re-sincronização. Além disso, deverá considerar as perdas relativas à soma de verificação (checksum) para garantia de integridade dos dados e quaisquer outras perdas / overhead da solução de armazenamento definida por software, inclusive perdas decorrentes do emprego de tecnologias para ganhos de eficiência como desduplicação e compressão. A área útil não poderá ser dimensionada considerando ganhos de erasure-coding, desduplicação e compressão. Pelo menos 100% desta capacidade deverá pertencer à camada de alto desempenho em drives SSD ou NVMe.

4.3.1.6.5.2	A solução deverá estar licenciada para uso de funcionalidades de otimização (desduplicação e compressão) de dados. Caso a solução requeira evacuação dos dados e/ou reformatação dos discos para ativar ou desativar as funcionalidades de otimização, a área de manobra (slack space) para esta evacuação deverá ser considerada com pelo menos 30% (trinta por cento) da capacidade de armazenamento, conforme recomendação expressa no manual do fabricante da solução de armazenamento definida por software. Se a solução não for capaz de otimizar os dados no nível do cluster (global), a licitante deverá considerar 30% (trinta por cento) de capacidade de armazenamento útil adicional para cada equipamento a fim de compensar a ineficiência da solução em manter cópias redundantes.
4.3.1.6.5.3	Para redução dos riscos de perda ou corrupção de dados em caso de falha de disco durante processos de atualização de firmwares e softwares que requeiram reinicialização de equipamentos, a falha de um disco de cache ou de capacidade não deve impactar ou interromper o funcionamento de outros discos na solução. Caso a solução não atenda este requisito, a capacidade de armazenamento útil do cluster deverá considerar a existência de três cópias dos dados (original e duas réplicas). Neste cenário a licitante também deverá considerar tempo de reposição de discos em no máximo 4h (quatro horas), a fim de reduzir o tempo e o impacto de reconstrução (rebuild) no cluster. O fabricante deverá garantir a troca de quaisquer discos mesmo quando as aplicações excederem seus limites de gravação (DWPD).
4.3.1.6.5.4	Todos os nós do cluster devem participar das operações de reconstrução de disco (rebuild), deixando-os mais eficientes à medida que o cluster cresce em número de nós. Caso a solução não atenda a este requisito, deverá ser ofertada com discos de até 3TB (três terabytes) a fim de minimizar o impacto e o tempo de reconstrução.
4.3.1.6.5.5	Para soluções que dependam da configuração de RAID, as licitantes deverão considerar, no dimensionamento da capacidade útil, a quantidade de grupos de discos e o nível de RAID que garantam o melhor desempenho da solução ofertada conforme estabelecido nos manuais do respectivo fabricante da solução de armazenamento definida por software.
4.3.1.6.5.6	A solução de hiperconvergência contratada deve, através de soft ware próprio ou de terceiros, proveras seguintes funções, para pelo menos 20 imagens de conteiner:
4.3.1.6.5.7	Analisar, testar e reportar falhas de segurança em aplicações em Containers Docker como parte dos ativos a serem inspecionados;
4.3.1.6.5.8	Analisar imagens preparadas pelos desenvolvedores na esteira DevOps em busca de imagens com vulnerabilidadesidenti fi cadas e malware residente no sistema de arquivos;
4.3.1.6.5.9	Integrar a esteira DevOps através de API, invocando o envio da imagem para análise em repositório próprio dasolução ou uti lizando scanner implementado em infraestrutura proprietária do órgão com a finalidade de evitar oenvio de imagens e propriedade intelectual da contratante;
4.3.1.6.5.10	A console de administração destas funções deverá possuir controle de acesso no mínimo permiti ndousuários com capacidade de somente visualizar as informações, e usuários com capacidade para efetuar análisedas imagens;
4.3.1.6.5.11	Inventariar o sistema operacional de cada imagem analisada e suas vulnerabilidades encontradas;
4.3.1.6.5.12	Identificar containers que não foram analisados antes de sua implementação em produção;
4.3.1.6.5.13	Analisar as camadas (layers) de um container;

4.3.1.6.5.14	Identificar containers que tiveram mudanças de arquivos entre a análise e a sua implementação emprodução;
4.3.1.6.5.15	Informar os CVEs para cada vulnerabilidade encontrada nos pacotes e bibliotecas residentes na imagem;
4.3.1.6.5.16	Deve ter a capacidade de testar automaticamente todas as imagens armazenadas, ou previamente testadas, sempre que uma nova vulnerabilidade for publicada e atualizada no banco de dados de vulnerabilidadeda solução, sem qualquer tipo intervenção manual;
4.3.1.6.5.17	Inventariar os pacotes e bibliotecas e suas respectivas versões e listar as mesmas dentro do relatóriode resultados de análise de cada imagem;
4.3.1.6.5.18	Fornecer scanner em formato Docker para implementação local e análise de imagens sem a necessidade de envio destas para repositório remoto, fora do ambiente da contratante;
4.3.1.6.5.19	Deve ser capaz de configurar políti cas usando como condições: CVSS Score, CVEs específi cos eMalware identificado;
4.3.1.6.5.20	Deve permitir a criação de políticas especificas por repositório;
4.3.1.6.5.21	Deve prover integração com as seguintes plataformas de integração contínua: Bamboo, CircleCI, Codeship, Distelli, Drone.io, Jenkins, Shippable, Solano Labs, Travis CI, Wrecker e Kubernets.
4.4	**ITEM 02 – SOFTWARE PARA HCI**
4.4.1	Cada unidade deste item deverá prover licenciamento/subscrição de software para um núcleo (core) de processador, com suporte 24x7 e atendimento para chamados críticos em até uma hora, com vigência de 60 (Sessenta) meses.
4.4.2	**Requisitos de Virtualização e Gerenciamento:**
4.4.2.1	A CONTRATADA deverá fornecer o licenciamento, suporte e subscrição, durante a vigência da garantia da solução, para o hipervisor nativo da solução, com a respectiva solução de gerenciamento centralizado, de modo a permitir o uso de suas funcionalidades para configuração e gerenciamento de um ambiente altamente disponível, sendo minimamente capaz de:
4.4.2.2	Permitir operações de live migration (migração da máquina virtual para outro host com a máquina virtual em operação);
4.4.2.3	Disponibilizar gerenciador de imagens através de um repositório centralizado e permitir o uso de discos ou imagens nos formatos qcow, qcow2, vmdk, VHD, VHDx, raw, ISO para que seja possível a utilização destes discos e imagens com as máquinas virtuais do cluster;
4.4.2.4	A solução deve ser capaz de distribuir os servidores virtuais entre os nós do cluster de modo que ocorra distribuição da carga.
4.4.2.5	O hipervisor deverá possuir um planejador (scheduler) com acesso a telemetria do host para tomar decisões de posicionamento das máquinas virtuais:
4.4.2.6	Posicionamento inicial: a melhor posição em um cluster para inicialização da máquina virtual ou carga de trabalho;
4.4.2.7	Otimização de tempo de execução: movimento de cargas de trabalho com base em métricas durante tempo de execução.
4.4.2.8	Posicionamento das VMs deverá seguir pelo menos os seguintes fatores: Computação (CPU/MEM).
4.4.2.9	Utilização da CPU
4.4.2.10	Utilização de memória Contenção de recursos

4.4.2.11	Limiares e/ou marcas d'água para métricas de computação Desempenho de armazenamento
4.4.2.12	Utilização do processo de gestão das operações de I/O Propriedade do disco virtual
4.4.2.13	Localização dos volumes Regras de afinidade e anti-afinidade
4.4.2.14	Políticas definidas pelo usuário para o local (host) onde será executada a VM Agrupamento de VMs
4.4.2.15	Separação de VMs
4.4.2.16	Com intuito de simplificar as configurações de rede, a solução deverá dispor de switch virtual distribuído baseado em, ou compativel com Open Virtual Switch (OVS), de modo que a gestão seja centralizada e todas as configurações sejam igualmente aplicadas e mantidas entre todos os hosts do cluster.
4.4.2.17	A solução de rede virtual deverá permitir IP address management (IPAM) para a configuração de pools de endereços IP para atribuição às máquinas virtuais automaticamente sem a necessidade de um serviço de DHCP.
4.4.2.18	A solução deverá permitir a visualização de informações dos switches topo de rack na console Web de administração do cluster. Através do protocolo Link Layer Discovery Protocol (LLDP) ou Cisco Discovery Protocol (CDP) a solução deverá prover visualização gráfica das portas dos switches que estão conectadas às respectivas portas de redes das unidades computacionais. Adicionalmente, deverá ser possível a configuração dos protocolos SNMP v3 ou SNMP v2c nos switches topo de rack, para visualizar na mesma interface gráfica de gestão do cluster, as informações estatisticas das interfaces dos switches tais como:
4.4.2.19	Número de pacotes unicast transmitidos e recebidos;
4.4.2.20	Número de pacotes transmitidos e recebidos com um erro;
4.4.2.21	Número de pacotes transmitidos e recebidos que foram descartados;
4.4.2.22	Deverá permitir a criação de redes virtuais completamente isoladas no conceito multi-tenant com capacidade de provisionamento de redes em autoatendimento, possibilidade de sobreposição de endereços IP e preservação destes endereços através de encapsulamento.
4.4.2.23	VPCs (Virtual Private Clouds): estrutura de rede virtual totalmente isolada com uma instância de roteador virtual para conexão com todas as sub-redes dentro da VPC. Esta construção deverá permitir a sobreposição (overlap) de endereços IP existentes dentro de uma VPC sem qualquer conflito com qualquer outra VPC e até mesmo endereços já existentes na estrutura de rede física. Uma VPC poderá expandir para incluir qualquer outro cluster HCI pertencente à mesma zona de disponibilidade sob a gestão da mesma ferramenta de gerenciamento centralizado ofertada.
4.4.2.24	Sub-redes de sobreposição: As diferentes sub-redes dentro de uma VPC deverão se conectar através do roteador virtual pertencente a respectiva VPC. A solução deverá prover um túnel de encapsulamento de tráfego entre os diferentes hosts de virtualização sem a necessidade de configuração das sub-redes nos switches topo de rack para que as VMs operando em diferentes hosts se comuniquem. A solução deverá permitir a escolha para atribuição de rede para máquinas virtuais diretamente associada a uma sub-rede de sobreposição (overlay subnet) ou em VLAN tradicional (VLAN backed subnet).
4.4.3	**Rotas:**

4.4.3.1	Redes externas: devem ser o destino padrão do prefixo de rede 0.0.0.0/0 para toda a VPC. Deve ser possível escolher uma rota de prefixo de rede alternativa para cada rede externa em uso. Para VPCs completamente isoladas, deverá ser possível não definir uma rota padrão. Uma rede externa deverá ser a principal maneira de o tráfego entrar e sair de uma VPC. Essa rede definirá a VLAN, o gateway padrão, o pool de endereços IP e o tipo de NAT para todas as VPCs que a utilizam. Uma rede externa poderá ser usada por muitas VPCs.
4.4.3.2	Uma rede externa NAT (Network Address Translation) deverá ocultar os endereços IP das VMs na VPC atrás de um IP flutuante ou do endereço VPC SNAT (NAT de origem). Cada VPC tem um endereço IP SNAT selecionado aleatoriamente no pool de IP de rede externa e o tráfego que sai da VPC é reescrito com esse endereço de origem. Os endereços IP flutuantes também serão selecionados no pool de IPs de rede externa e serão atribuídos a VMs em uma VPC para permitir o tráfego de entrada. Quando um IP flutuante for atribuído a uma VM, o tráfego de saída deverá ser reescrito com o IP flutuante em vez do IP SNAT da VPC, para que seja possível anunciar serviços públicos fora da VPC sem revelar o endereço IP privado da VM.
4.4.3.3	As redes externas roteadas ou NoNAT devem permitir que o espaço de endereço IP
4.4.3.4	da rede física seja compartilhado dentro da VPC por meio de roteamento. Em vez de um endereço IP VPC SNAT, o IP do roteador VPC será selecionado aleatoriamente no pool de rede externa. Deverá ser possível compartilhar esse IP de roteador VPC com a equipe de rede física para que eles possam definir esse IP de roteador virtual como o próximo salto (hop) para todas as sub-redes provisionadas dentro da VPC.
4.4.3.5	Rotas conectadas diretamente: a solução deverá permitir a criação destas rotas para cada sub-rede dentro da VPC, com possibilidade de atribuir o primeiro endereço IP de cada subrede como o gateway padrão para essa sub-rede. O gateway padrão e o prefixo de rede serão determinados pela configuração da sub-rede e não pode ser alterado diretamente. O tráfego entre duas VMs no mesmo host e na mesma VPC, mas em duas subredes diferentes, deverá ser roteado localmente nesse host.
4.4.3.6	Conexões remotas: tal como conexões VPN e Redes Externas, poderão ser definidas como o próximo destino de salto (hop) para um prefixo de rede.
4.4.3.7	Políticas: O roteador virtual deverá atuar como um ponto de controle para o tráfego dentro de uma VPC. Deverá permitir aplicar políticas stateless simples; qualquer tráfego que fluir pelo roteador deverá ser avaliado pelas políticas. O tráfego de uma VM para outra dentro da mesma sub-rede não poderá passar por uma política. Dentro de uma VPC, as políticas deverão ser avaliadas em ordem de prioridade, da mais alta (1.000) à mais baixa (10).
4.4.3.8	Gateways de rede: deverá prover vários métodos de conexão entre sub-redes: VPN de camada 3
4.4.3.9	Gateway de rede para gateway de rede
4.4.3.10	Gateway de rede para firewall físico ou VPN Camada 2 VXLAN VTEP
4.4.3.11	Gateway de rede para gateway de rede
4.4.3.12	Gateway de rede para roteador físico ou switch VTEP Camada 2 VXLAN VTEP sobre VPN Gateway de rede para gateway de rede
4.4.3.13	A solução ofertada deverá estar habilitada para uso de microssegmentação de rede virtual, provendo controle granular e governança de todo o tráfego de entrada e saída de uma máquina virtual (VM) e de grupos de máquinas virtuais (VMs).

4.4.3.14	A microssegmentação deverá permitir a associação de políticas de rede a VMs e aplicativos ao invés de segmentos de rede específicos (por exemplo VLANs) ou identificadores (endereços IP ou MAC).
4.4.3.15	Deverá prover visualização de todo tráfego e relacionamentos com a descoberta automática dos fluxos entre as máquinas virtuais.
4.4.3.16	Deverá prover uma estrutura de segurança orientada por políticas que inspecionam o tráfego dentro do data center, da seguinte maneira:
4.4.3.17	As políticas de segurança inspecionam o tráfego originado e terminado dentro de um datacenter, ajudando a eliminar a necessidade de firewalls adicionais no datacenter.
4.4.3.18	A estrutura deve utilizar uma abordagem centrada na carga de trabalho em vez de uma abordagem centrada na rede, permitindo examinar o tráfego de, e para as VMs, independentemente de como as configurações de rede mudam e onde residem no data center.
4.4.3.19	Deverá prover uma abordagem agnóstica a estrutura de rede, centrada na carga de trabalho, permitindo que a equipe de virtualização implemente essas políticas de segurança sem depender de equipes de segurança de rede.
4.4.3.20	As políticas de segurança deverão ser aplicadas às categorias (um agrupamento lógico de VMs) e não às próprias VMs, não importando quantas VMs são inicializadas em uma determinada categoria. O tráfego associado às VMs em uma categoria deverá ser protegido sem intervenção administrativa, em qualquer escala.
4.4.3.21	A interface de gerenciamento deve oferecer uma abordagem baseada em visualização para configurar políticas e monitorar o tráfego ao qual uma determinada política se aplica:
4.4.3.21.1	Política de Segurança de Aplicação: quando for necessário proteger um aplicativo especificando origens e destinos de tráfego permitidos.
4.4.3.21.2	Política de Isolamento do Ambiente: quando for necessário bloquear todo o tráfego, independentemente da direção, entre dois grupos de VMs identificados por sua categoria. VMs dentro de um grupo podem se comunicar umas com as outras.
4.4.3.21.3	Política de Quarentena: quando for necessário isolar uma VM comprometida ou infectada e, opcionalmente, desejar submetê-la à perícia.
4.4.3.22	Deverá garantir que seja apenas permitido o tráfego entre camadas de aplicativos ou outros limites lógicos, garantindo a proteção contra ameaças avançadas para que não sejam propagadas no ambiente virtual.
4.4.3.23	Deverá garantir que seja apenas permitido o tráfego entre camadas de aplicativos ou outros limites lógicos, assegurando a proteção contra ameaças avançadas para que não sejam propagadas no ambiente virtual, bem como identificar e avaliar riscos baseados em vulnerabilidades que possibilitem lateralização, detectando potenciais caminhos de ataque e de movimentação lateral entre os ativos, analisando continuamente configurações, permissões e conexões entre componentes do sistema, a fim de prevenir a exploração e propagação de ameaças dentro do ambiente virtual, mitigando proativamente riscos de lateralização..
4.4.3.24	Deverá permitir a atualização automática durante todo o ciclo de vida da VM, eliminando a carga do gerenciamento de mudanças de políticas.
4.4.3.25	A Solução deve permitir categorizar as Máquinas Virtuais de forma a permitir a criação de políticas de segurança com no mínimo as seguintes funções:

4.4.3.25.1	Isolar o tráfego de dados entre Máquinas Virtuais de Diferentes categorias.
4.4.3.25.2	Isolar o tráfego de dados de Máquinas Virtuais específicas para modo de quarentena, tanto forense quanto restrita, de forma a prover uma rápida reação ao time de infraestrutura em caso de Máquinas Virtuais contaminadas ou pertencentes a usuários que foram desligados ou sob procedimento de custódia de dados.
4.4.3.25.3	Mapear o tráfego de entrada, entre as camadas e de saída de aplicações, permitindo ao administrador determinar quais servidores tem acesso de entrada na aplicação, o tipo de protocolo e o número da porta que o fluxo de dados pode ocorrer, permitir ou restringir também o fluxo de dados entre as camadas, máquinas virtuais, pertencentes à aplicação, através da especificação do protocolo e o número da porta, realizar também o mesmo procedimento para conexões de saída das camadas da aplicação, também através da especificação de protocolo e número de porta.
4.4.3.26	Deve permitir integração com softwares de terceiros para que seja possível o redirecionamento do tráfego das VMs para ferramentas de detecção e prevenção de intrusos (IDS/IPS), monitoração de performance de aplicações (APM), balanceadores de carga.
4.4.3.27	Visibilidade da conformidade com a segurança: fornecer um mapa de calor relacionado à segurança provendo visibilidade completa da postura de segurança do ambiente da CONTRATANTE. Identificar vulnerabilidades de segurança usando verificações de auditoria automatizadas.
4.4.3.28	Controle sobre conformidade de segurança: permitir a definição de políticas que detectam continuamente vulnerabilidades de segurança em tempo real e automatizam as ações necessárias para corrigi-las. Permitir criar verificações de auditoria personalizadas para atender às necessidades de conformidade de segurança específicas do CONTRATANTE.
4.4.3.29	Com relação a estrutura de nuvem privada do CONTRATANTE, a solução deverá prover auditorias de segurança com detalhes de quaisquer configurações incorretas ou inadequadas dos recursos instalados, classificados no mínimo pelas seguintes categorias:
4.4.3.29.1	Auditorias de rede, como exemplo as portas TCP/UDP publicamente acessíveis. Auditorias de máquinas virtuais, como exemplo as VMs sem proteção de acesso. Auditorias de dados, como exemplo dados não criptografados.
4.4.3.29.2	Auditorias de acesso.
4.4.3.30	Além de detectar estes recursos que falhem durante as auditorias, a solução deverá prover ações de remediação necessárias para melhorar a segurança da infraestrutura.
4.4.3.31	Permitir operações de alta disponibilidade automatizada, onde em caso de falha de um nó, as máquinas virtuais que dependam desse recurso, sejam automaticamente iniciadas em outro nó.
4.4.3.32	A solução deverá ser capaz de automatizar o processo de criação de clusters Kubernetes:
4.4.3.33	A solução deverá otimizar a implantação e o gerenciamento de clusters Kubernetes com uma interface gráfica simples e integrada ao gerenciamento centralizado do cluster hiperconvergente.
4.4.3.34	Os clusters Kubernetes deverão ser instalados com as ferramentas Prometheus, ElasticSearch, Fluent Bit e Kibana (pilha EFK) para monitoração, registro (logging), e alertas. Caso não sejam instalados com estas ferramentas, deverão ser fornecidos com ferramentas semelhantes para exercer as mesmas funções.
4.4.3.35	Monitoramento continuo com alertas exibidos na interface de gestão gráfica.

4.4.3.36	Permitir a configuração de clusters com alta-disponibilidade para os master nodes, com ou sem balanceador de carga.
4.4.3.37	Deverá permitir a gestão do ciclo de vida com atualizações da versão kubernetes de maneira simples e sem interrupções.
4.4.3.38	Prover armazenamento persistente através de integração com Container Storage Interface (CSI) conectados ao SDS para armazenamento de blocos e arquivos. Também deverá ser possível configurar armazenamento de objetos compativel com S3;
4.4.3.39	Deverá suportar os modos de acesso ao armazenamento persistente: Read-Write-Once Read-Write-Many.
4.4.3.40	Permitir filtrar e analisar logs de sistemas, pods e nós.
4.4.3.41	Fornecer um mecanismo de monitoramento que aciona alertas no cluster Kubernetes.
4.4.3.42	Deverá usar o sistema de monitoramento de saúde para interagir com o Suporte do fabricante objetivando agilizar a resolução de problemas dos cluster Kubernetes.
4.4.3.43	Permitir escalabilidade (scale out e scale in) dos nodes pela mesma interface gráfica e por linha de comando (CLI).
4.4.3.44	Deverá preservar a experiência nativa dos usuários Kubernetes com APIs abertas.
4.4.3.45	Permitir desativar autenticação baseada em senha em todos os nodes Kubernetes de forma que seja possível estabelecer o uso de chaves SSH com validade de até 24h (vinte e quatro horas).
4.4.3.46	A solução deve possuir console de administração WEB sem necessidade de instalação de qualquer componente adicional para essa finalidade;
4.4.3.47	A solução de gerenciamento WEB deve ser capaz de gerenciar qualquer hipervisor especificado neste termo de referência;
4.4.3.48	A console WEB deve ser acessível por browsers que suportam a tecnologia HTML5.
4.4.3.49	A console WEB deve fornecer acesso à um Dashboard principal personalizável com informações da saúde do Sistema (cluster) tanto no site local como em sites remotos, sumário dos equipamentos e das Máquinas Virtuais, visão geral da utilização dos recursos computacionais do cluster (processamento, memória, armazenamento), bem como visualização de alertas e eventos, visualização das informações de desempenho da solução (utilização de banda do cluster, IOPS do cluster e latência do cluster).
4.4.3.50	A solução deve permitir, através de uma interface de gestão gráfica, a atualização do storage definido por software, Hipervisor, BIOS e firmwares dos dispositivos de todos os equipamentos do cluster de forma simples e automatizada, eliminando a intervenção manual do administrador e parada no ambiente;
4.4.3.51	Com a finalidade de automatizar os processos de implementação, manutenção e gerenciamento do cluster, o sistema operacional em execução na solução hiperconvergente deverá oferecer REST APIs;
4.4.3.52	O gerenciador do cluster deve enviar periodicamente informações e estatisticas, de maneira automática, para o suporte. Esta funcionalidade tem por objetivo aplicar análises avançadas para otimizar a implementação da solução ou atuar proativamente na identificação de problemas. Deverá ser permitido desabilitar este recurso a qualquer momento através da interface WEB;
4.4.3.53	A solução deverá possuir ferramenta de checagem interna integrada a console de gerenciamento, buscando por problemas de saúde no cluster proativamente;

4.4.3.54	A solução deve permitir que os usuários e administradores personalizem a visualização dos painéis de gerenciamento;
4.4.3.55	Ferramenta de gerenciamento deve possuir funcionalidade de busca (search) que suporte busca contextualizada;
4.4.3.56	Deve ter a capacidade de definir permissões específicas para os usuários dependendo de sua função (Role Based Access Control – RBAC), definidas pelo usuário gestor da solução;
4.4.3.57	A solução deve suportar o envio de alertas críticos automaticamente para o fabricante da solução:
4.4.3.58	Deve suportar envio de alertas e eventos via SNMP;
4.5	**CARACTERÍSTICAS DA SOLUÇÃO DE SOFTWARE DE ARMAZENAMENTO - STORAGE - SDS:**
4.5.1	O controlador de armazenamento deverá permitir atualização de seu software independente do hipervisor, sendo assim baseado em máquina virtual, executando sistema operacional próprio desenvolvido no conceito de armazenamento definido em software. Cada servidor físico, também definido por nó em uma solução hiperconvergente, deverá hospedar um controlador de armazenamento virtual, possibilitando a criação de um cluster, apresentando ao hipervisor um sistema de arquivos único e distribuído.
4.5.2	Os recursos de armazenamento devem ser compartilhados entre todos os nós da solução por meio de armazenamento definido por software (Software Defined Storage), criando uma área de armazenamento compartilhada, distribuída e otimizada para ambientes virtuais;
4.5.3	O licenciamento do SDS não deverá impor um limite para o número de equipamentos que compõem o mesmo cluster;
4.5.4	Deverá permitir a configuração de cluster heterogêneo composto por equipamentos de gerações e configurações distintas a fim de atender aos diferentes requisitos de cargas de trabalho. A solução deverá suportar nós híbridos (com HDD e SSD) e all-flash (somente SSD) no mesmo cluster.
4.5.5	Fornecer suporte nativo para snapshots e clones que aproveitam o algoritmo de redirecionamento na gravação (redirect-on-write), para maior eficácia e eficiência.
4.5.6	A solução deverá se utilizar de um mecanismo para mover os dados não acessados para os discos rígidos pertencentes ao cluster, deixando os discos SSD para dados acessados com frequência. Caso o dado volte a ser requisitado, o mesmo deverá ser migrado para os discos SSD.
4.5.7	O SDS deve implementar escalabilidade horizontal (scale-out), ou seja, permitir aumentar a capacidade de armazenamento, processamento e memória do ambiente virtual de forma linear, através da adição de novos nós (appliances) ao cluster, além de crescer de forma linear o desempenho do ambiente, sem a parada do ambiente de produção. Também deverá permitir a adição de novos equipamentos com propósito de expandir a capacidade de armazenamento do cluster (storage-only nodes);
4.5.8	O licenciamento do SDS deverá permitir a definição do nível de redundância para os dados de modo que o administrator possa estabelecer a existência de duas cópias (original e uma réplica) para aplicações menos críticas e três cópias (original e duas réplicas) para aplicações mais críticas, todas em execução no mesmo cluster.
4.5.9	O licenciamento do SDS deverá permitir a configuração de domínios de disponibilidade para que seja possível tolerar a falha de nó, bloco e rack sem impacto para disponibilidade dos dados armazenados no SDS.
4.5.10	Deve implementar, via software, compressão inline (durante o processo de gravação).

4.5.11	Deve implementar, via software, desduplicação de dados inline (durante o processo de gravação).
4.5.12	Deve implementar compressão pós-processada, sendo que após a operação de escrita, exista um atraso em minutos para iniciar o processo de compressão. O atraso deverá ser configurável pelo administrador do sistema.
4.5.13	Implementar desduplicação pós-processado, que diferentemente da inline, deverá ocorrer em um processo posterior a gravação.
4.5.14	O licenciamento do SDS deverá permitir a implementação de método de proteção de dados Erasure Coding, no qual os dados são divididos em fragmentos, estendidos e codificados com pedaços de dados redundantes e armazenados em diferentes nós.
4.5.15	A fim de proporcionar melhor aproveitamento de espaço para armazenamento, com o mínimo impacto em performance quanto possível, a solução deve permitir algum tipo de segregação lógica, de armazenamento de VMs, que possibilite a aplicação dos recursos de compressão e/ou desduplicação, para cargas específicas. Em outras palavras, por exemplo, deve ser possível aplicar compressão apenas para VMs de banco de dados, bem como desduplicação apenas para VMs que desempenhem o papel de File Servers.
4.5.16	Deverá suportar QoS (Quality of Service) na camada de armazenamento a fim de limitar a quantidade de I/Os que uma determinada máquina virtual, ou conjunto de máquinas virtuais podem executar na infraestrutura;
4.5.17	Deverá permitir a priorização de uso da camada de desempenho baseada em drives SSD para VMs que demandem maior desempenho.
4.5.18	Com o objetivo de atender às demandas específicas de certas aplicações por acesso a armazenamento via protocolo iSCSI, o SDS deverá permitir a apresentação de armazenamento em nível de blocos para máquinas virtuais dentro e fora do cluster HCI.
4.5.19	A solução deverá dispor de recursos para a replicação de dados entre clusters distantes geograficamente. Deverá permitir a configuração de diferentes planos de proteção para as cargas de trabalho, na mesma estrutura, de acordo com sua criticidade. Por exemplo:
4.5.20	Quando disponíveis links com Round Trip Time de cinco milissegundos (RTT=5ms), as cargas de trabalho mais críticas deverão ser replicadas de maneira síncrona (RPO=0). Neste cenário, a solução também deverá suportar a migração online de máquinas virtuais entre os clusters;
4.5.21	Para aplicações do ambiente produção de menor criticidade, a solução deverá permitir a configuração de políticas de proteção com objetivos de ponto de recuperação entre um e quinze minutos (1min ≥ RPO ≤ 15min);
4.5.22	Para sistemas em ambientes de desenvolvimento, testes e homologação, a solução deverá permitir a configuração de políticas de proteção com objetivo de ponto de recuperação mínimo de uma hora (RPO≥1h).
4.5.23	Em situação de falência de um cluster, a solução deverá orquestrar o processo de recuperação e restabelecimento das máquinas virtuais no cluster funcional. A solução deverá permitir níveis de proteção por máquinas virtuais individualmente ou para o cluster em sua totalidade, sendo possível estabelecer sequências de inicialização, reconfiguração de redes, execução de scripts, além de permitir a definição de intervalos necessários para funcionamento dos serviços.

4.5.24	O SDS, independentemente do hipervisor, deve realizar snapshots das máquinas virtuais nativamente, armazenando esses snapshots no cluster para proteção local, além de permitir a replicação para outros clusters com capacidade de otimização global dos dados a fim de reduzir o consumo de links de comunicação. O snapshot realizado deve ser do tipo crash consistent, ou seja, o snapshot poderá ser feito com o ambiente em produção e irá garantir a proteção dos dados que estão gravados em disco. O SDS deve suportar realizar snapshots com consistência dos dados em memória (application-consistent) para máquinas com sistemas operacionais Linux e Windows, através de integração com VSS e semelhantes.
4.5.25	O licenciamento do SDS não deverá limitar o número de retenções dos snapshots, permitindo manter pelo menos 24 (vinte e quatro) snapshots horários, 7 (sete) snapshots diários e 4 (quatro) snapshots semanais. O recurso de snapshots das máquinas virtuais, realizado pelo sistema de armazenamento definido por software (SDS), deverá operar com redirecionamento na escrita (redirect-on-write), oferecendo mais velocidade e eficiência, sem sacrificar o desempenho do cluster. Caso a solução não atenda este requisito, cada equipamento deverá ser ofertado com 20% (vinte por cento) de recursos adicionais para processamento e armazenamento das cópias de proteção realizadas.
4.5.26	Deve permitir ao usuário administrator de uma determinada máquina virtual, restaurar de maneira granular, arquivos armazenados em snapshots a partir da máquina virtual em execução sem a necessidade de intervenção do administrador do SDS.
4.5.27	A solução deve suportar a proteção dos dados com definições de políticas customizadas de tolerância a falhas com granularidade de Máquina Virtual;
4.5.28	Deverá ser permitida a troca de discos avariados, sem interrupção das operações de I/O das aplicações que estão acessando os dados;
4.5.29	A falha isolada de um nó da solução não pode impactar a disponibilidade da infraestrutura de armazenamento para as máquinas virtuais. A falha isolada de um disco não deve interromper o funcionamento de outros discos;
4.5.30	Suportar a criação de domínios de falhas permitindo configurar as máquinas virtuais em proteção local e entre sites garantindo a proteção entre os domínios;
4.5.31	Permitir upgrades de Software e Firmware não disruptivos, ou seja, que não necessitem de parada nas Máquinas Virtuais ou Aplicações;
4.6	**ITEM 03 – SOFTWARE PARA ARMAZENAMENTO DE ARQUIVOS E OBJETOS**
4.6.1	Cada unidade deste item deverá prover licenciamento/subscrição de software para armazenamento de 1TB (um terabytes) de arquivos e objetos, com suporte 24x7 e atendimento para chamados críticos em até uma hora, com vigência de 60 (sessenta) meses.
4.6.2	Caso a solução hiperconvergente ofertada não suporte nativamente o armazenamento de arquivos (NFS e SMB) e de objetos (S3), é facultado a LICITANTE o fornecimento de unidade externa dedicada ao armazenamento de dados não estruturados. Neste caso, deverão ser entregues as mesmas capacidades líquidas e utilizáveis mínimas para o armazenamento de arquivos e de objetos. O suporte para ambas as soluções (HCI e storage para dados não estruturados) deverá ser realizado pelo mesmo fabricante;
4.6.3	Em qualquer modelo de oferta, a solução deverá atender aos seguintes requisitos para armazenamento de arquivos:
4.6.4	Compartilhamento através de protocolos NFSv3 e NFSv4 e SMBv2 e SMBv3. A solução deverá estar devidamente dimensionada para suportar o número de 1.500 (um mil e quinhentos) usuários conectados de forma simultânea;

4.6.5	A solução deverá possuir arquitetura na modalidade "scale-out", ou seja, ser possível adicionar nós ou máquinas virtuais de acordo com a necessidade de performance, números de usuários conectados de forma simultânea ou escalabilidade de volumetria;
4.6.6	A solução deverá suportar escalabilidade para pelo menos 5 (cinco) petabytes de volumetria útil;
4.6.7	A solução deverá ser composta de no mínimo 3 nós ou máquinas virtuais, e possuir sistema de Alta
4.6.8	Disponibilidade Nativa para realizar o "fail-over" automático dos serviços para um nó ou máquina virtual remanescente em caso de falha;
4.6.9	Deverá possuir um assistente na própria solução para recomendações de "scale in", adição de recursos de CPU e/ou memória nos nós ou máquinas virtuais existentes ou "scale out", adição de novos nós ou máquinas virtuais com balanceamento de recursos baseado no nível de utilização da solução;
4.6.10	Deverá suportar as seguintes funcionalidades para compartilhamento de arquivos via Protocolo SMB:
4.6.10.1	Autenticação via Active Directory;
4.6.10.2	Filtro de pasta e arquivos para listar apenas aqueles que o usuário possui permissão via Access-based enumeration (ABE);
4.6.11	Habilitar assinatura digital para cada pacote enviado através da rede para assegurar a autenticidade e prevenir adulteração (SMB Signing);
4.6.12	Habilitar encriptação em nível de pasta (SMB Encryption);
4.6.13	Deverá suportar a organização de pastas compartilhadas entre diferentes servidores em um mesmo local ou geograficamente distantes através de um único "Single namespace", inserindo um diretório hierárquico unificado de modo a simplificar a integração com soluções existentes ou futuras atravé do protocolo DFS-N (DFS Namespaces);
4.6.14	Deverá suportar autenticação via "Active Directory", "LDAP" e acesso não gerenciado a compartilhamento via NFSv4 e autenticação via LDAP e acesso não gerenciado via protocolo NFSv3;
4.6.15	Deverá suportar acesso multiprotocolo a uma ou mais pastas, ou seja, ser capaz de prover acesso tanto via SMB quanto via NFS a um mesmo compartilhamento utilizando de protocolos como Windos ACLs (Access Control Lists) e Unix mode bits;
4.6.16	Deverá suportar a configuração de acesso a Home Share por nível de diretório (User Home Shares);
4.6.17	Deverá suportar a otimização de um determinado compartilhamento de acordo com a natureza de tamanho do bloco, sendo possível personalizar entre:
4.6.17.1	Padrão: 64KB por bloco; Randômico: 16KB por bloco; Sequencial: 1MB por bloco;
4.6.21	A solução deverá possuir um painel de visualização de utilização que especifique as seguintes métricas em um intervalo mínimo de 7 dias:
4.6.21.1	Número de arquivos existentes; Capacidade Utilizada;
4.6.21.2	Número de conexões abertas;
4.6.21.3	Espaço consumido por compartilhamento;
4.6.25	A solução deverá possuir um painel de visualização de performance que especifique as seguintes métricas em um intervalo mínimo de 7 dias:

4.6.25.1	Latência; Banda (MB/s);
4.6.25.2	IOPs (I/O por segundo)
4.6.26	Deverá suportar a aplicação de cotas para controle de consumo do sistema de arquivos de forma granular a modo de avisar quando o usuário atingir consumo limite (soft limit) ou bloquear a escrita de novos arquivos (Hard limit). A cota deve ser possível de ser aplicada nos seguintes elementos:
4.6.26.1	Por usuário; Por grupo;
4.6.26.2	Nível da própria pasta no momento de sua criação (Directory Level Quotas)
4.6.27	Deverá suportar o bloqueio de gravação de arquivos baseado em sua extensão a nível de servidor ou pasta, para os protocolos SMB, NFS e compartilhamentos multiprotocolo;
4.6.28	Deverá suportar o envio de eventos de notificação em tempo real como, criação, deleção, leitura, escrita e mudança de permissão em qualquer arquivo armazenado na solução a fim de retenção e auditoria através de soluções como "syslog servers";
4.6.29	Deverá ser fornecido nativamente ou através de integração com software de terceiros, solução que seja capaz de capturar os eventos de notificação e seja capaz de prover de forma simplificada um dashboard de auditoria que forneça no mínimo as seguintes informações:
4.6.29.1	Tendência de capacidade, com foco no que foi consumido e como foi na linha do tempo;
4.6.29.2	Idade dos arquivos, demonstrando cálculo de quando o arquivo foi alterado pela última vez e a porcentagem dos dados baseado no intervalo de variação de sua idade;
4.6.29.3	Detecção de anomalias, demonstrando todas as operações que excedem uma determinada política pré-determina, como a deleção de múltiplos arquivos em um intervalo menor do que 1 (uma) hora;
4.6.29.4	Distribuição por tamanho e tipo de arquivo;
4.6.29.5	Ranking dos usuários mais ativos no sistema de armazenamento; Ranking dos arquivos mais acessados no sistema de armazenamento;
4.6.29.6	Lista das operações mais frequentes (criação, escrita, leitura, deleção e alteração de permissionamento) seja pela média, tendência ou pico da operação;"
4.6.30	A solução de auditoria deverá ser capaz de analisar e reter para consulta um tempo mínimo de 12 (doze) meses de dados capturados;
4.6.31	Deverá suportar a integração de software de anti-vírus de terceiros através do protocolo ICAP (Internet Content Adaptation Protocol) para compartilhamento via SMB e permitir a varredura de arquivos em tempo real quando o arquivo é aberto, fechado ou modificado.
4.6.32	A interface de gerenciamento da solução de armazenamento deverá mostrar o estado do arquivo após varredura de arquivos, tal como modo de quarentena, além dos eventos ocorridos com os mesmos (limpo, quarentena, deletado);
4.6.33	A interface de gerenciamento da solução de armazenamento deverá mostrar a lista de arquivos escaneados, as ameaças detectadas e os arquivos colocados em modo quarentena;
4.6.34	A interface de gerenciamento da solução de armazenamento deverá realizar ações voltadas aos arquivos, tais como:
4.6.34.1	Rescan;
4.6.34.2	Mover os arquivos para fora da Quarentena;
4.6.34.3	Deletar arquivos na quarentena de forma permanente.

4.6.44	Deverá suportar a criação de domínios de proteção de forma automatizada a fim de proteger com cópias locais e remotas a solução de armazenamento, através de agendamentos periódicos de snapshots (horas, dias, semanas e meses)
4.6.45	Deverá suportar a possibilidade de recuperação a nível de arquivo pelo próprio usuário final (self service restore) baseado no agendamento de cópias locais (snapshots) previamente estabelecidos. Para o protocolo SMB a recuperação deverá ser realizada pela propriedade de Versões Prévias da pasta destino. Para o protocolo NFS, através da listagem do subdiretório escondido (snapshot)
4.6.46	Deverá suportar a replicação remota habilitando a recuperação de desastres com intervalo mínimo de um minuto entre cópias para um segundo sistema de armazenamento ou cluster;
4.6.47	Referente ao Serviço de Armazenamento de Objetos, deverá ser configurado de maneira altamente disponível e distribuído, projetado com uma interface de API REST compatível com o Amazon Web Services Simple Storage Service (AWS S3) para lidar com dados não estruturados e gerados por máquina para fins de armazenamento para backup, armazenamento e retenção de longo prazo e desenvolvimento de aplicativos nativos para nuvem usando APIs padrão S3.
4.6.48	Também deverá possuir arquitetura na modalidade "scale-out", ou seja, ser possível adicionar nós, clusters ou máquinas virtuais de acordo com a necessidade de performance, números de requisições ou escalabilidade de volumetria;
4.6.49	A solução deverá estar devidamente dimensionada para suportar o número de 1.500 (mil e quinhentas) requisições por segundo;
4.6.50	A solução deverá possuir um assistente para criação de Object Stores capaz de dimensionar os recursos computacionais necessários com base no número de requisições por segundo e ainda permitir adequação destes recursos antes mesmo da criação do Object Store de acordo com a necessidade;
4.6.51	Permitir a criação de unidades organizacionais lógicas (buckets) para armazenamento dos objetos. Os objetos consistem em dados e metadados que descrevem os dados;
4.6.52	Deverá permitir a configuração de serviços de diretórios, compatível com Microsoft Active Directory e OpenLDAP, para adicionar facilmente pessoas que devem ter acesso a objetos;
4.6.53	Deverá permitir a geração e o controle de chaves de acesso para garantia de segurança;
4.6.54	A solução deverá permitir o compartilhamento dos "buckets" com os usuários que possuem as chaves de acesso, assim como, permitir a delegação de permissões como escrita e leitura de acordo com o nível de acesso
4.6.55	Deverá permitir a listagem dos buckets compartilhados, identificando quais usuários possuem acesso a cada um deles;
4.6.56	Deve ser possível gerenciar os buckets e seus respectivos objetos usando APIs REST compatíveis com a solução de gerenciamento central do cluster ou S3 depois que um administrador autorizar os aplicativos e usuários a acessarem os buckets adequadamente;
4.6.57	A solução deverá permitir o versionamento de múltiplas versões de um objeto dentro de um mesmo bucket. Opção deverá ser possível de ser habilitada na criação ou edição de um bucket existente;
4.6.58	A solução deverá permitir a criação de um conjunto de regras para definir ações do ciclo de vida de um objeto, como permitir que um objeto se apague automaticamente depois de um determinado número de dias, meses ou anos, assim como, apagar determinada versão de um objeto após um determinado período de tempo;

4.6.59	A solução deverá permitir a prevenção da deleção ou alteração de um objeto existente de acordo com um determinado período de retenção, utilizando de algoritmos de WORM (Write-Once-Rean- Many).
4.6.60	A solução deverá possuir painel de visualização de performance que demonstre a quantidade de requisições por segundo, banda utilizada (MB/s) e tempo de leitura de operação de leitura (GET);
4.6.61	Deverá suportar a atribuição de políticas de cotas de utilização notificando os respectivos usuários de acordo com nível de consumo de espaço ou número de buckets criados;
4.6.62	Deverá suportar o envio de eventos de notificação em tempo real como, criação, deleção, leitura, escrita e mudança de permissão em qualquer objeto armazenado na solução a fim de retenção e auditoria através de soluções como "syslog servers";
4.7	**ITEM 04 – SWITCH DE TOR COM 48 PORTAS SFP**
4.7.1	ESPECIFICAÇÕES GERAIS
4.7.1.1	Deve permitir instalação em rack de 19” padrão Telco EIA;
4.7.1.2	Deve possuir altura máxima 1 (um) rack unit (RU);
4.7.1.3	Deve possuir fonte de alimentação interna, do tipo auto-sense, para operar de 100 a 240 VAC;
4.7.1.4	Deve possuir fonte de alimentação redundante interna e hot-swappable;
4.7.1.5	Deve possuir capacidade de **processamento** igual ou superior a 2000 (dois mil) Mpps;
4.7.1.6	Deve possuir capacidade de switching igual ou superior a 4000 (quatro mil) Gbps;
4.7.1.7	Deve possuir latência média de, no mínimo, 0,8 microssegundos.
4.7.1.8	Deve possuir, no mínimo, 48 (quarenta e oito) interfaces 1/10/25GbE compatíveis com SFP, SFP+ e SFP28 usando conectores LC;
4.7.1.9	Deve possuir, no mínimo, 08 (oito) portas 40/100GbE utilizando QSFP+/QSFP28;
4.7.1.10	Todas as portas 40/100GbE devem permitir operação em modo breakout 4x10GbE ou 4x25GbE.
4.7.1.11	Deve ser compatível com SFP 1000BASE-SX, 1000BASE-LX e 1000Base-T;
4.7.1.12	Deve ser compatível com SFP+ 10GBASE-SR,10GBASE-LR, 10GBASE-ER;
4.7.1.13	Deve ser compatível com SFP28 25GBASE-SR, 25GBASE-LR;
4.7.1.14	Deve ser compatível com QSFP+ 40GBASE-SR4, 40GBASE-LR4 e 40G-BiDi;
4.7.1.15	Deve ser compatível com QSFP28 100GBASE-SR4, 100GBASE-LR4 e 100GBASE-CWDM4;
4.7.1.16	Deve possuir pelo menos 32MB de buffer de pacotes;
4.7.1.17	Deve possuir, no mínimo, 4GB de memória DRAM e 32GB de memória NVRAM (flash);
4.7.1.18	Deve permitir empilhamento de até 10 (dez) unidades outros equipamentos em topologia linear e em anel, e permitir gerenciar a pilha com um único endereço IP;
4.7.1.19	Deve possuir banda agregada de empilhamento mínima de 800 (quatrocentos) Gbps, podendo ser através de 4 (duas) portas de 100 (cem) Gbps operando em full-duplex;
4.7.1.20	As interfaces de empilhamento podem ser compartilhadas com as 8 (oito) portas 40/100GbE supracitadas;
4.7.1.21	O equipamento deve permitir empilhamento através de cabos de fibra óptica com distância de pelo menos 10 (dez) km entre cada uma das unidades da pilha;
4.7.1.22	deve possuir ventilação front to back, isto é, o fluxo de ar deve seguir no sentido das portas de interface para as fontes de energia;

4.7.1.23	Deve suportar a inversão do fluxo de ar de ventilação para o modo “back to front” através de pelo menos um dos seguinte métodos: troca de ventiladores e fontes, atualização de firmware ou alteração do arquivo de configuração;
4.7.1.24	Deve possuir porta de gerenciamento “out-of-band” operando a 10/100/1000 Mbps;
4.7.1.25	Deve possuir porta de console para gerenciamento utilizando conector RJ-45, USB, mini-USB ou USB Tipo C;
4.7.1.26	Possui slot USB para inserção de uma mídia de armazenamento removível para fazer upgrade de imagem do switch e backup da configuração;
4.7.1.27	Deve possuir LEDs indicativos de energização, status de slot USB, atividade do link e velocidade das portas;
4.7.1.28	Deve possuir LED de indicação de atividade, velocidade das portas mesmo em modo breakout de forma individual de cada “lane”;
4.7.1.29	Deve permitir realizar troubleshooting visual da unidade na pilha, identificando através de LEDs se o switch é master ou slave da pilha, e sua identificação na pilha;
4.7.1.30	Deve permitir identificar através de sinalização visual onde o switch está localizado no rack através de comandos para ligar e desligar os LEDs do equipamento;
4.7.1.31	Deve possuir botão de reset voltar a para configuração default de fábrica;
4.7.1.32	O proponente deve apresentar carta oficial de revenda autorizada pelo fabricante do equipamento ofertado;
4.7.1.33	A proposta comercial deve descriminar o fabricante e o modelo do equipamento ofertado bem como seus respectivos “P/Ns”;
4.7.1.34	Deve ser novo e em plena fabricação. Não serão aceitos equipamentos com avisos de “End of Life” emitidos pelo fabricante;
4.7.1.35	Deve possuir certificado de homologação junto à ANATEL de acordo a resolução 242 com documentos disponíveis publicamente no sítio público dessa agência na Internet;
4.7.2	**FUNÇÕES DE CAMADA 2**
4.7.2.1	Deve suportar capacidade de no mínimo 200.000 (duzentos mil) endereços MAC;
4.7.2.2	Deve possuir capacidade de configuração de grupos de portas agregadas de acordo com o protocolo IEEE 802.3ad. Deve permitir a configuração de pelo menos 250 (duzentos e cinquenta) grupos de LACP com pelo menos 16 (dezesseis) portas dentro de um mesmo grupo;
4.7.2.3	Deve permiter a configuração de grupos de portas agregadas (LAGs) com balanceamento simétrico, garantindo que o tráfego de um mesmo origem e destino passe pelo mesma porta de um LAG de forma bidirecional;
4.7.2.4	Deve implementar o protocolo IEEE 802.1Q para criação de pelo menos 4000 (quatro mil) vlans ativas;
4.7.2.5	Deve implementar o protocolo IEEE 802.1s (Multiple Spanning Tree), IEEE 802.1w (Rapid Spanning Tree) e IEEE 802.1D (Spanning Tree);
4.7.2.6	Deve ser compatível com o protocolo PVST+;
4.7.2.7	Deve permitir a configuração de pelo menos 250 (duzentas e cinquenta) instâncias de Spanning Tree;
4.7.2.8	Deve implementar BPDU Guard e Root Guard;
4.7.2.9	Deve permitir a configuração de VLANs “trunking” de acordo com o protocolo 802.1Q e VLANs nativas (sem tag) simultaneamente na mesma porta;

4.7.2.10	Deve permitir a criação VLANs privadas;
4.7.2.11	Deve permitar a configuração de VLAN Q-in-Q Tagging de acordo com o padrão IEEE802.1ad ou IEEE802.1QinQ;
4.7.2.12	Deve implementar selective QinQ;
4.7.2.13	Deve implementar para o protocolo UDLD (Uni-Directional Link Detection) ou DLDP (Device Link Detection Protocol) ou similar;
4.7.2.14	Deve implementar jumbo frames até 9000 bytes nas portas Gigabit Ethernet;
4.7.2.15	Deve implementar mecanismos para controle do tráfego broadcasts, multicast e unknown unicast;
4.7.2.16	Deve implementar VPC (Virtual Port Channel), MCT (Multi-Chassis Trunk) ou funcionalidade similar que permita a formação de grupos de portas agregadas com o protocolo IEEE 802.3ad utilizando simultaneamente portas locais e portas de outro equipamento idêntico;
4.7.2.17	Deve implementar mecanismo de detecção ativa de loops através do envio frames de detecção. Na detecção de um evento de loop, deve ser capaz de realizar o bloqueio da porta (port shutdown) ;
4.7.2.18	Deve permitir a configuração de endereços MAC de unicast multicast estáticos em múltiplas portas ethernet simultaneamente, para permitir a configuração de “clusters” de firewalls;
4.7.2.19	Deve implementar IGMP Snooping para IGMPv1, IGMPv2 e IGMPv3;
4.7.2.20	Deve implmenetar MLD snooping v1 e v2;
4.7.2.21	Deve implementar MVRP (Multiple VLAN Registration Protocol);
4.7.2.22	Deve possuir funcionalidade de refletir a tráfego de entrada de uma porta Ethernet, retornando para um gerador de teste para permitindo medir a continuidade da rede e o desempenho da porta ethernet;
4.7.2.23	Deve implementar protocolo de proteção de topologia em anel;
4.7.2.24	Deve implemetar VXLAN;
4.7.2.25	Deve implementar Precision Timing Protocol (PTP) Transparent Clock baseado no padrão IEEE1588v2;
4.7.3	**Funções de camada 3**
4.7.3.1	Deve permitir roteamento local entre VLANs utilizando interfaces virtuais ou SVIs;
4.7.3.2	Deve permitir a configuração de rotas estáticas usando endereços IPv4 e IPv6;
4.7.3.3	Deve permitir a configuração de endereço IPv6 com prefixo de 127 bits para links point-to-point;
4.7.3.4	Deve implementar roteamento IP usando os protocolos RIPv1/v2 e RIPng;
4.7.3.5	Deve implementar roteamento IP usando os protocolos OSPFv2 e OSPFv3;
4.7.3.6	Deve implementar roteamento usando o protocolo BGP4 e BGP4+;
4.7.3.7	Deve implementar BFD (bidirectional forwarding detection) para rotas estáticas, OSPFv2, OSPFv3, BGP4 e BGP4+;
4.7.3.8	Deve implementar criação de túneis GRE;
4.7.3.9	Deve implementar VRF ou VRF-lite, com suporte a pelo menos 128 (cento e vinte e oito) instâncias;
4.7.3.10	Deve implementar os protocolos VRRP e VRRPv3;
4.7.3.11	Deve implementar ECMP com no mínimo 32 (trinta e dois) caminhos;
4.7.3.12	Deve implementar os protocolos de roteamento de multicast PIM-S, PIM-SSM e PIM-DM;

4.7.3.13	Deve suportar PIM-Passive para reduzir e minimizar tráfego de controle.
4.7.3.14	Deverá possuir no mínimo 500 (quinhentas) interfaces virtuais para roteamento entre VLANs
4.7.3.15	Deve permitir a configuração de pelo menos 2.000 (duas mil) rotas estáticas IPv4;
4.7.3.16	Deve permitir a configuração de pelo menos 1.000 (mil) rotas estáticas IPv6;
4.7.3.17	Deverá suportar a capacidade pelo menos 300.000 (trezentas mil) entradas em sua tabela de roteamento IPv4;
4.7.3.18	Deverá suportar a capacidade de pelo menos 35.000 (trinta e cinco mil) entradas em sua tabela de roteamento IPv6;
4.7.3.19	Deve possuir DHCP Server para IPv4 e IPv6;
4.7.3.20	Deve permitir a configuração de DHCP Relay;
4.7.3.21	Deve implementar PBR (Policy-Based Routing) para IPv4 e IPv6;
4.7.3.22	Deve implementar IPv6 router advertisement (RA) preference na mensagem de RA com informações de múltiplos routers para a escolher a rota default apropriada pelo host IPv6;
4.7.4	**Qualidade de Serviço**
4.7.4.1	Deve pemitir priorização de tráfego usando 8 (oito) filas de priorização por porta;
4.7.4.2	Deve permitir priorização de tráfego baseado no padrão IEEE 802.1p e no campo DSCP do protocolo Diffserv;
4.7.4.3	Deve implementar pelos menos os seguintes métodos para configuração das filas de priorização: ponderada, prioridade estrita e ambas combinadas;
4.7.4.4	Implementar priorização de tráfego baseado em porta física, protocolo IEEE 802.1p, endereços IP de origem e destino e portas TCP/UDP de origem e destino;
4.7.4.5	Deve permitir a configuração de Rate Limiting de entrada;
4.7.4.6	Deve permitir a configuração de Rate Shaping de saída;
4.7.4.7	Deve implementar os seguintes algoritmos de fila: Strict Priority e Round Robin com distribuição de pesos WRR (Weighted Round Robin) e uma combinação entre os dois métodos SP e WRR;
4.7.5	**Segurança**
4.7.5.1	Deve permitir autenticação de usuários usando o padrão IEEE 802.1x, permitindo associação dinâmica de VLANs e ACLs usando profiles definidas por um servidor RADIUS externo;
4.7.5.2	Deve permitir a associação de VLANs restritas para usuários que falhem durante a autenticação 802.1X;
4.7.5.3	Implementar método de autenticação baseado em endereço MAC para os dispositivos que não possuirem suplicantes 802.1X;
4.7.5.4	Deve possuir capacidade de autenticação 802.1x com atribuição de VLAN, regras de acesso de segurança e QoS individuais para, no mínimo, 02 (dois) dispositivos (Ex.: Telefone IP e PC) conectados em uma única porta e usando VLANs distintas;
4.7.6	**Deve permitir, no mínimo e em cada porta, os seguintes tipos de autenticação usando VLANs distintas:**
4.7.6.1	2 (dois) dispositivos que suportam o padrão IEEE 802.1x;
4.7.6.2	2 (dois) dispositivos MAC que não suportam o padrão IEEE 802.1x;
4.7.6.3	1 (um) dispositivo que suporta o padrão IEEE 802.1x e 1 (um) dispositivo MAC que não suporta o padrão IEEE 802.1x;

4.7.6.4	O equipamento deve permitir a configuração de reautenticação 802.1x periódica;
4.7.6.5	O equipamento ofertado deve permitir a autenticação via Web Authentication para usuários que não possuem 802.1x;
4.7.6.6	Deve implementar “Change of Authorization” de acordo com a RFC 5176;
4.7.6.7	Deve permitir a autenticação de usuários para acesso às funções de gerenciamento usando-se os protocolos RADIUS e TACACS+;
4.7.6.8	Deve permitir a criação de ACLs para a filtragem de tráfego IPv4 baseado no endereço IP de origem e destino, portas TCP e UDP de origem e destino, bits do protocolo 802.1p e campo DSCP do protocolo Diffserv;
4.7.6.9	Deve permitir a criação de ACLs para a filtragem de tráfego IPv6 baseado no endereço IP de origem e destino, portas TCP e UDP de origem e destino, campo PCP do protocolo 802.1p e campo DSCP do protocolo Diffserv;
4.7.6.10	Deve implementar ACLs de entrada e ACLs de saída para IPv4;
4.7.6.11	Deve implementar ACLs de entrada e ACLs de saída para IPv6;
4.7.6.12	Deve implementar segurança de acesso baseada em endereços MAC de origem, com a possibilidade de bloqueio permanente ou temporário das portas onde for detectada uma violação de segurança;
4.7.6.13	Deve permitir a criação de filtros de endereço MAC de origem e destino;
4.7.6.14	Deve possuir protocolos para proteção de ataques de Denial of Service;
4.7.6.15	Deve possuir funcionalidade de proteção contra servidores DHCP não autorizados DHCPv4 snooping e DHCPv6 snooping;
4.7.6.16	Deve possuir funcionalidade de proteção contra ataques do tipo “ARP Poisoning”;
4.7.6.17	Deve permitir a configuração de Dynamic ARP Inspection em pelo menos 500 vlans;
4.7.6.18	Deve implementar IP Source Guard;
4.7.6.19	Deve implementar proteção contra ataques do tipo TCP SYN e ataques do tipo Smurf;
4.7.6.20	Deve permitir o monitoramento da movimentação de um endereço MAC de uma porta para outra, facilitando a distinção entre um movimento legítmo com um movimento malicioso de um ataque de MAC spoofing;
4.7.6.21	Deve implementar IPv6 RA guard e IPv6 ND inspection;
4.7.6.22	Deve implementar RADsec conforme RFC6614;
4.7.6.23	Deve implementar unicast Reverse Path Forwarding (uRPF) como ferrametna para evitar ataques do tipo source IP spoofing;
4.7.7	**Gerenciamento**
4.7.7.1	Deve permitir monitoração e configuração usando SNMP v1, v2 e v3;
4.7.7.2	Deve permitir o gerenciamento via SNMPv3 com as seguintes opções: sem autenticação e sem privacidade, com autenticação e sem privacidade e com autenticação e com privacidade;
4.7.7.3	Deve ser possível enviar “traps” e realizar o gerenciamento via SNMP através das redes IPv4 e IPv6;
4.7.7.4	Deve permitir a configuração de porta para espelhamento de tráfego, para a coleta de pacotes em analisadores de protocolo ou detecção de intrusão;
4.7.7.5	Deve permitir espelhamento de tráfego baseado em Porta, VLAN, Filtro MAC e ACL;
4.7.7.6	Deve permitir a configuração de porta para espelhamento de tráfego para uma porta em um switch remoto;

4.7.7.7	Deve implementar gerenciamento usando SSH v2 utilizando os algoritimos de criptografia 3DES e AES. Deve ser permitido a utilização de endereços IPv4 e IPv6 para a funcionalidade solicitada;
4.7.7.8	Deve implementar gerenciamento via Telnet. Deve ser permitido a utilização de endereços IPv4 e IPv6 para a funcionalidade solicitada;
4.7.7.9	Deve permitir o monitoramento dos transceivers óticos, retornando informação de temperatura, potência de transmissão (dBm), potência de recepção (dBm) e status;
4.7.7.10	Deve permitir a atualização de arquivos de configuração e imagens de firmware usando TFTP ou FTP. Em ambos os casos deve ser permitido a utilização de redes IPv4 e IPv6 para a funcionalidade solicitada;
4.7.7.11	Deve permitir a atualização de imagens de firmware dos equipamentos de uma pilha sem a necessidade de reinicialização simultânea de todos os equipamentos da pilha, permitindo a continuidade do tráfego de dados durante o processo de atualização;
4.7.7.12	Deve permitir configuração automática do seu próprio endereço IP e a seguir carga automática de um arquivo de configuração pré-definido, usando um servidor DHCP e um servidor TFTP ou FTP;
4.7.7.13	Deve implementar o protocolo LLDP conforme o padrão IEEE 802.1AB, bem como LLDP-MED;
4.7.7.14	Deve permitir o monitoramento de tráfego através dos protocolos sFlow, NetFlow ou IPFIX. Deve ser possível exportar o tráfego de redes IPv4 e IPv6;
4.7.7.15	Deve permitir a configuração de seu relógio interno de forma automática através do protocolo NTP. Em ambos os casos deve ser permitido a utilização de redes IPv4 e IPv6 para a funcionalidade solicitada;
4.7.7.16	Deve permitir armazenamento simultâneo de duas imagens de firmware em memória flash.
4.7.7.17	Deve permitir atualização de imagem de firmware através de mídia de armazenamento externa conectado ao slot USB;
4.7.7.18	Deve permitir o envio de mensagens de syslog à pelo menos 2 servidores distintos. Deve ser permitido a utilização de redes IPv4 e IPv6 para a funcionalidade solicitada;
4.7.7.19	Deve permitir o envio de syslog com formato conforme RF5424 para prover mais informações no seu header;
4.7.7.20	Deve implementar funcionalidade de rollback automático de configuração, permitindo que o switch retorne automaticamente para uma configuração estável prévio caso o administrador não confirmar a alteração realizada dentro de um prazo de tempo configurável.
4.8	**ITEM 5 - IMPLANTAÇÃO, CONFIGURAÇÃO E REPASSE DE CONHECIMENTO**
4.8.1	**REQUISITOS DO PROJETO DE IMPLANTAÇÃO (montagem, instalação e configuração)**
4.8.1.1	A equipe de servidores do setor de infraestrutura da FUNDAÇÃO BIBLIOTECA NACIONAL deverá verificar se a aquisição está de acordo com as especificações do contrato. Após verificação, não constatando nenhuma inconformidade, deverá seguir o projeto de implantação junto à CONTRATADA.
4.8.1.2	O responsável pela instalação deverá comunicar a FUNDAÇÃO BIBLIOTECA NACIONAL com antecedência, informando-lhe a forma e período de instalação. Após a instalação, deverá ser também comunicada a equipe de contratação, para as devidas providências formais de recebimento.
4.8.1.3	Os seguintes requisitos devem ser observados:

4.8.1.4	Os serviços de instalação física e lógica deverão ser executados pela CONTRATADA, e seguirão as fases de abertura do projeto, de planejamento, de execução e fase de documentação, conforme detalhamento a seguir; Para a fase de abertura:
4.8.1.5	Validar e homologar escopo do projeto; Validar objetivos e premissas do projeto; Validar riscos e restrições do projeto;
4.8.1.6	Identificar e validar os requisitos do projeto. Para a fase de planejamento:
4.8.1.7	Elaborar plano de projeto;
4.8.1.8	Definir as pessoas envolvidas por parte da FUNDAÇÃO BIBLIOTECA NACIONAL no projeto; Reunir as equipes da CONTRATADA e da FUNDAÇÃO BIBLIOTECA NACIONAL ;
4.8.1.9	Apresentação do cronograma do projeto com os prazos e responsabilidades; Verificar os pré-requisitos do projeto;
4.8.1.10	Apresentar plano do projeto para a homologação por parte da FUNDAÇÃO BIBLIOTECA NACIONAL.
4.8.1.11	O serviço de instalação consiste na colocação dos equipamentos em pleno funcionamento, em conformidade com o disposto nesta especificação técnica e seus anexos, e em perfeitas condições de operação, de forma integrada ao ambiente de infraestrutura de informática da FUNDAÇÃO BIBLIOTECA NACIONAL e deve contemplar, no mínimo, o seguinte:
4.8.1.12	Instalação física do appliance/nó no local indicado pela FUNDAÇÃO BIBLIOTECA NACIONAL;
4.8.1.13	Conexão e configuração do(s) nó(s) nos equipamentos de rede da FUNDAÇÃO BIBLIOTECA NACIONAL; Atualização de softwares, firmwares e drives que compõem a solução;
4.8.1.14	A CONTRATADA deverá garantir todos os equipamentos, componentes, acessórios e cabos de conexão para interligar fisicamente todos os componentes da solução entregue;
4.8.1.15	Aplicação das licenças de todos os softwares relacionados, incluindo mas não se limitando a virtualização, gerenciamento, SDN e SDS com respectivos serviços de armazenamento de blocos (iSCSI), arquivos (NFS e SMB) e objetos (S3);
4.8.1.16	Configuração das funcionalidades de desduplicação, compressão e aceleração (caso aplicável);
4.8.1.17	Entrega, por parte da CONTRATADA, da documentação completa do ambiente configurado e instalado.
4.8.1.18	A instalação física do equipamento será realizada pela fornecedora da solução, com acompanhamento de uma equipe destacada pela FUNDAÇÃO BIBLIOTECA NACIONAL;
4.8.1.19	A CONTRATADA deverá providenciar um profissional certificado pelo fabricante na solução para garantir a conformidade da instalação e a configuração dos equipamentos e softwares que compõem a solução.
4.8.1.20	A instalação, configuração e testes do equipamento deverão ser feitos com o acompanhamento de técnicos da FUNDAÇÃO BIBLIOTECA NACIONAL, visando o repasse de conhecimentos e observados os padrões de segurança da Instituição;
4.8.1.21	O equipamento deverá estar com todas as funcionalidades e recursos de hardware e software solicitados disponíveis e configurados. Os sistemas de gerenciamento também deverão estar ativos e em pleno funcionamento, levando em consideração todas as características solicitadas;

4.8.1.22	A instalação e a configuração dos equipamentos deverão ocorrer preferencialmente em dias úteis, em horário comercial, ficando a cargo da FUNDAÇÃO BIBLIOTECA NACIONAL a definição dos horários para configuração do equipamento em produção. Atividades a serem realizadas fora deste horário, assim como a necessidade de interrupção de serviços em produção, estarão sujeitas à aprovação prévia da equipe técnica da FUNDAÇÃO BIBLIOTECA NACIONAL.
4.8.2	**As atividades de instalação deverão ser acompanhadas na modalidade hands-on (aprender fazendo), devendo a CONTRATADA:**
4.8.2.1	Efetuar o hands-on com carga horária de, no mínimo, 8 (oito) horas, para o repasse de conhecimento do as-built, com a transferência das informações básicas de operação e conteúdo de referência de alguns tópicos do treinamento;
4.8.2.2	O repasse de informações deverá cobrir conhecimentos necessários para instalação, administração, configuração, otimização, resolução de problemas e utilização da solução;
4.8.2.3	A FUNDAÇÃO BIBLIOTECA NACIONAL, responsável pela infraestrutura, deverá disponibilizar 3 (três) técnicos para o acompanhamento das atividades de hands-on;
4.8.2.4	Independente da quantidade contratada, ou do número de nós adquiridos da solução, a atividade de hands-on será executada apenas 1 (uma) vez, com relação ao escopo e carga horária definidos;
4.8.2.5	As horas de acompanhamento do hands-on deverão ser distribuídas ou organizadas da melhor maneira durante as atividades de instalação/configuração, mediante proposição da equipe técnica da FUNDAÇÃO BIBLIOTECA NACIONAL;
4.8.2.6	Não serão recebidos os serviços de hands-on prestados por profissionais que não estejam hábeis a demonstrar, na prática, as funcionalidades principais dos equipamentos e, particularmente, as atividades relacionadas à operação da solução;
4.8.2.7	A não realização do hands-on implicará na não aceitação da entrega definitiva do serviço;
4.8.2.8	Todas as despesas com instrutor(es), seu(s) deslocamento(s) e demais itens relacionados ao repasse do handson serão de responsabilidade da CONTRATADA;
4.8.2.9	A empresa deverá declarar, na proposta, que não realizará subcontratação para a execução dos serviços.

5. PRAZO PARA ENTREGA E CRITÉRIOS DE ACEITAÇÃO DO OBJETO

5.1. Os equipamentos deverão ser entregues na Fundação Biblioteca Nacional, Av. Rio Branco, 219, Rio de Janeiro, RJ – 20.040-008 , em até 60 (sessenta) dias corridos, a partir do recebimento da Autorização de fornecimento.

5.2. Os equipamentos serão avaliados pelo responsável pelo acompanhamento e fiscalização da Autorização de fornecimento, para efeito de posterior verificação de sua conformidade conforme especificações no Termo de Referência e na proposta.

5.3. Os equipamentos poderão ser rejeitados, quando em desacordo com as especificações constantes no Termo de Referência e na proposta, devendo ser substituído no prazo de **até 15 (quinze) dias**, a contar da notificação da contratada, às suas custas, sem prejuízo de aplicação das penalidades.

6. LOCAL DE ENTREGA E CONDIÇÕES DE FORNECIMENTO

6.1. Os equipamentos deverão ser entregues no seguinte endereço: **Local:** Fundação Biblioteca Nacional, Av. Rio Branco, 219, Rio de Janeiro, RJ – 20.040-008**– Horário de 09:00h às aos A/C: Coordenador de Tecnologia da Informação.**

6.2. Os equipamentos serão recebidos:

6.2.1. Provisoriamente, no ato da entrega, para efeito de posterior verificação da conformidade dos equipamentos com a especificação, oportunidade em que se observarão apenas as informações constantes da fatura e das embalagens, em confronto com a respectiva nota de empenho;

6.2.2. Definitivamente, após a verificação da qualidade e quantidade dos equipamentos e consequente aceitação, que deverá acontecer em até **05 (cinco) dias úteis**, contados a partir do recebimento provisório.

6.3. O descarregamento dos equipamentos ficará a cargo do fornecedor, devendo ser providenciada a mão-de-obra necessária.

7. VALOR GLOBAL ESTIMADO DA CONTRATAÇÃO

7.1. O valor global estimado para aquisição dos equipamentos (solução) será na ordem de R$ 4.250.000,00 (Quatro milhões, duzentos e cinquenta mil reais).

7.2. O valor global informado acima é estimativo e não indica qualquer compromisso futuro para a Contratante. Somente será realizado o pagamento do equipamento efetivamente entregue(s) de acordo com as especificações estabelecidas nesse Termo de Referência.

7.3. Por se tratar de investimento proveniente de financiamento público, caso a financiadora descontinue o projeto, por qualquer razão, a Autorização de fornecimento e/ou contrato, fruto deste Termo de Referência também terá seu pagamento suspenso.

8. FONTE DE RECURSO

8.1. As despesas decorrentes da presente Seleção Pública correrão à conta dos recursos consignados no Projeto intitulado "**Resgate e Preservação do Acervo Científico da Biblioteca Nacional"**, Convênio 01.25.0095.00 - Ref.: 3067/24.

9. CONDIÇÕES DE PAGAMENTO

9.1. O pagamento será realizado conforme o **Item 9.4 – Críterios de medição e de pagamento,** desse Termo de referência.

9.2. A Nota Fiscal ou Fatura apresentada deverá conter expressamente os elementos necessários e essenciais do documento, tais como:

a) A data de Emissão;
b) Prazo de Validade;
c) Os dados do Contrato e do órgão Contratante;
d) O período do fornecimento;
e) O valor a pagar; e
f) Eventual destaque do valor de retenções tributárias cabíveis.

9.3. Havendo erro na apresentação da Nota Fiscal/Fatura, ou circunstância que impeça a liquidação da despesa, o pagamento ficará sobrestado até que a Contratada providencie as medidas saneadoras. Nesta hipótese, o prazo para pagamento iniciar-se-á após a comprovação da regularização da situação, não acarretando qualquer ônus para a Contratante.

9.4. CRITÉRIOS DE MEDIÇÃO E DE PAGAMENTO

9.4.1. Após o recebimento dos itens 1, 2, 3 e 4, constantes no **Item 3 - DESCRIÇÃO DO OBJETO E QUANTIDADE,** será emitido o Termo de Recebimento Provisório (TRP) – Anexo I, a fim de garantir que os itens foram entregues dentro do prazo e especificações estipulado.

9.4.2. O Termo de Recebimento Definitivo (TRD) – Anexo II, será emitido em até 10 (dez) dias úteis após a emissão do Termo de Recebimento Provisório (TRP), desde que todos os itens 1, 2, 3, 4 e 5 estejam devidamente instalados, configurados e em pleno funcionamento, conforme as condições estabelecidas no Termo de Referência e seus respectivos anexos.

9.4.3. O prazo para pagamento será de até 15 (quinze) dias após a entrega do Termo de Recebimento Definitivo (TRD) e emissão da Nota Fiscal devidamente atestada pelo setor competente.

9.4.4. O pagamento será realizado desde que constatado o adimplemento das obrigações contratuais, emissão do Termo de Recebimento Definitivo (TRD) e Plano de Execução – ANEXO III, conforme os critérios abaixo:

ITEM	OBJETO	EVENTO DE PAGAMENTO
1	Hardware para Infraestrutura Hiperconvergente (HCI), incluindo, suporte técnico "onsite" dentro da garantia de 60 meses.	Após entrega, instalação, validação técnica, execução dos serviços, apresentação de relatórios e emissão do Termo de Recebimento Definitivo (TRD).
2	Software para HCI com subscrição e suporte 24x7 durante 60 meses, por núcleo de processamento (core).	
3	Software para armazenamento de arquivos e objetos, com subscrição e suporte 24x7 durante 60 meses, por terabyte de dados.	
4	Switches TOR 48 portas, incluindo, serviço de implantação, configuração, repasse de conhecimento, suporte técnico "onsite" dentro da garantia de 60 meses.	
5	Implantação, configuração repasse de conhecimento	

9.5. GARANTIA, MANUTENÇÃO E ASSISTÊNCIA TÉCNICA

9.5.1. O prazo de garantia contratual dos bens, complementar à garantia legal, é 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.

9.5.2. 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.

9.5.3. A garantia abrange a realização da manutenção corretiva dos bens pelo próprio CONTRATADA, ou, se for o caso, por meio de assistência técnica autorizada, de acordo com as normas técnicas específicas.

9.5.4. 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.

9.5.5. 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.

9.5.6. Uma vez notificado, a CONTRATADA realizará a reparação ou substituição dos bens que apresentarem vício ou defeito no prazo de até 10 (dez) dias úteis, contados a partir da data de retirada do equipamento das dependências da CONTRATANTE pela CONTRATADA ou pela assistência técnica autorizada.

9.5.7. O prazo indicado no subitem anterior, durante seu transcurso, poderá ser prorrogado uma única vez, por igual período, mediante solicitação escrita e justificada da CONTRATADA, aceita pelo CONTRATANTE.

9.5.8. Na hipótese do subitem acima, a CONTRATADA 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.

9.5.9. Decorrido o prazo para reparos e substituições sem o atendimento da solicitação do CONTRATANTE ou a apresentação de justificativas pelo CONTRATADA, 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.

9.5.10. O custo referente ao transporte dos equipamentos cobertos pela garantia será de responsabilidade do CONTRATADA.

9.5.11. A garantia legal ou contratual do objeto tem prazo de vigência própria 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.

9.5.12. A empresa CONTRATADA deverá fornecer recurso, disponibilizado via site do próprio fabricante (informar URL para comprovação), que faça a validação e verificação da garantia do equipamento através da inserção do seu número de série e/ou modelo/número do equipamento;

9.5.13. A manutenção deve ser proativa buscando, através do monitoramento contínuo da solução de TI, identificar as causas básicas das falhas para acionar de forma automatizada a equipe para o reparo. Tal manutenção deve ter o objetivo de restaurar as condições iniciais e ideais de operação de máquinas e equipamentos, eliminando as fontes de falhas que possam existir, podendo ocorrer na modalidade on-site (no ambiente da CONTRATADA) ou não;

9.5.14. As manutenções de caráter corretivo emergencial devem ser realizadas após a falha funcional do equipamento e, portanto, o equipamento deve ser reparado em caráter de urgência. Havendo necessidade de remoção do equipamento para as dependências da CONTRATADA, as despesas de transporte, seguros e embalagens correrão por conta da CONTRATADA;

9.5.15. No caso de retirada de qualquer equipamento, a CONTRATADA deverá assinar termo de retirada, se responsabilizando integralmente pelo equipamento (hardware e software), enquanto ele estiver em suas dependências ou em trânsito sob sua responsabilidade.

9.5.16. Somente os técnicos da CONTRATADA, ou pessoas a quem ela autorizar por escrito, poderão executar os serviços de manutenção. Os técnicos, ou pessoas autorizadas pela CONTRATADA, deverão apresentar, no ato do atendimento, credenciamento (crachá da empresa) e documento de identidade pessoal (RG), para efetuar qualquer serviço nas dependências a CONTRATANTE.

9.5.17. O regime de atendimento (Central de Atendimento) da assistência técnica indicada pela fornecedora deve ser de 8 (oito) horas por dia, 5 (cinco) dias da semana, em dias úteis.

9.5.18. Após o início da operação a Solução deve ser acompanhada pelos técnicos da CONTRATADA, de forma presencial por 03 (três) dias.

9.6. SANÇÕES ADMINISTRATIVAS E PROCEDIMENTOS PARA RETENÇÃO OU GLOSA NO PAGAMENTO

9.6.1. Nos casos de inadimplemento na execução do objeto, as ocorrências serão registradas pela Contratante, conforme métricas abaixo:

9.6.2. 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

9.6.3. Serão aplicadas ao contratado que incorrer nas infrações acima descritas as seguintes sanções:

I. Advertência, quando o contratado der causa à inexecução parcial do contrato, sempre que não se justificar a imposição de penalidade mais grave (art. 156, §2º, da Lei nº 14.133, de 2021);

II. Impedimento de licitar e contratar, quando praticadas as condutas descritas nas alíneas “b”, “c” e “d” do subitem acima deste Contrato, sempre que não se justificar a imposição de penalidade mais grave (art. 156, § 4º, da Lei nº 14.133, de 2021);

III. Declaração de inidoneidade para licitar e contratar, quando praticadas as condutas descritas nas alíneas “e”, “f”, “g” e “h” do subitem acima deste Contrato, bem como nas alíneas “b”, “c” e “d”, que justifiquem a imposição de penalidade mais grave (art. 156, §5º, da Lei nº 14.133, de 2021).

9.6.4. Multa:

I. moratória de 10% (dez por cento) por dia de atraso injustificado sobre o valor da parcela inadimplida, até o limite de 60 (sessenta) dias;

II. moratória de 0,07% (sete centésimo 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.

III. O atraso superior a 25 (vinte e cinco) dias 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.

IV. Compensatória, para as infrações descritas nas alíneas “e” a “h” do subitem 12.1, de 10% a 20% do valor do Contrato.

V. Compensatória, para a inexecução total do contrato prevista na alínea “c” do subitem 12.1, de 10% a 20% do valor do Contrato.

VI. Para infração descrita na alínea “b” do subitem 12.1, a multa será de 20% a 30% do valor do Contrato.

VII. Para infrações descritas na alínea “d” do subitem 12.1, a multa será de 10% a 20% do valor do Contrato.

VIII. Para a infração descrita na alínea “a” do subitem 12.1, a multa será de 5% a 10% do valor do Contrato.

IX. A aplicação das sanções previstas neste Contrato não exclui, em hipótese alguma, a obrigação de reparação integral do dano causado ao Contratante (art. 156, §9º, da Lei nº 14.133, de 2021).

X. Todas as sanções previstas neste Contrato poderão ser aplicadas cumulativamente com a multa (art. 156, §7º, da Lei nº 14.133, de 2021).

XI. Antes da aplicação da multa será facultada a defesa do interessado no prazo de 15 (quinze) dias úteis, contado da data de sua intimação (art. 157, da Lei nº 14.133, de 2021).

XII. 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 (art. 156, §8º, da Lei nº 14.133, de 2021).

XIII. Previamente ao encaminhamento à cobrança judicial, 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.

XIV. 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.

9.6.5. Na aplicação das sanções serão considerados (art. 156, §1º, da Lei nº 14.133, de 2021):

a) a natureza e a gravidade da infração cometida;

b) as peculiaridades do caso concreto;

c) as circunstâncias agravantes ou atenuantes;

d) os danos que dela provierem para o CONTRATANTE;

e) a implantação ou o aperfeiçoamento de programa de integridade, conforme normas e orientações dos órgãos de controle.

9.7. 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 (art. 159).

9.8. 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 Contrato 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 (art. 160, da Lei nº 14.133, de 2021).

9.9. 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. (Art. 161, da Lei nº 14.133, de 2021).

9.10. 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 14.133/21.

10. EXIGÊNCIAS ESPECÍFICAS DE HABILITAÇÃO

10.1. A relação dos documentos referente a habilitação jurídica, regularidade fiscal e econômico-financeira constam informadas no Edital.

10.2. **Da Documentação Relativa à Capacitação Técnica**

10.2.1. Apresentação de no mínimo 01 (um) atestado de capacidade técnica, declaração ou certidão, emitida por pessoa jurídica de direito público ou privado, comprovando que a proponente forneceu equipamento(s), material(is) e/ou produto(s) do Lote 1, compatível em características e/ou com complexidade igual ou superior ao objeto desta Seleção Pública, com boa avaliação por parte do emissor.

I. O atestado deverá estar emitido em papel timbrado do órgão ou da Empresa que o expediu, ou deverá conter carimbo do CNPJ do mesmo ou outra informação que permita a devida identificação do emitente.

II. O atestado de capacidade técnica poderá ser apresentado em nome da empresa, com CNPJ da matriz e/ou da filial do Proponente.

III. Não será aceito atestado de capacidade técnica emitido pelo próprio proponente.

IV. O(s) atestado(s) de capacidade técnica deverá(ão) ser apresentado(s) o(s) original(is), ou por meio de **cópia autenticada** por cartório competente.

V. Para fins da comprovação de que trata este subitem, deve ser fornecido Atestado de Capacidade Técnico Operacional, comprovando entrega de soluções similares aos que se pretende adquirir em quantidade mínima de 50% (cinquenta) do item 1, 30% (trinta) do item 2 e 20% (vinte) do item 4 do lote 1.

VI. Será admitida, para fins de comprovação de quantitativo mínimo, a apresentação e o somatório de diferentes atestados executados de forma concomitante.

11. FUNDAMENTAÇÃO, NORMAS E REGULAMENTOS

11.1. Nos termos do Decreto Federal nº 8.241/2014 (Dispõe sobre a aquisição de bens e a contratação de obras e serviços pelas fundações de apoio) e subsidiariamente, no que for cabível, nos termos do Decreto Federal nº 10.024/2019 (Regulamenta a licitação, na modalidade pregão, na forma eletrônica, para a aquisição de bens e a contratação de serviços comuns, incluídos os serviços comuns de engenharia, e dispõe sobre o uso da dispensa eletrônica, no âmbito da administração pública federal.) e Lei nº 14.133/2021 (Lei de Licitações e Contratos Administrativos).

11.2. Fica a cargo dos interessados a responsabilidade de tomar conhecimento de todos os

esclarecimentos, atas, comunicados, recursos, decisões e quaisquer outras comunicações, devidamente publicados no site da Fundação na área de Editais (www.facc10.org.br).

12. CONSIDERAÇÕES GERAIS

12.1. A FACC, mediante simples comunicação, poderá, a qualquer tempo, alterar padrões, critérios, parâmetros e normas, mediante substituições e/ou supressões, desde que não alterem o objeto deste Termo de Referência.

Petrópolis, XX de ..... de 202x.

Assinado eletronicamente por:

FUNDAÇÃO DE APOIO AO DESENVOLVIMENTO DA COMPUTAÇÃO CIENTÍFICA – FACC

Francisco Roberto Leonardo
Diretor Geral

Flávio Barbosa Toledo
Diretor Administrativo-Financeiro

FUNDAÇÃO BIBLIOTECA NACIONAL - FBN

Marco Américo Lucchesi
Presidente

Maria José da Silva Fernandes
Coordenadora do Projeto

ANEXO II - TERMO DE RECEBIMENTO PROVISÓRIO – COMPRAS DE TIC

1 – IDENTIFICAÇÃO			
CONTRATO/NOTA DE EMPENHO Nº	xx/aaaa		
CONTRATADA	<Nome da Contratada>	**CNPJ**	xxxxxxxxxxxx
Nº DA OFB	<xxxx/aaaa>		
DATA DA EMISSÃO	<dd/mm/aaaa>		

2 – ESPECIFICAÇÃO DOS PRODUTO(S)/BEM(S) E VOLUMES DE EXECUÇÃO			
SOLUÇÃO DE TIC			
<Descrição da solução de TIC solicitada relacionada ao contrato anteriormente identificado>			
ITEM	**DESCRIÇÃO DO BEM OU SERVIÇO**	**MÉTRICA**	**QUANTIDADE**
1	<Descrição igual ao da OFB de abertura>	<Ex.: UNID.>	<n>
...	...	...	...
...	...	...	...
...	...	...	...
TOTAL DE ITENS			

3 – RECEBIMENTO

Por este instrumento ATESTO que os <bem(s)/produto(s)> correspondentes à <OFB> acima identificada, conforme definido no Modelo de Execução do contrato supracitado, foram entregues, estando sujeitos à avaliação específica para verificação do atendimento às demais exigências contratuais, de acordo com os Critérios de Aceitação previamente definidos no Modelo de Gestão do contrato.

Ressaltamos que o recebimento definitivo destes <bem(s)/produto(s)> ocorrerá somente após a verificação desses requisitos e das demais condições contratuais, desde que não se observem inconformidades ou divergências quanto às especificações constantes do Termo de Referência e do Contrato acima identificado que ensejem correções por parte da **CONTRATADA**. Por fim, reitera-se que o objeto poderá ser rejeitado, no todo ou em parte, quando estiver em desacordo com o contrato.

4 – ASSINATURA
FISCAL TÉCNICO
_____ <Nome do Fiscal Técnico do Contrato> **Matrícula:** xxxxxx <Local>, <dia> de <mês> de <ano>.
PREPOSTO
_____ <Nome do Preposto do Contrato> **Matrícula**: xxxxxx <Local>, <dia> de <mês> de <ano>.

ANEXO III - TERMO DE RECEBIMENTO DEFINITIVO

1 – IDENTIFICAÇÃO			
CONTRATO/NOTA DE EMPENHO Nº	xx/aaaa		
CONTRATADA	<Nome da Contratada>	**CNPJ**	xxxxxxxxxxxx
Nº DA OS/OFB	<xxxx/aaaa>		
DATA DA EMISSÃO	<dd/mm/aaaa>		

2 – ESPECIFICAÇÃO DOS PRODUTO(S)/BEM(S)/SERVIÇOS E VOLUMES DE EXECUÇÃO

SOLUÇÃO DE TIC

<descrição da solução de TIC solicitada relacionada ao contrato anteriormente identificado>

ITEM	DESCRIÇÃO DO BEM OU SERVIÇO	MÉTRICA	QUANTIDADE	TOTAL
1	<descrição igual à da OS/OFB de abertura>	<Ex.: PF>	<n>	<total>
...				
TOTAL DE ITENS				

3 – ATESTE DE RECEBIMENTO

Por este instrumento ATESTO/ATESTAMOS que o(s) <serviço(s)/ bem(s)> correspondentes à <OS/OFB> acima identificada foram <prestados/entregues> pela **CONTRATADA** e ATENDEM às exigências contratuais, discriminadas abaixo, de acordo com os Critérios de Aceitação previamente definidos no Modelo de Gestão do Contrato acima indicado.

ITEM	EXIGÊNCIA CONTRATUAL	ATENDIMENTO	OBSERVAÇÃO
1	<exigência contratual estabelecida no TR >	...	.....
...	...	...	.....
...	...	...	.....
...	...	...	.....

4 – DESCONTOS EFETUADOS E VALOR A LIQUIDAR

De acordo com os critérios de aceitação e demais termos contratuais, <não> há incidência de descontos por desatendimento dos indicadores de níveis de serviços definidos.

<Não foram / Foram> identificadas inconformidades técnicas ou de negócio que ensejam indicação de glosas e sanções, <cuja instrução corre em processo administrativo próprio (nº do processo)>.

Por conseguinte, o valor a liquidar correspondente à <OS/OFB> acima identificada monta em R$ <valor> (<valor por extenso>).

Referência: <Relatório de Fiscalização nº xxxx ou Nota Técnica nº yyyy>.

5 – ASSINATURA

GESTOR DO CONTRATO

_____
<Nome do Gestor do Contrato>
Matrícula: xxxxxxxx

<Local>, <dia> de <mês> de <ano>.

6 – AUTORIZAÇÃO PARA FATURAMENTO

GESTOR DO CONTRATO

AUTORIZA-SE a **CONTRATADA** a <faturar os serviços executados / apresentar as notas fiscais dos bens entregues> relativos à supracitada <OS/OFB>, no valor discriminado no item 4, acima.

_____
<Nome do Gestor do Contrato>
Matrícula: xxxxxxxx

<Local>, <dia> de <mês> de <ano>

7 – CIÊNCIA

PREPOSTO

_____
<Nome do Preposto do Contrato>
Matrícula: xxxxxxx

<Local>, <dia> de <mês> de <ano>

ANEXO IV – PLANO DE EXECUÇÃO

O Plano de Execução deverá observar integralmente as etapas a seguir:

ENTREGA DA SOLUÇÃO		
MARCO	**AÇÃO PREVISTA**	**RESPONSÁVEL**
AC	Assinatura do Contrato - AC	Contratada e Contratante
AC+2 dias úteis	Reunião Inicial (kickoff) - RI	Contratada e Contratante
RI + 2 dias úteis	Entrega e Aprovação do Plano de Execução	Contratada e Contratante

INSTALAÇÃO E CONFIGURAÇÃO DA SOLUÇÃO		
MARCO	**AÇÃO PREVISTA**	**RESPONSÁVEL**
AC+60 dias	Entrega da Solução - ES	Contratada
ES+TRP	Emissão do Termo de Recebimento Provisório	Contratante
IC (10 dias)	Instalação e Configuração da Solução - IC	Contratada
	Instalação Física da Solução	Contratada
	Configuração da Solução	Contratada
	Migração das Máquinas Virtuais	Contratada
	Repasse de Conhecimento	Contratada e Contratante
TRD	Emissão do Termo de Recebimento Definitivo	Contratante

PAGAMENTO		
MARCO	**AÇÃO PREVISTA**	**RESPONSÁVEL**
TRD+15 dias	Emissão e Envio da Nota Fiscal - NF	Contratada
NF+15 dias	Pagamento Efetivado	Contratante

IMPLANTAÇÃO:

A solução deverá observar integralmente os requisitos de implantação, instalação e fornecimento descritos a seguir:

O processo de entrega da solução deverá ser realizado pela CONTRATADA sob a supervisão do preposto, que dará conhecimento do andamento do fornecimento a CONTRATANTE.

A CONTRATADA deverá apresentar as declarações/certificados do FABRICANTE, comprovando que o produto possui a garantia solicitada neste TR.

As atividades necessárias à implantação e configuração da solução deverão ser obrigatoriamente de responsabilidade da CONTRATADA;

A CONTRATADA deverá instalar a solução ofertada nas instalações da CONTRATANTE.

Os serviços que eventualmente acarretem risco para os sistemas em produção ou requeiram parada de servidores, equipamentos e rede elétrica, somente poderão ser executados fora do horário de expediente, previamente acordados com a área de TI da CONTRATANTE;

A CONTRATADA deverá fazer o repasse de conhecimento à equipe indicada pela CONTRATANTE (“hands-on”), de modo que ela possa ser capaz de operar, configurar, otimizar e/ou aplicar novas configurações ao equipamento fornecido sem auxílio da CONTRATADA, com carga horária de 08 (oito) horas;

ANEXO I - TERMO DE REFERÊNCIA - SP15-2025 - REPAC (1).pdf

Documento número #0ef68b03-6499-4442-95a8-3855cf09fc30

Hash do documento original (SHA256): fb92bcd506be36d90e8e40bcb08dc5b07afa65b11d7f731aec059f8ccd97d69d

Assinaturas

Marco Américo Lucchesi
CPF: 805.145.707-25
Assinou como parte em 12 ago 2025 às 15:46:14

Flávio Barbosa Toledo
CPF: 350.604.504-06
Assinou como parte em 11 ago 2025 às 11:22:37

Maria José da Silva Fernandes
CPF: 637.863.387-87
Assinou como parte em 11 ago 2025 às 11:50:15

Francisco Roberto Leonardo
CPF: 386.665.457-04
Assinou como parte em 11 ago 2025 às 10:48:14

Log

11 ago 2025, 10:35:31	Operador com email crislayne.santos@facc10.org.br na Conta 0d2fec55-6c6d-46ac-93e0-3e2ba7b6a490 criou este documento número 0ef68b03-6499-4442-95a8-3855cf09fc30. Data limite para assinatura do documento: 10 de setembro de 2025 (10:35). Finalização automática após a última assinatura: habilitada. Idioma: Português brasileiro.
11 ago 2025, 10:37:50	Operador com email crislayne.santos@facc10.org.br na Conta 0d2fec55-6c6d-46ac-93e0-3e2ba7b6a490 alterou o processo de assinatura. Data limite para assinatura do documento: 10 de setembro de 2025 (08:51).
11 ago 2025, 10:37:50	Operador com email crislayne.santos@facc10.org.br na Conta 0d2fec55-6c6d-46ac-93e0-3e2ba7b6a490 alterou o processo de assinatura. Finalização automática após a última assinatura: não habilitada.

11 ago 2025, 10:37:50	Operador com email crislayne.santos@facc10.org.br na Conta 0d2fec55-6c6d-46ac-93e0-3e2ba7b6a490 adicionou à Lista de Assinatura: maria.fernandes@bn.gov.br para assinar como parte, via E-mail. Pontos de autenticação: Token via E-mail; Nome Completo; CPF; endereço de IP. Dados informados pelo Operador para validação do signatário: nome completo Maria José da Silva Fernandes.
11 ago 2025, 10:37:50	Operador com email crislayne.santos@facc10.org.br na Conta 0d2fec55-6c6d-46ac-93e0-3e2ba7b6a490 adicionou à Lista de Assinatura: dirgeral@facc10.org.br para assinar como parte, via E-mail. Pontos de autenticação: Token via E-mail; Nome Completo; CPF; endereço de IP. Dados informados pelo Operador para validação do signatário: nome completo Francisco Roberto Leonardo e CPF 386.665.457-04.
11 ago 2025, 10:37:50	Operador com email crislayne.santos@facc10.org.br na Conta 0d2fec55-6c6d-46ac-93e0-3e2ba7b6a490 adicionou à Lista de Assinatura: flavio@facc10.org.br para assinar como parte, via E-mail. Pontos de autenticação: Token via E-mail; Nome Completo; CPF; endereço de IP. Dados informados pelo Operador para validação do signatário: nome completo Flávio Barbosa Toledo e CPF 350.604.504-06.
11 ago 2025, 10:37:50	Operador com email crislayne.santos@facc10.org.br na Conta 0d2fec55-6c6d-46ac-93e0-3e2ba7b6a490 adicionou à Lista de Assinatura: presidencia@bn.gov.br para assinar como parte, via E-mail. Pontos de autenticação: Token via E-mail; Nome Completo; CPF; endereço de IP. Dados informados pelo Operador para validação do signatário: nome completo Marco Américo Lucchesi.
11 ago 2025, 10:48:14	Francisco Roberto Leonardo assinou como parte. Pontos de autenticação: Token via E-mail dirgeral@facc10.org.br. CPF informado: 386.665.457-04. IP: 189.105.181.86. Localização compartilhada pelo dispositivo eletrônico: latitude -22.8830174 e longitude -43.4200683. URL para abrir a localização no mapa: https://app.clicksign.com/location. Componente de assinatura versão 1.1277.2 disponibilizado em https://app.clicksign.com.
11 ago 2025, 11:22:37	Flávio Barbosa Toledo assinou como parte. Pontos de autenticação: Token via E-mail flavio@facc10.org.br. CPF informado: 350.604.504-06. IP: 200.20.100.53. Localização compartilhada pelo dispositivo eletrônico: latitude -22.9539113 e longitude -43.174275. URL para abrir a localização no mapa: https://app.clicksign.com/location. Componente de assinatura versão 1.1277.2 disponibilizado em https://app.clicksign.com.
11 ago 2025, 11:50:15	Maria José da Silva Fernandes assinou como parte. Pontos de autenticação: Token via E-mail maria.fernandes@bn.gov.br. CPF informado: 637.863.387-87. IP: 177.223.196.212. Componente de assinatura versão 1.1277.2 disponibilizado em https://app.clicksign.com.
12 ago 2025, 15:46:14	Marco Américo Lucchesi assinou como parte. Pontos de autenticação: Token via E-mail presidencia@bn.gov.br. CPF informado: 805.145.707-25. IP: 187.102.153.3. Componente de assinatura versão 1.1279.0 disponibilizado em https://app.clicksign.com.
13 ago 2025, 10:19:13	Operador com email crislayne.santos@facc10.org.br na Conta 0d2fec55-6c6d-46ac-93e0-3e2ba7b6a490 finalizou o processo de assinatura. Processo de assinatura concluído para o documento número 0ef68b03-6499-4442-95a8-3855cf09fc30.

Documento assinado com validade jurídica.
Para conferir a validade, acesse https://www.clicksign.com/validador e utilize a senha gerada pelos signatários ou envie este arquivo em PDF.
As assinaturas digitais e eletrônicas têm validade jurídica prevista na Medida Provisória nº. 2200-2 / 2001

Este Log é exclusivo e deve ser considerado parte do documento nº 0ef68b03-6499-4442-95a8-3855cf09fc30, com os efeitos prescritos nos Termos de Uso da Clicksign, disponível em www.clicksign.com.