GOVERNO DO ESTADO DE MINAS GERAIS

POLÍCIA MILITAR DE MINAS GERAIS

Centro de Tecnologia em Sistemas / Seção de Infraestrutura

Especificação de Material/Serviço PMMG/DTS/CTS-S INFRAESTRUTURA nº. 7/2025

Belo Horizonte, 07 de agosto de 2025.

ESPECIFICAÇÃO TÉCNICA

1. **OBJETO**

Aquisição de solução de Infraestrutura de Tecnologia da Informação (TI), com fornecimento de suporte técnico conforme demanda da CONTRATANTE, abrangendo os seguintes itens:

Item	Código SIAD	Quantidade	Unidade de medida	Descrição
1	1884093	2	Unidade	Appliance Hiperconvergente com licenciamento
2	201462	1		Appliance Hiperconvergente com GPU e licenciamento
3	1884069	2		Switch Topo de Rack (ToR)
4	107492	2		Solução de Segurança Virtualizada - Web Application Firewall (WAF)

2. **ESPECIFICAÇÕES TÉCNICAS MÍNIMAS**

As especificações abaixo tomaram por base diagnóstico do ambiente de produção e homologação da CONTRATANTE, no qual vige a arquitetura SAN. O estudo foi feito na fase preparatória do Estudo Técnico Preliminar e não reflete com precisão a condição atual do ambiente, devendo servir apenas como referência.

PHYSICAL OVERVIEW:

VIRTUAL OVERVIEW:

VM Profiling

Powered On VMs	249	OS Versions	26 derived OS types
Powered Off VMs	73	VM HW Versions	1
Guest iSCSI Present	19		

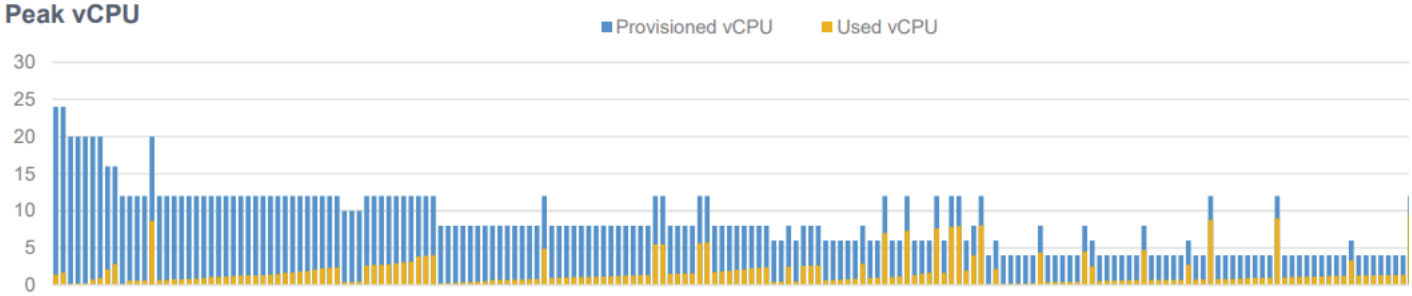
T-Shirt Sizes	52 different vCPU/vRAM VMs combinations
Unique VMs	19 unique vCPU/vRAM VMs

WINDOWS		LINUX		OTHER	
Windows Server 2008	10	Debian	210	FreeBSD	2
Windows Server 2022	8	Ubuntu	28	Oracle Solaris	1
Windows Server 2019	1	Generic Linux	19	Other	11
Windows Server 2003	1	SUSE	13		
		CentOS	11		
		Oracle 7	4		
		RHEL 7	1		
		VMware Photon	1		
		Other...	1		

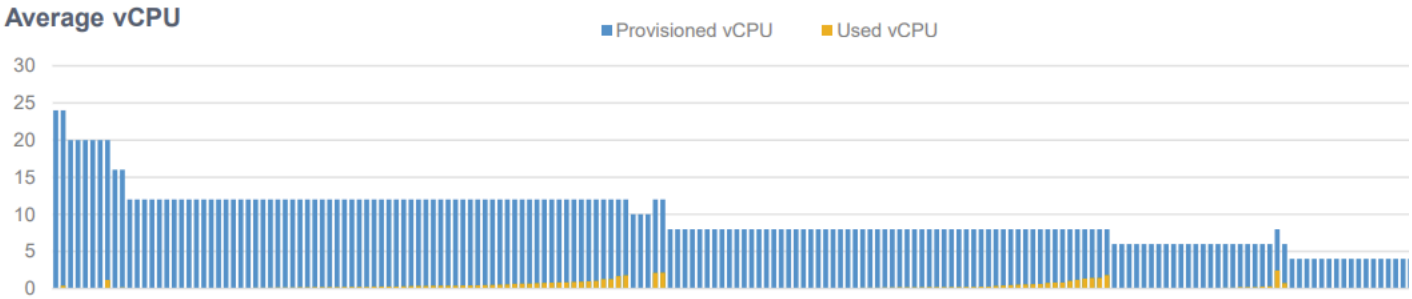
VM Overprovisioning – vCPU

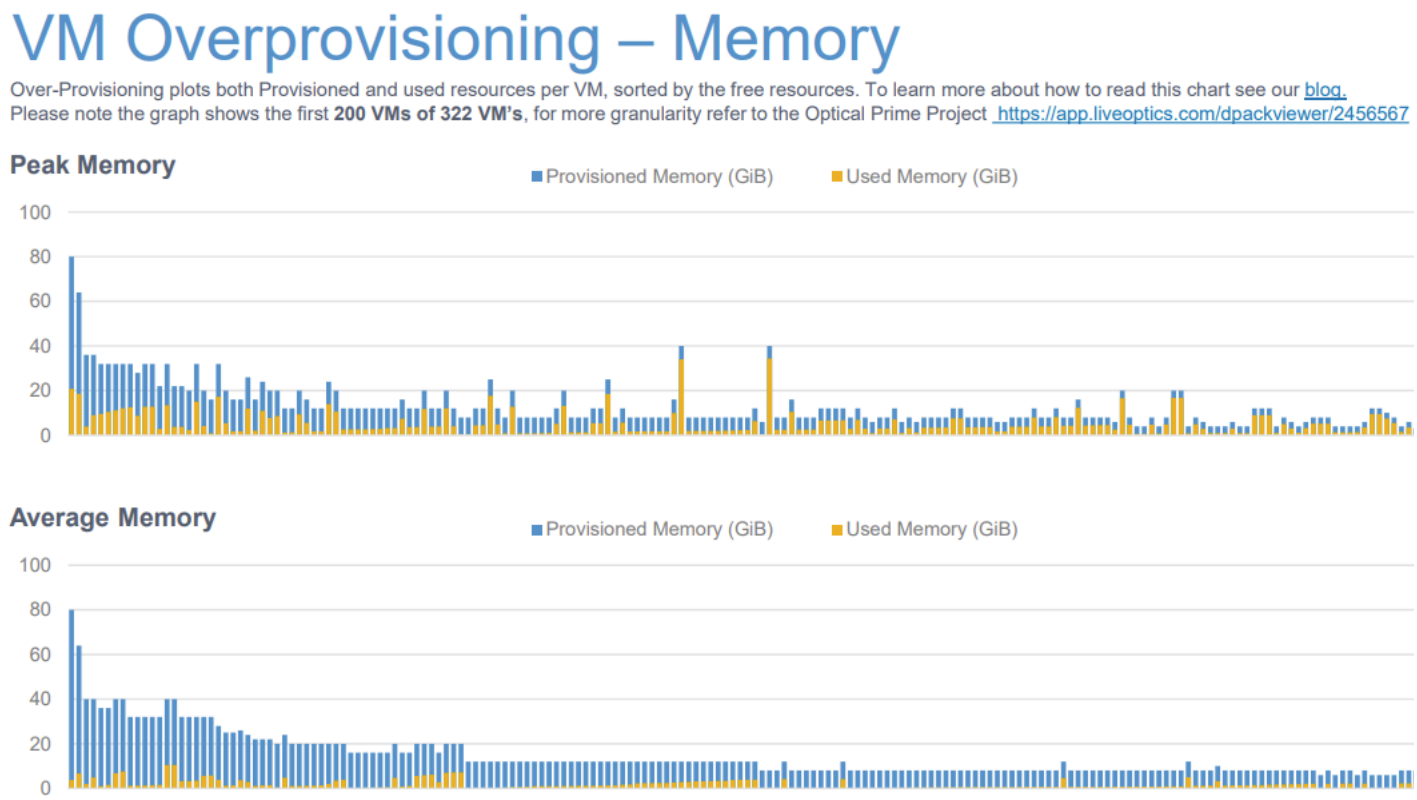
Over-Provisioning plots both Provisioned and used resources per VM, sorted by the free resources. To learn more about how to read this chart see our blog.
Please note the graph shows the first **200 VMs of 322 VM's**, for more granularity refer to the Optical Prime Project https://app.liveoptics.com/dpackviewer/2456567

Peak vCPU



Average vCPU





2.1. **Appliance Hiperconvergente com licenciamento - Item 1**

2.1.1. *Appliance Hiperconvergente:*

2.1.1.1. 2 Fontes Redundantes e Hot Plug de 1100W ou superior (N + 1);

2.1.1.2. *Processamento:*

2.1.1.2.1. Deve possuir uma das seguintes configurações de processadores:

1. 2 (dois) processadores simétricos (dois soquetes), cada um com, no mínimo, 14 (quatorze) núcleos, totalizando 28 (vinte e oito) núcleos. Núcleos com tecnologia SMT (núcleos lógicos) são considerados como 1 (um) núcleo físico apenas;
2. 1 (um) processador com, no mínimo, 28 (vinte e oito) núcleos;

2.1.1.2.2. Cada processador deverá ter velocidade base de clock mínima de 2,4 GHz;

2.1.1.2.3. Cada processador deve possuir memória cache L3 com uma das seguintes configurações:

1. no mínimo 16 MB caso use a configuração 2.1.1.2.1 (1);
2. no mínimo 32 MB caso use a configuração 2.1.1.2.1 (2);

2.1.1.2.4. Deve possuir tecnologia de suporte e otimização para virtualização;

2.1.1.2.5. Os processadores deverão ser compatíveis com as tecnologias especificadas nos requisitos de Memória RAM;

2.1.1.2.6. Para fins de referência, considerar-se-á superior ao processador especificado o processador que contenha, pelo menos, o número especificado de núcleos e "Multithread Rating" superior a 45000 no site www.cpubenchmark.net;

2.1.1.3. *Memória:*

2.1.1.3.1. 1TB de Memória RAM DDR5 de frequência mínima de 4400 MHz;

2.1.1.3.2. Possibilitar expansão de, pelo menos, mais 2TB de Memória RAM considerando cluster de 8 (oito) nós.

2.1.1.4. *Armazenamento interno:*

2.1.1.4.1. A solução ofertada contemplando os 3 (três) appliances (já contabilizando o appliance com GPU - item 2.2) deverá possuir pelo menos 210TB (duzentos e dez terabytes) líquidos em discos no cluster, sem considerar perdas com arranjos (RAID e/ou discos de spare) e sem considerar ganhos de área com a desduplicação e/ou compressão dos dados, totalmente disponíveis para armazenamento e para provisionamento das máquinas virtuais, considerando o fator de redundância com tolerância de perda de, no mínimo, 1 (um) appliance (nó);

2.1.1.4.1.1. Caso não seja atendida a exigência de volumetria, será admitido o acréscimo de nós na proposta até atingir a volumetria pretendida, respeitado o limite de espaço em rack definido no *item 2.8.5.1*;

2.1.1.4.2. A composição de discos deverá ser all-flash NVMe. Ou seja, deverá utilizar apenas unidades de armazenamento em estado sólido (SSDs) do tipo NVMe, sendo vedado o oferecimento de discos rígidos mecânicos (HDDs) ou SSD SATA;

2.1.1.4.3. Deverão ser desconsideradas as unidades de boot e espaços de armazenamento utilizados para cache. Também deverá ser desconsiderada a utilização de recursos de desduplicação, compressão de dados, Erasure Coding (EC) ou qualquer outra tecnologia de otimização de espaço. Deverão ainda ser usadas, para o cálculo, ferramentas oficiais do fabricante da solução;

2.1.1.4.4. Suporte a hot-swap (em caso de troca de unidades de armazenamento, as operações I/O das aplicações de em execução não deverão ser interrompidas ou prejudicadas durante a troca. A troca dos equipamentos com essas características não deverá interromper o funcionamento dos equipamentos redundantes);

2.1.1.5. No mínimo 2 (duas) placas com 2 (duas) interfaces Ethernet 10/25GbE SFP28 cada;

2.1.1.6. Incluir todos os transceivers 25G SFP28 e cordões de fibra óptica com conectores LC/LC de pelo menos 5 (cinco) metros para conexão da solução deste edital, podendo ser entregues cabos DAC passivos com pontas SFP28 com pelo menos 5 (cinco) metros de comprimento, no lugar dos transceivers e cordões ópticos, que atendam às especificações;

2.1.1.7. 1 Porta Gigabit Ethernet para gerenciamento;

2.1.1.8. Deverá ser permitida a troca de discos avariados, sem interrupção das operações de I/O das aplicações que estão acessando os dados;

2.1.1.9. Permitir o upgrade de nós de forma transparente e não disruptiva, ou seja, ao se inserir um nó no cluster, o Software Defined Storage deverá integrar o appliance ao cluster, aumentando imediatamente os recursos de processamento, memória e armazenamento;

2.1.1.10. A falha isolada de um componente do Sistema de Armazenamento definido por Software da solução não pode impactar a disponibilidade da infraestrutura de armazenamento para as máquinas virtuais;

2.1.1.11. Deverá vir acompanhado de kit trilhos para instalação no rack, braço gerenciador de cabos e bezel;

2.1.1.12. Serão aceitos apenas hardwares homologados pelos fabricantes, sendo necessária a comprovação documental na matriz de compatibilidade de hardwares.

2.1.2. *Software de gestão avançada de ambiente de virtualização e solução de virtualização:*

2.1.2.1. O appliance hiperconvergente deve vir acompanhado da licença de software de gestão avançada de ambiente virtualizado em sua última versão, em relação à data de publicação do edital;

2.1.2.1.1. A licença deverá vigorar com todas as funcionalidades descritas neste instrumento por, pelo menos, o período de garantia da solução (60 meses), incluindo o suporte na modalidade 24/7/365;

2.1.2.1.2. O licenciamento do(s) software(s) mencionado(s) no item 2.1.2 e seguintes deverá ser fornecido de forma a licenciar todo o ambiente, independente da métrica usada por cada fabricante;

2.1.2.1.3. Após o período descrito no item 2.1.2.1.1, a licença deverá permanecer em funcionamento, admitindo-se que apenas as funcionalidades indispensáveis ao regular funcionamento da solução permaneçam ativas;

2.1.2.2. A licença deverá ter, no mínimo, as seguintes funcionalidades:

2.1.2.3. Deve suportar e ser ofertada com pelo menos um hypervisor proprietário instalado, como por exemplo Acropolis Hypervisor (AHV) ou VMWare, em suas versões mais recentes. Os softwares que acompanham o hypervisor, tais como o Sistema de Armazenamento Definido por Software e o sistema de gerenciamento, também devem estar em suas versões mais recentes, devendo ainda atender aos requisitos de configurações e gerenciamento deste documento;

2.1.2.4. Deverá suportar, para máquinas virtuais Windows e Linux, a criação de snapshots com consistência (“application consistent” e “crash consistent”). Ou seja, os snapshots poderão ser feitos no ambiente em produção e execução, com garantia da proteção dos dados gravados nas unidades de armazenamento do próprio cluster;

2.1.2.5. Ser compatível com as principais cloud públicas do mercado (exemplo: Azure, AWS), permitindo o gerenciamento dos recursos locais e em nuvem no mesmo ambiente;

2.1.2.5.1. Suportar atualizações com poucos cliques, possibilitando a atualização de todos os nós do cluster de forma simples e automatizada, eliminando a intervenção manual do administrador e necessidade de parada do ambiente;

2.1.2.5.2. Deverá permitir o download ou atualização de drivers/firmwares dos equipamentos pela Internet;

2.1.2.5.3. Ter ferramenta unificada de monitoração e atualização de todo o hardware e software (armazenamento, máquinas virtuais, etc) da solução;

2.1.2.5.4. A solução de Sistema de Armazenamento definido por Software (SDS) deverá consolidar todo o armazenamento do cluster apresentando como uma única área ao hipervisor;

2.1.2.5.5. Toda operação de gravação de uma determinada máquina virtual deverá acontecer primariamente nos discos daquele nó que está hospedando a máquina virtual. Caso o disco local esteja com alta taxa de ocupação, a operação de gravação deverá ser redirecionada para um disco pertencente a outro nó do cluster;

2.1.2.5.6. Permitir escalabilidade horizontal (scale-out), isso é, a adição de novos nós ao cluster através de uma console gráfica, sem a parada do ambiente de produção, aumentando como um todo a capacidade de armazenamento, processamento e memória disponibilizados ao hipervisor, além de crescer de forma linear o desempenho do cluster;

2.1.2.5.7. Prover uma infraestrutura hiperconvergente de alta disponibilidade em configuração de cluster para ambientes virtualizados, composta por no mínimo 3 (três) appliances físicos e podendo chegar a, pelo menos, 16 (dezesseis) appliances físicos no mesmo cluster. 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;

2.1.2.5.8. Agregar todos os discos físicos dos appliances contidos no cluster, apresentando um único sistema de arquivos ao hypervisor;

2.1.2.5.9. Permitir remover nós do cluster sem parada do ambiente;

2.1.2.5.10. Garantir replicação de todos os dados gravados localmente para outros appliances que compõem o cluster, de modo que, se ocorrer a falha de um dos appliances, não ocorra a indisponibilidade do ambiente;

2.1.2.5.11. Manter os dados das máquinas virtuais no armazenamento local do próprio nó e, caso essa máquina virtual se movimente de um appliance a outro, os dados devem ser movidos, caso necessário, em segundo plano, para esse novo appliance, buscando o melhor desempenho possível;

2.1.2.5.12. Suportar, via software, compressão e desduplicação durante o processo de gravação. A funcionalidade deverá atuar na camada de performance presente em cada um dos nós;

2.1.2.5.13. Implementar compressão inline ou pós-processada;

2.1.2.5.14. Implementar desduplicação pós-processada, devendo atuar nos dados frios;

2.1.2.5.15. Implementar tecnologia de desduplicação como solução de otimização do armazenamento do cluster;

2.1.2.5.16. Suportar snapshots por máquinas virtuais nativamente, armazenando esses snapshots no cluster para proteção local. O snapshot poderá ser feito com o ambiente em produção e irá garantir a proteção dos dados que estão gravados em disco;

2.1.2.5.17. A funcionalidade de replicação nativa da solução deverá trabalhar com snapshots das máquinas virtuais e suportar topologia de replicação "um para um" entre clusters localizados em diferentes locais;

2.1.2.5.18. Limitar a quantidade de banda utilizada para a funcionalidade de replicação assíncrona;

2.1.2.5.19. Possuir console de administração via navegador, sem necessidade de instalação de qualquer componente adicional para essa finalidade;

2.1.2.5.19.1. A interface de administração via navegador deve permitir acesso a todos os nós configurados no cluster. A funcionalidade de alta disponibilidade também deve estar disponível para a interface de administração, garantindo que mesmo em caso de falhas, a interface de administração continue disponível;

2.1.2.5.19.2. A console de administração deverá ser web, sem necessidade de instalação de qualquer software adicional para essa finalidade, compatível com browsers que suportam a tecnologia HTML5. Deverá ainda suportar protocolo HTTPS utilizando certificados;

2.1.2.5.19.3. Deverá ser possível o acesso ao software de hiperconvergência e ao hypervisor através do protocolo SSH (Secure Shell), com autenticação por senha;

2.1.2.5.19.4. As interfaces de administração Web e SSH devem ser acessíveis a partir de qualquer um dos endereços IPs configurados para os nós e respectivos softwares de controle;

2.1.2.5.19.5. 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;

2.1.2.5.19.6. A console deve permitir integração com o Active Directory para autenticação, ou utilizar autenticação local;

2.1.2.5.19.7. Oferecer acesso a, pelo menos:

- Dashboard principal;
- Dashboard da saúde do cluster;
- Dashboard das máquinas virtuais;
- Dashboard do Storage;
- Dashboard do Hardware;
- Dashboard de Análise de Performance;
- Dashboard de Alertas e Eventos.

2.1.2.5.20. Os alertas e eventos deverão ser relacionados a, no mínimo, unidades de armazenamento, memória, processamento, fontes de alimentação, sistema de ventilação, e operação anormal de máquinas virtuais;

2.1.2.5.21. Deverá possuir dashboards integrados e customizáveis, para, pelo menos, monitoramento e análise de desempenho, capacidade e uso de recursos pela solução e máquinas virtuais instaladas, capacidade de armazenamento, uso de memória, de processamento, operações de I/O e de rede;

2.1.2.5.22. Deverá permitir a verificação de estado atual da solução, apresentando os erros e alertas dos elementos que a compõem;

2.1.2.5.23. Oferecer gerenciamento por APIs REST;

2.1.2.5.24. Implementar interface de linha de comando completa para administração e monitoramento dos componentes do cluster;

2.1.2.5.25. Possibilidade de impedir o acesso ao terminal de linha de comando;

2.1.2.5.26. Suportar envio de alertas e eventos via SNMP e mensagem de e-mail;

2.1.2.5.27. Suportar diferentes perfis de usuários, de acordo com suas funções:

- Visualização - Não permite nenhuma alteração na configuração;
- Administrador do ambiente - Pode realizar todas as operações disponíveis, exceto criar ou modificar os usuários;
- Administrador - Pode realizar todas as operações disponíveis.

2.1.2.5.28. Enviar automática e periodicamente informações e estatísticas para o suporte do fabricante (call-home), de forma a 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;

2.1.2.5.29. Oferecer portal de acesso do próprio fabricante para download de atualizações e de softwares agregados à solução;

2.1.2.5.30. A solução deverá possuir ferramenta de checagem interna integrada a console de gerenciamento, buscando por problemas de saúde no cluster proativamente;

2.1.2.5.31. Todos os manuais técnicos referentes aos componentes da solução devem ser fornecidos ou disponibilizados eletronicamente;

2.1.2.5.32. Apresentar, pelo menos, as seguintes informações consolidadas de todos os clusters registrados:

- Saúde dos clusters;
- Máquinas virtuais;
- Armazenamento;
- Processamento;
- Memória;
- Situação do Hardware;
- Dashboard de Análise de Performance;
- Dashboard de Alertas e Eventos.

2.1.2.5.33. Poder ser implementada em máquina virtual adicional, integrada a console de administração local da solução de hiperconvergência;

2.1.2.5.34. Gerenciar múltiplos clusters e as máquinas virtuais;

2.1.2.5.35. Fornecer sugestões de ajuste de configuração (CPU, memória e armazenamento) das máquinas virtuais baseada na utilização histórica dos recursos computacionais atribuídos a elas;

2.1.2.5.36. Possuir funcionalidade de busca que suporte busca contextualizada;

2.1.2.5.37. Possuir funcionalidade de atualização automatizada de múltiplos clusters de forma centralizada;

2.1.2.5.38. Prover monitoramento preditivo baseado em análises comportamentais em vez de métricas estáticas ou manuais a fim de detectar problemas de desempenho antes de impactar as cargas de trabalho;

2.1.2.5.39. Detectar possíveis gargalos no ambiente devido ao consumo de recursos não otimizados;

2.1.2.5.40. Possuir ferramenta de planejamento que permita a análise e predição de consumo de recursos de armazenamento, CPU e memória;

2.1.2.5.41. Oferecer funcionalidade de planejamento de capacidade para crescimento baseado na carga de trabalho empregada atualmente e mostrar previsão futura;

2.1.2.5.42. Oferecer funcionalidade de planejamento de capacidade para crescimento baseado na carga de trabalho planejada;

2.1.2.5.43. Deverá permitir o inventário dos equipamentos, apresentando marca, modelo e número de série desses equipamentos, de forma a ser possível identificá-los;

2.1.2.5.44. Emitir relatórios gerenciais e operacionais das funcionalidades acima descritas;

2.1.2.5.45. Oferecer possibilidade de agendamento de relatórios gerenciais e operacionais;

2.1.2.5.46. Oferecer funcionalidade de central de custos que permita precificar proporcionalmente os recursos alocados para determinada área de negócio no ambiente;

2.1.2.5.47. Ser otimizado para operar com nuvem híbrida e hiperconvergência;

2.1.2.6. Sobre a função de hypervisor que acompanha o licenciamento, deverá ter, no mínimo, as seguintes funcionalidades:

2.1.2.6.1. Possuir interface de usuário que facilite a operação pela camada de gestão da instituição;

2.1.2.6.2. Possuir recurso de migração dinâmica de máquina virtual em sua totalidade, bem como das cargas de trabalho em execução, de um nó (host) para outro;

2.1.2.6.3. Permitir operações de movimentação de máquinas virtuais de um nó físico para outro, com a máquina virtual em operação;

2.1.2.6.4. Possibilitar migração de máquina virtual de arquitetura SAN, do ambiente VMWare VSphere 7 da CONTRATANTE para a nova solução de HCI;

2.1.2.6.5. Possibilitar a extensão de clusters entre datacenters.

2.1.3. *Software para microssegmentação lógica de redes baseado em "Zero Trust"*

2.1.3.1. Segurança de ambiente Leste-Oeste;

2.1.3.2. Possibilitar a limitação de acesso implícito a apps e dados, por meio de microssegmentação;

2.1.3.3. Permitir o controle de comunicação entre aplicações e/ou máquinas virtuais;

2.1.3.4. Permitir a definição de políticas de segurança;

2.1.3.5. Emitir relatórios gerenciais e operacionais automatizados e agendáveis;

2.1.3.6. possibilitar a categorização de aplicações a nível de camada 4 do Modelo OSI, a fim de customizar o nível de inspeção da camada 7;

2.1.3.7. Permitir a encriptação de comunicações em trânsito;

2.1.3.8. Emitir alarmes que indicam quando as portas estão abertas.

2.1.4. O appliance deve ser entregue com infraestrutura pronta de componentes internos já preparados para a instalação eventual e futura de placa GPU compatível, nos mesmos moldes da placa GPU especificada no item 2.2 deste documento.

2.2. **Appliance Hiperconvergente com GPU e licenciamento - Item 2**

2.2.1. O appliance terá as mesmas especificações mínimas e licenciamentos do appliance descrito no item 2.1. Com relação à GPU, a referência será a NVIDIA H100 NVL Tensor Core GPU ou superior. Para fins de referência, considerar-se-á superiora a GPU que tenha mais de 94GB de memória de vídeo (VRAM) e largura de banda de memória de GPU de mais de 3.9TB/s;

2.2.2. A solução deverá ser oferecida com todo o licenciamento necessário para virtualização de GPU e distribuição para máquinas virtuais, bem como suporte a aplicações de Inteligência Artificial (IA). Para referência, considerar a licença NVIDIA AI Enterprise;

2.2.2.1. O período de todo o licenciamento será de, no mínimo, 5 (cinco) anos;

2.3. **Switch Topo de Rack (ToR) - Item 3**

2.3.1. Cada switch deverá vir acompanhado de 1 (um) cabo do tipo DAC 100G para empilhamento com pelo menos 50cm, 1 (um) transceiver 10GBASE-SR e 2 (dois) transceivers 1000BASE-T. Os cabos e transceivers devem ser compatíveis e ter pleno funcionamento com o switch;

2.3.2. 48 portas 25Gigabit Ethernet SFP28 SR;

2.3.2.1. As referidas portas deverão ser retrocompatíveis com o padrão SFP (1Gbps);

2.3.3. 4 portas 100Gigabit Ethernet QSFP28;

2.3.4. Banda agregada de empilhamento mínima de 200 (duzentos) Gbps;

2.3.5. Deve possuir capacidade de comutação de no mínimo 800 Gbps;

2.3.6. Deve possuir capacidade de encaminhamento de no mínimo 600 Mbps;

2.3.7. Deve possuir fonte de alimentação interna redundante 110/220VAC;

2.3.8. As fontes de alimentação devem suportar hot-swap;

2.3.9. Suportar Equal-Cost Multipath (ECMP);

2.3.10. Deve permitir empilhamento de até 6 (seis) unidades outros equipamentos em topologia linear e em anel, e permitir gerenciar a pilha com um único endereço IP;

2.3.11. Deve possuir pelo menos 8MB de buffer de pacotes;

2.3.12. O empilhamento deverá ser realizado através das portas 100 GbE ou através de módulo dedicado;

2.3.13. Deve possuir capacidade de no mínimo 110.000 (cento e dez mil) endereços MAC;

2.3.14. Deve suportar pelo menos 4094 VLANs;

2.3.15. Deve implementar Jumbo frames com tamanho de até 10000 bytes;

2.3.16. Deve implementar MSTP;

2.3.17. Deve implementar IEEE 802.3ad Link Aggregation Control Protocol (LACP);

2.3.18. Deve implementar IEEE 802.1w Rapid Reconfiguration of Spanning Tree;

2.3.19. Deve implementar IEEE 802.3x Flow Control;

2.3.20. Deve suportar dual stack IPv4/IPv6;

2.3.21. Deve implementar IGMP v2 e v3;

2.3.22. Deve implementar IGMP snooping;

2.3.23. Deve implementar MLD snooping;

2.3.24. Deve implementar Listas de Controle de Acesso (ACL);

2.3.25. Deve implementar SNMPv3 e SSHv2;

2.3.26. Deve implementar DHCP Snooping, DHCP Server e DHCP Relay;

2.3.27. Deve implementar espelhamento de porta;

2.3.28. Deve permitir a seleção por ACL do tráfego a ser espelhado;

2.3.29. Deve permitir múltiplos arquivos de configuração;

2.3.30. Deve implementar LLDP e LLDP-MED;

2.3.31. Deve implementar SFlow;

2.3.32. Deve implementar NTP ou SNTP para sincronização de horário;

2.3.33. Deve permitir roteamento local entre VLANs utilizando interfaces virtuais ou SVIs;

2.3.34. Deve permitir a configuração de rotas estáticas usando endereços IPv4 e IPv6;

2.3.35. Deve possuir DHCP Server para IPv4 e IPv6;

2.3.36. Deve permitir a configuração de DHCP Relay;

2.3.37. Deve implementar PBR (Policy-Based Routing) para IPv4 e IPv6;

2.3.38. Deve pemitir priorização de tráfego usando 8 (oito) filas de priorização por porta;

2.3.39. Deve permitir priorização de tráfego baseado no padrão IEEE 802.1p e no campo DSCP do protocolo Diffserv;

2.3.40. Deve implementar protocolo de VXLAN;

2.3.41. Deve implementar mecanismo EVPN-VXLAN em L2VPN e L3VPN sobre IP e MPLS;

2.3.42. Deve implementar protocolo de roteamento BGPv4 e Extensões Multiprotocolos MP-BGP;

2.3.43. Deve implementar mecanismo de detecção de falhas bidirecionais na convergência (BFD) em pelo menos nos seguintes protocolos: OSPF, BGP e VRRP em IPv4 e IPv6;

2.3.44. Deve implementar mecanismo de Graceful Restart para pelo menos os protocolos OSPF e BGP;

2.3.45. Deve implementar pelos menos os seguintes métodos para configuração das filas de priorização: ponderada, prioridade estrita e ambas combinadas;

2.3.46. 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;

2.3.47. Deve permitir a configuração de Rate Limiting de entrada;

2.3.48. Deve permitir a configuração de Rate Shaping de saída;

2.3.49. Deve permitir o envio de mensagens de syslog a pelo menos 2 servidores distintos;

2.3.50. Deve ser permitida a utilização de redes IPv4 e IPv6 para a funcionalidade solicitada;

2.3.51. O equipamento deverá ser homologado pela Agência Nacional de Telecomunicações (ANATEL).

2.4. **Solução de Segurança Virtualizada - Web Application Firewall (WAF) - Item 4**

2.4.1. *Requisitos técnicos específicos*

2.4.1.1. Deve ser do tipo *appliance* físico ou *appliance* virtual com software dedicado à função de Firewall de Aplicação (WAF) e Proteção de API não sendo permitido solução *open source* (produto montado);

2.4.1.2. A solução deve ser fornecida em Alta Disponibilidade (HA);

2.4.1.3. Deve oferecer cluster de alta disponibilidade entre dois dispositivos no modo Ativo-Passivo e Ativo-Ativo, para que na possibilidade de o principal falhar o tráfego de rede continue sendo processado;

2.4.1.4. Deve possuir throughput HTTP/HTTPS mínimo de 5 Gbps;

2.4.1.5. Deve suportar, pelo menos 10 (dez) interfaces virtuais 1/10Gbps;

2.4.1.6. Deve possuir suporte, no mínimo, a 8 (oito) VCPUs;

2.4.1.7. Deve suportar alocação de memória RAM ilimitada e disco de 1TB;

2.4.1.8. A máquina virtual deve suportar hipervisores como VMware e AHV (Acropolis Hypervisor);

2.4.1.9. A solução deve possuir softwares específicos, destinados à finalidade de Firewall de Aplicação Web (WAF), bem como todas as licenças necessárias, conforme requisitos e funcionalidades deste termo de referência, para o seu funcionamento e proteção de servidores e aplicações Web;

2.4.1.10. Todas as funcionalidades e requisitos técnicos descritos neste Termo de Referência para o WAF devem estar funcionais e licenciados junto ao fabricante. Em se tratando de licenças à parte/adicionais por parte do fabricante, o ônus da aquisição destas licenças é do fornecedor durante todo o prazo de vigência do contrato e prestação do serviço de suporte da CONTRATADA;

2.4.1.11. Os requisitos técnicos e de performance devem ser comprovados com documentação pública, disponível no site do fabricante.

2.4.2. *Requisitos macros*

2.4.2.1. Balanceamento de carga quando utilizado como Proxy Reverso;

2.4.2.2. Cache quando utilizado como Proxy Reverso;

2.4.2.3. Centralização do certificado Wildcard dos sistemas;

2.4.2.4. WAF e proteção de API.

2.4.3. *Funcionalidades de Rede*

2.4.3.1. A solução deve ser capaz de ser implementada no modo Proxy (Transparente e Reverso);

2.4.3.2. Suportar endereçamento IPv4 nas interfaces;

2.4.3.3. A solução ofertada deve aceitar configuração para seu funcionamento em cluster de alta disponibilidade entre dois dispositivos no modo Ativo-Passivo e Ativo-Ativo, para a ocasião em que o principal falhar, o tráfego continue sendo processado;

2.4.3.4. A solução deve suportar a sincronização de configuração entre dois appliances iguais, com o objetivo de operar no modo ativo-ativo, com a distribuição de tráfego sendo realizada por balanceador de carga da própria solução.

2.4.4. *Gerência*

2.4.4.1. Deve possuir administração baseada em interface web HTTPS;

2.4.4.2. Deve possuir recurso de API para gerência através de ferramentas de automação;

2.4.4.3. A solução deve possuir Interface Gráfica com informações sobre o sistema. Ex: (Informações do cluster, hostname, modo de operação, tempo em serviço, versão do firmware);

2.4.4.4. Deverá ser possível visualizar através da interface gráfica de gerência informações de licenças e assinaturas;

2.4.4.5. Deve prover, na interface de gerência, as seguintes informações do sistema: consumo de CPU e estatísticas das conexões;

2.4.4.6. Deve ser possível visualizar na interface de gerência as informações de consumo de memória, rede e disco;

2.4.4.7. Deverá possuir ferramenta, na interface gráfica de gerência que permita visualizar os últimos logs de ataque detectados/bloqueados;

2.4.4.8. Deve prover as seguintes informações, na interface de gráfica de gerência: estatísticas de throughput HTTP em tempo real, estatísticas dos eventos de ataque detectados/bloqueados, estatísticas de requisições HTTP em tempo real e últimos logs de eventos do sistema;

2.4.4.9. Deve possuir na interface gráfica estatísticas de conexões concorrentes e médias por segundo;

2.4.4.10. Deve possuir um painel de visualização com informações das interfaces de rede do sistema;

2.4.4.11. A configuração de administração da solução deve possibilitar a utilização de perfis de usuário, bem como a autenticação via Active Directory;

2.4.4.12. Deve ser possível executar e restaurar backup da configuração via interface Web (GUI). Ou ter a possibilidade de restaurar o backup por outros meios;

2.4.4.13. Deve ser capaz de realizar notificações de eventos de segurança, pelo menos, através de Slack e SYSLOG;

2.4.4.14. A solução deverá ter a capacidade de armazenar logs localmente em disco e em servidor externo via protocolo SYSLOG;

2.4.4.15. A solução deve ter a capacidade de enviar alertas, pelo menos por Slack ou webhook, de requisições ilegais ou que necessitam de análise;

2.4.4.16. A solução deve possuir dados analíticos, sendo possível visualizar top 10 por violações, por tipos de ataques, por políticas de segurança, por URL, por IP de cliente e por país de origem;

2.4.4.17. Deverá ter a capacidade de gerar relatórios baseados em requisições legais e ilegais.

2.4.5. *Autenticação*

2.4.5.1. Os usuários devem ser capazes de autenticar através login e senha na interface gráfica via WEB;

2.4.5.2. Deve possuir base local para armazenamento e autenticação contas de usuários;

2.4.5.3. A solução deve ter a capacidade de autenticar usuários em bases externas/remotas no Active Directory;

2.4.5.4. A solução deve ser capaz de criar grupos de usuários ou possuir separação de roles para controle de acesso.

2.4.6. *Funcionalidades de firewall de aplicação (WAF)*

2.4.6.1. Deve implementar proteção contra a lista de técnicas/ataques listados no OWASP TOP 10 (*Open Web Application Security Project*);

2.4.6.2. Deverá ser capaz de identificar e bloquear ataques através de um banco de dados de assinaturas de vírus e *IP reputation*, atualizado de forma automática;

2.4.6.3. Deverá implementar recurso positivo de segurança, onde o WAF aprende com tráfego real indicando fontes confiáveis e não confiáveis, de forma automatizada através da análise da utilização da aplicação, fazendo a descoberta da estrutura de parâmetros, urls, métodos de http, headers, buscando separar o comportamento normal do abusivo, detectando tentativas de ataques. Mesmo na forma automatizada, deverá possuir menu para visualização de sugestões de alteração na política de segurança, permitindo o analista aceitar ou rejeitar a sugestão de alteração;

2.4.6.4. Ter a capacidade de criação de assinaturas de ataque customizáveis;

2.4.6.5. Ter a capacidade de proteção para ataques do tipo Botnet;

2.4.6.6. Ter a capacidade de proteção para ataques do tipo *Browser Exploit Against SSL/TLS* (BEAST);

2.4.6.7. A solução deverá possuir funcionalidade de proteção positiva contra ataques como acesso por força bruta;

2.4.6.8. Deve suportar detecção de ataques de *Clickjacking*;

2.4.6.9. Deve suportar detecção e prevenção a ataques de cookie *Hijacking* (roubo de sessão);

2.4.6.10. Identificar e prevenir ataque *Cross Site Request Forgery* (CSRF);

2.4.6.11. A solução deverá possuir funcionalidade de proteção positiva contra ataques como *Cross Site Scripting* (XSS);

2.4.6.12. Deve possuir proteção contra ataques de *Denial of Service* (DoS);

2.4.6.13. Ter a capacidade de proteção para ataques do tipo *HTTP header overflow;*

2.4.6.14. Ter a capacidade de proteção para ataques do tipo *Local File inclusion* (FLI);

2.4.6.15. Ter a capacidade de proteção para ataques do tipo *Man-in-the-middle* (MITM);

2.4.6.16. Ter a capacidade de proteção para ataques do tipo *Remote File Inclusion* (RFI);

2.4.6.17. Ter a capacidade de proteção para ataques do tipo *Server Information Leakage;*

2.4.6.18. Proteção contra envios de comandos SQL escondidos nas requisições enviadas a bases de dados (SQL Injection);

2.4.6.19. Ter a capacidade de proteção para ataques do tipo *Malformed XML;*

2.4.6.20. Prevenção contra *Slow POST attack;*

2.4.6.21. Proteger contra ataques *Slowloris;*

2.4.6.22. Ter a capacidade de proteção para ataques do tipo *SYN flood;*

2.4.6.23. Ter a capacidade de proteção para ataques do tipo *Parameter Tampering;*

2.4.6.24. A solução deverá possuir funcionalidade de proteção positiva contra ataques de manipulação de campos;

2.4.6.25. Ter a capacidade de proteção para ataques do tipo *Directory Traversal;*

2.4.6.26. Ter a capacidade de proteção do tipo *rate limit* por *transação por segundo;*

2.4.6.27. Ter a habilidade de configurar proteção do tipo *TCP SYN flood* para prevenção de DoS para qualquer política ou virtual server, através de *Syn Cookie e Half Open Threshold;*

2.4.6.28. Permitir que sejam configuradas regras de bloqueio de upload por extensão de arquivo;

2.4.6.29. Permitir configurar listas negras de bloqueio e listas brancas de confiança, baseadas em endereço IP de origem;

2.4.6.30. Permitir a liberação temporária ou definitiva (*whitelist)* de endereços IP bloqueados por terem originado ataques detectados pela solução;

2.4.6.31. Deve permitir adicionar, automaticamente ou manualmente, em uma lista de bloqueio, os endereços IP de origem, de acordo com a base de *IP Reputation;*

2.4.6.32. Ter a funcionalidade de proteger o website contra ações de *file include* e *path transversal*;

2.4.6.33. Ter a funcionalidade de antivírus ou possuir integração com servidor antivírus através do protocolo ICAP;

2.4.6.34. Ter a capacidade de investigar e analisar todo o tráfego HTTP para atestar se está em conformidade com a respectiva RFC (*Request for Comments*), bloqueando ataques e tráfego em não-conformidade;

2.4.6.35. Deverá ser capaz de fazer offload SSL, onde os certificados digitais são instalados na solução e as requisições HTTP são enviadas aos servidores sem criptografia, ou em HTTPS utilizando certificado local com criptografia mais simples, que onere menos a infraestrutura;

2.4.6.36. A solução deve ser capaz de funcionar como Terminador de sessões SSL para a aceleração de tráfego;

2.4.6.37. Para SSL/TLS offload suportar no mínimo TLS 1.0, 1.1, 1.2 e 1.3;

2.4.6.38. A solução deve ter a capacidade de armazenar certificados digitais de CA's (*Certification Authority* - Autoridade Certificadora);

2.4.6.39. A solução deve ser capaz de gerar CSR (*Certificate Signing Request*) para ser assinado por uma CA;

2.4.6.40. A solução deve ser capaz de validar os certificados que são válidos e não foram revogados por uma lista de certificados revogados (CRL);

2.4.6.41. A solução deve conter as assinaturas de robôs conhecidos como indexadores de web ou crawlers, search engines ou search bots, network scanners e exploit tools que podem ser colocados nos perfis de controle de acesso ou virtual servers, bem como bloquear tais conexões;

2.4.6.42. A solução deve ter um sistema de reputação de endereços IP públicos conhecidos como fontes de ataques DDoS, botnets, spammers, etc. Tal sistema deve ser atualizado automaticamente;

2.4.6.43. A solução deverá ser capaz de limitar o total de conexões permitidas para cada servidor real de um pool de servidores;

2.4.6.44. A solução deve permitir a customização ou redirecionar solicitações e respostas HTTP no HTTP Host, Request URL HTTP, HTTP Referer, HTTP Body e HTTP Location;

2.4.6.45. A solução deve permitir criar regras definindo a ordem em que as páginas devem ser acessadas para prevenir ataques como *Cross-Site Request Forgery* (CSRF);

2.4.6.46. A solução deve ter a capacidade de definir restrições a métodos HTTP;

2.4.6.47. Permitir que sejam criadas assinaturas customizadas de ataques, através de expressões regulares;

2.4.6.48. Suportar redirecionamento e reescrita de requisições e respostas HTTP;

2.4.6.49. Permitir redirecionar requisições HTTP para HTTPS;

2.4.6.50. Permitir reescrever a linha URL no cabeçalho de uma requisição HTTP;

2.4.6.51. Permitir reescrever o campo "Host:" no cabeçalho de uma requisição HTTP;

2.4.6.52. Permitir reescrever o campo "Referer:" no cabeçalho de uma requisição HTTP;

2.4.6.53. Permitir redirecionar requisições para outro web site;

2.4.6.54. Permitir enviar resposta HTTP 403 Forbidden para requisições HTTP ou apresentar página de bloqueio customizável;

2.4.6.55. Permitir reescrever o parâmetro "Location:" no cabeçalho HTTP de uma resposta de redireção HTTP de um servidor web;

2.4.6.56. Permitir alterar o corpo ("body") de uma resposta HTTP de um servidor web, como por exemplo, alterar resposta contendo HTTP para HTTPS no corpo da mensagem;

2.4.6.57. Permitir adicionar o campo X-Forwarded-For para identificação do endereço real do cliente quando no modo de proxy reverso;

2.4.6.58. Possuir capacidade de *caching* para aceleração web;

2.4.6.59. Deve permitir ao Administrador a criação de novas assinaturas.

2.4.7. *Balanceamento de Carga*

2.4.7.1. A solução deve incluir funcionalidade de balanceamento de carga entre servidores web;

2.4.7.2. Deve ter a habilidade de configurar portas não-padrão para aplicação web HTTP e HTTPS;

2.4.7.3. Ter a capacidade de balancear/distribuir tráfego e rotear o conteúdo através de vários servidores web;

2.4.7.4. A solução deve permitir criar grupos de servidores (*Server Farm / Pool*) para distribuir as conexões dos usuários;

2.4.7.5. Suportar algoritmo *Round Robin* para balanceamento de carga de servidores;

2.4.7.6. Suportar algoritmo *Weighted Round Robin* para balanceamento de carga de servidores;

2.4.7.7. Suportar algoritmo *Least Connections* para balanceamento de carga de servidores;

2.4.7.8. Deve ser possível especificar o número máximo de conexões TCP simultâneas para um determinado servidor membro do *Server Pool*;

2.4.7.9. Permitir teste de disponibilidade de servidor web através do método TCP;

2.4.7.10. Permitir teste de disponibilidade de servidor web através do método *ICMP ECHO_REQUEST* (ping);

2.4.7.11. Permitir teste de disponibilidade de servidor web através do método *TCP Half Open*;

2.4.7.12. Permitir teste de disponibilidade de servidor web através do método *TCP SSL;*

2.4.7.13. Permitir teste de disponibilidade de servidor web através do método HTTP;

2.4.7.14. Permitir teste de disponibilidade de servidor web através do método HTTPS;

2.4.7.15. Nos testes de disponibilidade HTTP e HTTPS, permitir indicar a URL exata a ser testada;

2.4.7.16. Nos testes de disponibilidade HTTP e HTTPS, permitir escolher entre os métodos HEAD, GET e POST;

2.4.7.17. Nos testes de disponibilidade HTTP e HTTPS, permitir indicar o nome do campo HTTP "host" a ser testado;

2.4.7.18. Suportar roteamento das requisições dos clientes web baseado em conteúdo HTTP, através de "Host";

2.4.7.19. Suportar roteamento das requisições dos clientes web baseado em "Cabeçalho";

2.4.7.20. Suportar roteamento das requisições dos clientes web baseado em "Cookie";

2.4.7.21. Implementar Cache de Conteúdo para HTTP, permitindo que objetos sejam armazenados e requisições HTTP sejam respondidas diretamente pela solução;

2.4.7.22. A solução deverá ser capaz de balancear as sessões novas, mas preservar sessões existentes no mesmo servidor, implementando persistência por endereço IP de origem;

2.4.7.23. A solução deverá ser capaz de balancear as sessões novas, mas preservar sessões existentes no mesmo servidor, implementando persistência analisando qualquer parâmetro do header HTTP;

2.4.7.24. A solução deverá ser capaz de balancear as sessões novas, mas preservar sessões existentes no mesmo servidor, implementando persistência baseada em Cookie Persistente;

2.4.7.25. A solução deverá ser capaz de balancear as sessões novas, mas preservar sessões existentes no mesmo servidor, implementando persistência baseada em PHP Session ID;

2.4.7.26. A solução deverá ser capaz de balancear as sessões novas, mas preservar sessões existentes no mesmo servidor, implementando persistência baseada em JSP Session ID;

2.4.7.27. A solução deverá ser capaz de balancear as sessões novas, mas preservar sessões existentes no mesmo servidor, implementando persistência por sessão SSL.

2.4.8. *Proteção de API*

2.4.8.1. Fornecer proteção para a comunicação API, sejam elas implementadas usando XML, JSON API ou RESTful API;

2.4.8.2. Permitir a utilização de arquivos de esquema JSON para verificar o conteúdo JSON em solicitações HTTP, a fim de determinar o conteúdo aceitável e validar se o conteúdo está bem formado;

2.4.8.3. Permitir definir a limitação de parâmetros JSON tais como total de dados, tamanho da chave ou profundidade da estrutura, total de chaves/array/objetos, entre outros;

2.4.8.4. Permitir ações do tipo alertar, bloquear, bloquear temporariamente, redirecionar ou responder com erro 403;

2.4.8.5. Permitir definir o nível de severidade dos alertas ou violações;

2.4.8.6. Permitir a utilização de arquivos de esquema XML para verificar o conteúdo XML em solicitações HTTP, a fim de determinar o conteúdo aceitável e validar se o conteúdo está bem formado;

2.4.8.7. Permitir definir a limitação de parâmetros XML tais como total de atributo por elemento, tamanho do nome do atributo, tamanho de documento, permitir CDATA, entre outros;

2.4.8.8. Permitir definir o seguinte formato do esquema: SOAP ou XML;

2.4.8.9. Permitir ações do tipo alertar, bloquear, bloquear temporariamente, redirecionar ou responder com erro 403;

2.4.8.10. Fornecer suporte a proteção OpenAPI;

2.4.8.11. Permitir o upload de arquivo de descrição OpenAPI, e bloquear as solicitações que não correspondam às definições do arquivo;

2.4.8.12. Suportar as seguintes funções de API gateway:

2.4.8.12.1. Verificação de chaves na API;

2.4.8.12.2. Controle de acesso API;

2.4.8.12.3. Controle de limite de taxa;

2.4.8.12.4. Permitir a restrição baseada em endereçamento IP;

2.4.8.12.5. Permitir restringir o acesso à API através de regras envolvendo verificação de chave API e ações específicas de qualquer violação de chamada API.

2.5. **Suporte Técnico**

2.5.1. O suporte técnico será devido desde o primeiro dia de vigência contratual e se estenderá a toda a solução adquirida;

2.5.2. Os serviços de suporte técnico contemplam as atividades de assistência técnica "onsite" para atendimento em caso de problemas na solução, esclarecimentos de dúvidas técnicas, atualização de firmware e software;

2.5.3. O suporte técnico aos produtos fornecidos deverá contemplar serviços de atendimento a dúvidas técnicas, por telefone, site e/ou e-mail, bem como serviços de suporte "onsite", sem limites de chamados técnicos em qualquer modalidade;

2.5.4. O suporte da solução deve ser entregue de forma unificada em relação à CONTRATANTE, ou seja, feito através de um único ponto de contato;

2.5.5. O suporte técnico, obrigatoriamente, deverá ser realizado pelo fabricante da solução e/ou pela CONTRATADA;

2.5.6. Todas as correções que necessitarem de urgência e/ou alterações ou correções que impactarem no ambiente (necessidade de reiniciar o equipamento) deverão ser feitas após o expediente, devendo assim considerar que o suporte deva prever atendimento em horário comercial (de segunda-feira a sexta-feira, de 08:00 horas às 18:00 horas), com exceção de atendimentos a situações de Nível 1 de Severidade (conforme item 2.5.11);

2.5.7. O serviço de suporte técnico deverá prever o aconselhamento sobre a implementação e a melhor utilização dos produtos adquiridos, objetivando o aumento de desempenho e a estabilidade do ambiente;

2.5.8. Inicialmente, todo atendimento será realizado via telefone (0800) e/ou telefone local e/ou site eletrônico e/ou e-mail, salvo quando os especialistas da CONTRATADA julgarem necessário ou quando uma visita técnica for solicitada pelo CONTRATANTE para solução de um problema. Os dias e horários de atendimento obedecerão à conveniência do CONTRATANTE;

2.5.9. Os chamados somente poderão ser fechados após concordância e autorização do CONTRATANTE;

2.5.10. A CONTRATADA entregará ao final do atendimento on-site, relatório de serviço que conste, pelo menos, os dados do técnico da CONTRATADA, os dados do colaborador que abriu o chamado junto à CONTRATADA, o problema descrito no ato da abertura do chamado, a avaliação e solução implementada, observações, hora de abertura e fechamento do chamado, e campo para assinatura de representantes da CONTRATADA e do CONTRATANTE;

2.5.11. O Acordo de Nível de Serviços deverá obedecer aos seguintes parâmetros:

ACORDO DE NÍVEL DE SERVIÇOS

SEVERIDADE	DESCRIÇÃO
Severidade 1 - Crítico	Falha gravíssima que ocasiona a paralisação total dos equipamentos do ambiente. A falha restringe totalmente a utilização dos sistemas. Ambiente produtivo totalmente impactado. Tempo de atendimento: em até 03 horas úteis. SLA: 98% Tempo de atuação visando solução ou contingenciamento: em até 06 horas após atendimento.
Severidade 2 - Urgente	Falha grave que ocasiona a paralisação parcial dos equipamentos (50% ou mais). A falha restringe moderadamente a utilização do sistema. Impacto parcial no ambiente produtivo. Tempo de atendimento: em até 08 horas úteis. SLA: 90% Tempo de atuação visando solução ou contingenciamento: em até 10 horas úteis após atendimento.
Severidade 3 - Importante	Falha de componentes ou módulos isolados que não resultem em restrições substanciais ou indisponibilidade de uso. Solicitações de reprogramações são classificadas como Severidade 3. Atividades com menores impactos ao ambiente produtivo. Tempo de atendimento: em até 16 horas úteis. SLA: 80% Tempo de atuação visando solução ou contingenciamento: em até 16 horas úteis após atendimento.

2.5.12. Os chamados abertos terão seus tempos de atendimento contabilizados a partir do momento em que a CONTRATADA for notificada da anomalia pela área técnica da CONTRATANTE, seja por contato telefônico ou sistema de abertura de chamados técnicos por meio eletrônico (call home), ou quaisquer formas de contato formal implementadas admitidas pelo direito;

2.5.13. Envio de técnico a campo: caso seja constatada a necessidade de envio de um técnico para resolver a anomalia, a CONTRATADA deve enviar um técnico ao local onde o sistema está instalado até o próximo dia útil;

2.5.14. Chamados para software: podem ser realizados remotamente;

2.5.15. Reposição de peças/hardware defeituosas: caso seja constatada a necessidade de troca de peças/hardware defeituosas para resolver a anomalia, a CONTRATADA deve enviar as peças ao local onde o sistema está instalado até o próximo dia útil;

2.5.16. A solução deverá possuir função de acesso remoto para diagnóstico pelo respectivo fabricante em caso de falhas ou defeitos. A função deve estar disponível para toda a solução, de modo integral (lâminas, armazenamento, chassis, software). Os dispositivos necessários para a implementação dessa funcionalidade são de responsabilidade da CONTRATADA, à exceção de eventual linha telefônica comum, ou conexão à internet, que será fornecida pela CONTRATANTE;

2.5.17. O acesso remoto será controlado pela CONTRATANTE e só poderá ser habilitado com autorização expressa da CONTRATANTE;

2.5.18. A CONTRATADA deve informar antecipadamente à CONTRATANTE qualquer necessidade de acesso remoto;

2.5.19. Todas as intervenções realizadas remotamente são de responsabilidade da CONTRATADA, cabendo ao mesmo responder por quaisquer danos porventura decorrentes dessas intervenções;

2.5.20. Os appliances deverão possuir função de "call-home", através de linha VPN ("Virtual Private network") ou acesso seguro e diagnóstico remoto em caso de erros/defeitos, para a central do fabricante;

2.5.21. Deverá ser fornecido número telefônico do tipo 0800 com atendimento na central de suporte do fabricante 24x7 para a abertura de chamados técnicos;

2.5.22. Serviços de suporte e assistência técnica para HARDWARE e SOFTWARE, gerenciados e prestados pelo fabricante da solução, nos locais onde os equipamentos estiverem instalados ("on-site"), incluindo o fornecimento de peças originais para reposição (exceto peças consumíveis, quando aplicável, de acordo com o manual do fabricante) e demais reparos necessários por um período de 60 meses, no regime 24x7 (vinte e quatro horas por sete dias por semana), incluindo feriados e finais de semana, com solução em até o próximo dia útil para chamados de HARDWARE para as situações onde a falha de componentes de hardware impeça a execução de atividades críticas de negócios;

2.5.23. Todos os chamados serão atendidos e gerenciados pela central de atendimento do fabricante da solução de hardware e software através de número telefônico 0800 ou equivalente de ligação gratuita ou com custo local, fornecendo neste momento o número, data e hora da abertura do chamado;

2.5.24. A CONTRATADA deverá manter o mais rigoroso sigilo sobre quaisquer dados, informações, documentos e especificações que a ela venham a ser confiados ou que venha a ter acesso em razão da execução dos serviços, não podendo, sob qualquer pretexto, revelá-los, divulgá-los, reproduzi-los ou deles dar conhecimento a quaisquer terceiros;

2.5.24.1. O sigilo mencionado no item anterior se estende aos funcionários e ex-funcionários da CONTRATADA, estando esta responsável por formalizar o consentimento de seus colaboradores;

2.5.25. A CONTRATADA deverá possuir nas suas instalações, onde atividades serão executadas de modo remoto, padrões de segurança da informação e de tecnologia da informação para evitar a perda ou o vazamento, ataques externos e tentativas de invasão, como firewall e sistemas antivírus;

2.5.26. Cada profissional a serviço da CONTRATADA deverá assinar o Termo de Sigilo e Responsabilidade da Política de Segurança de TIC, bem como declaração de estar ciente de que a estrutura computacional da CONTRATADA ou CONTRATANTE não poderá ser utilizada para fins diversos daqueles do objeto relacionado à prestação do serviço;

2.5.26.1. O referido documento deverá ser elaborado pela CONTRATADA e esta o remeterá preenchido e assinado pelos profissionais em até 60 (sessenta) dias após a assinatura do contrato. Para profissionais incluídos nos quadros de funcionários da CONTRATADA após o referido prazo, a documentação deverá ser enviada em até 30 (trinta) dias após a inclusão;

2.6. **Especificações gerais**

2.6.1. Os itens 1 e 2 são appliances, e são entendidos como tal segundo os critérios da *Storage Networking Industry Association* - SNIA, não sendo aceitas soluções baseadas em servidores montados para atender estas especificações, Ready Nodes, Certified Nodes ou similares. Assim, deverão ser integrados no fabricante do equipamento, de modo que sejam tratados como um produto único para efeitos de garantia, suporte e atualização;

2.6.2. Para os itens 1 e 2, o overhead máximo admitido será de 15% com compressão e deduplicação;

2.6.3. A duração mínima da prestação de serviço de suporte técnico será de 60 (sessenta) meses;

2.6.4. Nos termos do art. 114 da Lei Federal nº 14.133, de 2021, a presente aquisição tem por objetivo a operação continuada de sistemas estruturantes de tecnologia da informação, constituídos por itens de hardware e software essenciais ao desempenho das atividades do Centro de Tecnologia em Sistemas da PMMG, que nos termos da Resolução nº 4.820, de 2019, é a Unidade responsável pelas atividades relacionadas ao desenvolvimento tecnológico e manutenção na Polícia Militar de Minas Gerais, de tecnologia da informação, incumbindo-lhe prover a infraestrutura de processamento de dados (*data center*) e desenvolvimento, sustentação e manutenção de softwares para atendimento das demandas institucionais;

2.6.5. Em caso de força maior, caso fortuito ou fato do príncipe ou em decorrência de fatos imprevisíveis ou previsíveis de consequências incalculáveis, que inviabilizem a execução do contrato tal como pactuado, respeitada, em qualquer caso, a repartição objetiva de risco estabelecida no contrato, este poderá ser objeto alteração para reestabelecimento do equilíbrio econômico-financeiro;

2.6.6. Os custos operacionais de espaço e energia elétrica e controle de acesso serão de responsabilidade da CONTRATANTE;

2.6.6.1. A infraestrutura será instalada na Prodemge, em regime de Colocation. Por questões de dimensionamento de custos dos equipamentos que compõem a solução, admite-se a ocupação máxima de 10 (dez) U, podendo ser instalada toda a solução no mesmo rack ou com divisão em racks separados;

2.6.7. Os requisitos de performance devem ser comprovados com documentação pública, disponível no site do fabricante;

2.6.8. Os conceitos de hot-swap e hot-plug mencionados neste documento estão associados à possibilidade de substituir unidades de armazenamento, fontes e/ou unidades de ventilação, independente do motivo pela qual a substituição seja necessária, sem interrupção da operação plena do equipamento;

2.6.9. As atividades de instalação deverão ser realizadas dentro do horário comercial e deverão atender às melhores práticas indicadas pelo fabricante;

2.6.10. A implantação deverá abranger a migração da solução antiga para a nova, com o acompanhamento da equipe técnica da CONTRATANTE, ou quem ela indicar, em horário acordado entre as partes, inclusive devendo considerar a atividade em dias e horários fora do horário comercial;

2.6.10.1. Deverá ser feita a migração do ambiente virtualizado da CONTRATANTE para o cluster de hiperconvergência, conforme orientações da CONTRATANTE. A CONTRATADA deverá importar, no mínimo, as máquinas virtuais existentes no ambiente, bem como eventuais máquinas virtuais que forem acrescidas no período entre a publicação do edital e o início da prestação do serviço de implantação. Para fins de referência, o ambiente de produção conta atualmente com 280 (duzentos e oitenta) máquinas virtuais;

2.6.10.2. Deverão ser configurados, após a migração, os planos de backup, emissão e envio de alertas da ferramenta de gerenciamento, e demais configurações de máquinas virtuais, em acordo com o determinado pela CONTRATANTE;

2.6.10.3. As configurações de rede (ex: IPs, VLANs, etc) e alocação de recursos (processador, memória, armazenamento, etc) deverão ser mantidas ou minimamente modificadas durante a migração, seguindo as melhores práticas do fabricante da solução e recomendações da CONTRATANTE;

2.6.10.4. É responsabilidade da CONTRATADA possíveis conversões das máquinas virtuais de um hypervisor para outro, caso necessário;

2.6.10.5. A implantação também deve abranger a configuração de quaisquer funcionalidades suportadas pelo equipamento/software, desde que especificadas neste documento. Estas informações serão documentadas no termo de abertura do projeto a ser elaborado pela CONTRATADA após alinhamento do escopo de trabalho entre CONTRATADA e CONTRATANTE;

2.6.11. Todo o processo de instalação e configuração realizado deverá ser documentado pela CONTRATADA sob a forma de relatório, contendo o passo-a-passo de toda instalação e configuração dos equipamentos envolvidos no projeto;

2.6.11.1. A documentação deverá ser entregue em meio eletrônico, em formato PDF, contendo, no mínimo:

- Identificação e resumo dos equipamentos instalados;
- Prospectos e manuais oficiais dos produtos;
- Diagrama visual da solução (as-built), demonstrando no mínimo as conexões elétricas e de dados, tipos de conexões, portas usadas, tipos de cabos, redundâncias, VLANs e IPs;
- Lista de protocolos de conexão utilizados e configurados;
- Lista de portas físicas usadas e suas configurações de VLAN nos equipamentos;
- Lista de todos os equipamentos, sistemas de gerenciamento e demais funções, com os respectivos endereços IP implementados e suas VLANs;
- Lista de softwares instalados e configurados e respectivos equipamentos;
- Relatório técnico dos procedimentos de instalação e configuração dos equipamentos, bem como das configurações realizadas nos softwares da solução;
- Lista de todos usuários e senhas configuradas para cada função da solução (sistemas de gerenciamento, consoles de configuração, usuários de acesso diversos, dentre outros);
- Lista de licenças e respectivos sistemas, softwares, equipamentos ou componentes, com data de vigência, e número serial, código, ou outra informação que permita a identificação;
- Lista dos telefones, endereços de e-mail, e ferramenta web para contato e suporte da CONTRATADA e dos fabricantes dos itens que compõem a solução.

2.6.12. A instalação física deverá compreender a desembalagem e montagem de todos os componentes que integram a especificação dos dispositivos, montagem, conexão à rede de dados e alimentação elétrica dos equipamentos, e o que mais for necessário à completa instalação;

2.6.13. A configuração deverá compreender a realização dos ajustes de hardware e software necessários ao funcionamento dos dispositivos a fim de apresentarem a melhor performance de funcionamento possível, e o que mais for necessário à completa configuração;

2.6.14. Deverão ser feitas todas as atualizações de firmware ou qualquer outro software componente da solução para a versão mais atualizada disponível ou a última compatível com os demais componentes desta solução e considerada estável;

2.6.15. Devem ser realizados todos os testes e ajustes de hardware e software necessários ao perfeito funcionamento da solução;

2.6.16. A solução ofertada deverá ser fornecida com todos os licenciamentos necessários para o completo atendimento dos requisitos deste documento (para software de gerenciamento, hypervisor, e qualquer outro sistema, software, hardware ou componente que necessite licenciamento);

2.6.17. Todos os softwares da solução devem ser ofertados em sua última versão estável e homologada para o funcionamento em ambiente de produção na data de entrega da solução e que suporte todas as características mínimas especificadas neste documento;

2.6.18. Devem ser disponibilizadas todas as atualizações de firmware ou software que compõem a solução para a versão mais atualizada ou a última compatível e considerada estável;

2.6.19. Deverão ser habilitadas todas as licenças que porventura sejam adquiridas e recursos dos equipamentos que serão utilizados no projeto;

2.6.20. Deverá ser providenciado todo o acabamento necessário, evitando que restem fios e cabos expostos, preservando a qualidade estética do ambiente;

2.6.21. A solução deverá ser pré integrada logicamente, com seus componentes interligados sem ponto único de falha, de acordo com as melhores práticas do fabricante, permitindo o acesso ao portal de configuração da solução como um todo imediatamente após a energização e conexão física e lógica do sistema;

2.6.22. A CONTRATADA deverá aplicar os patches de segurança nos equipamentos que compõem a solução sempre que forem disponibilizados pelo fabricante;

2.6.23. Todos os componentes de hardware e software da solução deverão ser devidamente licenciados, garantidos e suportados por pelo menos 5 (cinco) anos, sendo que o licenciamento relativo aos appliances hiperconvergentes e switches (se aplicável) deverão ser fornecidos em caráter permanente.

3. **DOS LOTES**

3.1. Considerando:

- A necessidade de otimizar a gestão contratual por parte da Administração, em atenção ao princípio da eficiência da Administração Pública (art. 37 CRFB/1988);
- A solução mais assertiva de eventuais intercorrências de ordem técnica na vigência contratual;
- A imprescindibilidade da continuidade na prestação dos serviços ofertados pela Diretoria de Tecnologia e Sistemas, a qual atende os públicos interno e externo;
- A natureza integrada da solução - as soluções de data center e segurança necessariamente devem ter compatibilidade e interoperabilidade;
- O não proveito de eventual contratação parcial, uma vez que, mesmo que a solução fosse dividida em lotes, a contratação só seria levada a efeito caso todos os lotes fossem bem sucedidos;

Não é possível dividir a solução em lotes. A CONTRATADA será a responsável por fornecer a solução e, juntamente com o fabricante dos respectivos itens, prestar o suporte técnico relativo à solução.

4. **DA JUSTIFICATIVA DA CONTRATAÇÃO**

4.1. Conforme Estudo Técnico Preliminar (94976532).

5. **DA PARTICIPAÇÃO DE CONSÓRCIOS**

5.1. Não será permitida a participação de empresas reunidas em consórcio, devido à baixa complexidade do objeto a ser adquirido, considerando que as empresas que atuam no mercado têm condições de fornecer a solução de forma independente.

6. **DA QUALIFICAÇÃO TÉCNICA**

6.1. Para a comprovação da qualificação técnica, deverá ser atendida pelo menos uma das hipóteses:

6.1.1. Atestados comprovando o fornecimento anterior, de 25% (vinte e cinco porcento) do objeto especificado, fornecidos por pessoa jurídica de direito público ou privado, vedado o auto atestado;

6.1.2. Declaração fornecida pelo(s) fabricante(s) dos itens que compõem a solução e ofertada pelo Licitante que ateste a capacidade para atender aos itens especificados;

6.2. Para atendimento do quantitativo indicado, é admitido o somatório de atestados, desde que compatíveis com as características do objeto da licitação e definidas no item 6.1.1.

7. **DOS CRITÉRIOS DE ACEITABILIDADE DAS PROPOSTAS**

7.1. A proposta deve vir acompanhada do datasheet dos produtos ofertados;

7.2. A proposta deverá incluir no preço o serviço de implantação da solução, prevendo a configuração, ativação e colocação em produção dos equipamentos descritos;

7.3. A licença mencionada na descrição do item 2.1 deve integrar o fornecimento do nó, mas vir separada na precificação da proposta;

7.4. Caso seja necessário mais de uma licença para atender aos requisitos descritos nos itens 2.1 e 2.2, o preço de cada licença deverá constar separadamente na proposta;

7.5. Deverão ser fornecidos os prospectos, folders, fichas técnicas ou outro documento que comprove que os produtos ofertados atendem as especificações técnicas deste Termo de Referência;

7.6. A quantidade necessária das licenças ofertadas deve ser devidamente explicada na proposta, expondo de forma clara todos os critérios de licenciamento para cada tipo de métrica (por exemplo: número de nó de hiperconvergência/número de núcleos de processamento/número de máquinas virtuais), sendo que o escolhido deverá ser o de menor preço final. Em virtude de cada fabricante possuir sua própria lógica de licenciamento, o licitante poderá consultar formalmente o CONTRATANTE a fim de obter os dados necessários para fins de dimensionamento;

7.7. Deverão oferecer na proposta o telefone de suporte ou interface web para abertura e acompanhamento dos chamados para acionamento da garantia. O contato telefônico deverá ser do tipo 0800 ou telefone local em português do Brasil.

8. **DA EXECUÇÃO DO OBJETO**

8.1. **Prazo de entrega**

8.1.1. A entrega correrá conforme quadro abaixo:

DESCRIÇÃO DO ITEM	QTD
Appliance Hiperconvergente com licenciamento	2
Appliance Hiperconvergente com GPU e licenciamento	1
Switch Topo de Rack (ToR)	2
Solução de Segurança Virtualizada - Web Application Firewall (WAF)	2

8.1.2. A solução deverá ser integralmente entregue em até 90 (noventa) dias corridos contados do dia seguinte ao recebimento da Nota de Empenho, Autorização de Fornecimento ou documento equivalente;

8.1.3. O prazo de instalação deverá ocorrer em até 30 (trinta) dias corridos, a contar do recebimento provisório dos itens (item 8.3.1.1);

8.1.4. A entrega deve ser agendada com antecedência mínima de 24 horas, sob o risco de não ser autorizada;

8.1.5. Para itens de software, poderá ser fornecido sem mídia de instalação, desde que seja indicado local para download do arquivo de instalação;

8.1.6. Devidamente justificado e antes de finalizado o prazo de entrega, o fornecedor do produto poderá solicitar prorrogação da entrega, ficando a cargo da área demandante aceitar a solicitação, desde que não haja prejuízo na prestação do serviço público face ao atraso;

8.2. **Local de instalação e horário de entrega**

8.2.1. Para o local de entrega e a instalação da solução, deverá ser considerada a cidade de Belo Horizonte/MG**;**

8.2.2. A entrega será realizada em horário comercial;

8.2.3. A instalação do hardware ou software correrão sob a responsabilidade da CONTRATADA, que deverá entregar toda a solução plenamente funcional e pronta para uso pela CONTRATANTE, sendo inclusive responsável por fornecer um repasse básico da administração dos itens adquiridos, de forma que a equipe da CONTRATANTE esteja minimamente preparada para operar os equipamentos adquiridos, especialmente os de primeiro uso na instituição, sem prejuízo do treinamento detalhado no item 10;

8.2.4. Todas as fases de planejamento, instalação e configuração deverão ser realizadas com a presença de técnicos da CONTRATADA, que deverão possuir capacidade técnica necessária à execução do serviço;

8.2.5. Os trabalhos deverão ser realizados dentro do horário comercial, das 08:30 horas às 17:00 horas, salvo casos em que se necessite de parada no ambiente que demande janelas de manutenção. Neste último caso, devem ser ajustados os horários com antecedência.

8.3. **Condições de recebimento**

8.3.1. Os itens que compõem a solução serão recebidos:

8.3.1.1. Provisoriamente, no ato da entrega, pelo fiscal ou equipe de fiscalização nomeada pela CONTRATANTE, para efeito de posterior verificação da conformidade do material/serviço 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;

8.3.1.2. Definitivamente, após a verificação da qualidade e quantidade do produto e consequente aceitação, por comissão designada pela CONTRATANTE, que deverá acontecer em até 30 (trinta) dias corridos, contados a partir do recebimento provisório;

8.3.2. O recebimento/aprovação do(s) itens(s) que compõem a solução, pela Polícia Militar de Minas Gerais, não exclui a responsabilidade civil do fornecedor por vícios de quantidade ou qualidade do(s) itens(s) que compõem a solução ou disparidades com as especificações estabelecidas, verificadas posteriormente, garantindo-se a Administração as faculdades previstas no art. 18 da Lei n° 8.078/90;

8.3.3. Somente serão aceitos equipamentos novos e sem uso. Não serão aceitos equipamentos remanufaturados, NFR (Not For Resale) ou de demonstração. Os equipamentos deverão ser entregues nas caixas lacradas pelo fabricante, não sendo aceitos equipamentos com caixas violadas;

8.3.4. Nos casos de sinais externos de avaria de transporte ou de mau funcionamento do equipamento, verificados na inspeção do mesmo, este deverá ser substituído por outro com as mesmas características, no prazo de até 30 (trinta) dias corridos, a contar da data de realização da inspeção.

9. **DAS GARANTIAS**

9.1. A CONTRATADA deverá prover garantia técnica da solução, isto é, o pleno e correto funcionamento de seus equipamentos e componentes de hardware e software, pelo período de 60 (sessenta) meses, a partir da data de ativação da primeira licença que compõe a solução. Os fabricantes serão responsáveis solidários pela garantia, naquilo que lhes couber;

9.2. Não serão aceitos, em hipótese alguma, outros condicionantes para o início da garantia, tais como: auditorias, estudos ou avaliações técnicas prévias, aplicações de recomendações por parte da CONTRATADA;

9.3. Durante todo o período de garantia, a CONTRATADA obriga-se a substituir, recuperar e/ou modificar os softwares e firmwares instalados, sem ônus de qualquer natureza à CONTRATANTE, nos casos comprovados de mau funcionamento e de outras falhas, de modo a ajustá-los aos resultados que atendam às especificações técnicas solicitadas para o equipamento. Durante o prazo de garantia, deverá ser substituído o equipamento, componente, parte ou peça que porventura apresente defeito, sem ônus para a CONTRATANTE;

9.4. Defeitos decorrentes de projeto, fabricação, construção, montagem, acondicionamento, transporte, erros na instalação física e/ou desgaste prematuro, envolvendo, obrigatoriamente, a substituição dos componentes defeituosos, sem qualquer ônus adicional para o CONTRATANTE;

9.5. São consideradas obrigações decorrentes da garantia de funcionamento, no que se refere aos aplicativos e serviços da implantação, eventuais correções de problemas relativos a defeitos (bugs etc.), bem como o fornecimento de todas as correções e evoluções de softwares (patches, novas versões etc.) tornadas disponíveis no mercado por seus fabricantes;

9.6. Deve disponibilizar recurso via Web do site do fabricante de cada componente da solução (em documentação entregue), que permita verificar a garantia dos equipamentos através da inserção do seu número de série, dentre outras informações;

9.7. Toda e qualquer peça ou componente consertado ou substituído fica automaticamente coberto até o final do prazo estabelecido para a garantia técnica da solução. Em caso de recorrência de defeito em uma mesma peça ou componente consertada, essa deverá ser substituída. As peças e componentes que substituírem os defeituosos deverão ser novos;

9.8. Os prazos para substituição de componentes defeituosos devem seguir os prazos mencionados no item de suporte técnico (SLA);

9.9. Ao final do período de garantia e suporte técnico, a solução ofertada (hardware e software) não poderá perder suas funcionalidades. A solução deve permanecer completamente funcional independente do prazo de garantia e suporte técnico. No caso de funcionalidades que dependam de licenciamento específico, as licenças de uso da solução deverão ser perpétuas;

9.10. A CONTRATADA, como integradora da solução, deverá garantir a completa interoperabilidade e compatibilidade entre os equipamentos a serem contratados. Deverá, ainda, prover o auxílio técnico necessário à interoperação da rede, a fim de garantir a perfeita comunicação entre os ativos contratados com os demais ativos existentes no ambiente da CONTRATANTE;

9.11. Sendo a CONTRATADA designada para realizar a implantação da solução, será de sua responsabilidade a correção das falhas decorrentes de erros durante as atividades de implantação, sejam operacionais ou por problemas de mau funcionamento, responsabilizando-se por todos os custos envolvidos na

correção dos desvios, sejam de interoperabilidade, incompatibilidade ou quaisquer outras falhas que impeçam a instalação ou o perfeito funcionamento dos equipamentos contratados, até o aceite da implantação pela CONTRATANTE;

9.12. Atualização pertinente aos produtos de software, inclusive dos softwares embarcados nos equipamentos. Para fins desta especificação técnica, entende-se como atualização o provimento de toda e qualquer evolução, incluindo-se patches, hot fixes, correções, updates, service packs, novas releases, builds e funcionalidades, e o provimento de upgrades englobando, inclusive, versões não sucessivas, caso a disponibilização ocorra durante o período da vigência contratual;

9.12.1. A CONTRATADA deve disponibilizar, sem quaisquer custos adicionais à CONTRATANTE, a atualização de novas versões dos softwares e firmwares fornecidos, ou de parte deles, decorrentes da evolução funcional ou correções dos anteriormente fornecidos, durante o prazo da garantia da solução;

9.13. Cabe à CONTRATADA informar à equipe técnica da CONTRATANTE a disponibilidade de novas versões e atualizações, assim como quanto aos respectivos procedimentos de instalação;

9.14. A CONTRATANTE reserva-se o direito de aceitar ou não atualizações no software ou parte dele;

9.15. A CONTRATADA deve garantir que uma nova versão do software ou firmware mantenha a compatibilidade e contenha todas as funções das versões anteriores e que a introdução desta não prejudique a interoperabilidade da mesma na rede, mantendo as especificações deste documento;

9.16. A CONTRATADA deve garantir a independência entre a correção de defeitos (patches) e a geração de novas versões do software, sem ônus adicional à CONTRATANTE, em função da necessidade de atualização de componente para suportar nova versão do software;

9.17. A CONTRATADA, no caso da atualização de equipamento para corrigir falhas apresentadas, deve se responsabilizar pelos custos envolvidos, inclusive eventuais trocas de hardware;

9.18. A CONTRATADA deve garantir o funcionamento dos equipamentos, em acordo com as características descritas nos manuais e nas especificações dos fabricantes;

9.18.1. Caso a CONTRATADA verifique a necessidade de encaminhar equipamento para assistência técnica, deverá providenciar o imediato empréstimo de outro equipamento ao CONTRATANTE, em perfeito estado de funcionamento e com características técnicas idênticas ou superiores àquelas do equipamento defeituoso, o qual o substituirá até a conclusão de seus reparos. É responsabilidade da CONTRATADA instalar e configurar o novo equipamento, garantindo o funcionamento da solução dentro das mesmas condições anteriores ao problema. Cabe lembrar que a CONTRATADA é responsável pela garantia do sigilo das informações configuradas no equipamento;

9.18.2. Para retirada do equipamento defeituoso das dependências do CONTRATANTE, deverá a CONTRATADA relatar, formalmente, a situação ao colaborador responsável pelo acompanhamento dos serviços, que, após constatar tal necessidade, autorizará a saída também por meio formal;

9.18.3. Os componentes instalados em substituição aos danificados deverão ter características, no mínimo, iguais aos originais do equipamento. Caso sejam utilizados componentes com características superiores, não haverá ônus adicional para o contratante. Os componentes, instalados em substituição a componentes defeituosos passarão a fazer parte do equipamento, sendo, portanto, objeto de opção de aquisição posterior do CONTRATANTE;

9.18.4. O equipamento colocado em substituição ficará instalado nas dependências do CONTRATANTE até a devolução do equipamento consertado, que deverá ocorrer no prazo de até 30 (trinta) dias corridos após a sua retirada para reparos;

9.18.5. Caso os equipamentos fornecidos sejam descontinuados na linha de fabricação do fabricante, durante a vigência da garantia, a CONTRATADA deverá manter as condições da garantia nesta contratação explicitadas ou providenciar a substituição por outros modelos disponíveis que executem as mesmas funcionalidades exigidas no edital, sem ônus adicionais para o CONTRATANTE;

9.18.6. Toda e qualquer substituição deverá ser acompanhada pelo fiscal do contrato ou por colaborador designado por ele;

9.18.7. A CONTRATADA deverá disponibilizar, via web, relatório técnico indicando os defeitos, procedimentos realizados, data/hora e nome do colaborador que fez o atendimento;

9.18.8. Deverá ser disponibilizada central telefônica do(s) fabricante(s) para abertura de chamados técnicos através de ligação gratuita para atendimento técnico, bem como possuir site na internet com a disponibilização de drivers, firmwares e todas as atualizações existentes relativas ao equipamento ofertado.

10. **DO TREINAMENTO**

10.1. Deverá ser ministrado treinamento "hands on" (operação assistida), cuja carga horária mínima será de 80 (oitenta) horas e poderá ser realizado nos equipamentos recém-instalados;

10.2. O treinamento deverá ocorrer nas dependências da CONTRATANTE, em datas e horários previamente acordados entre as partes;

10.3. Todas as despesas decorrentes do treinamento, tais como transporte e alimentação dos profissionais, correrão às expensas da CONTRATADA;

10.4. A CONTRATADA deverá efetuar o repasse de conhecimento avançado, abrangendo configuração, operação, segurança, disponibilidade e melhores práticas sobre os equipamentos e softwares contratados;

10.5. O treinamento poderá ocorrer no ambiente de produção da CONTRATADA, entretanto, caso sejam necessárias operações que possam inviabilizar o funcionamento da solução, a CONTRATADA deverá providenciar ambiente de testes/treinamento específico para estas operações, ou usar abordagem que seja suficiente para o repasse de conhecimento;

10.6. O treinamento deverá incluir teoria, saneamento de dúvidas, exercícios e laboratórios (hands-on), durante 10 (dez) dias úteis sucessivos ou não, a critério da CONTRATANTE;

10.7. O treinamento deverá ser ministrado para pelo menos 10 (dez) participantes, a critério da CONTRATANTE, que poderá designar menos participantes;

10.8. Deverão ser considerados na ementa do treinamento, pelo menos, os seguintes tópicos:

10.8.1. Configuração, operação e gerenciamento dos equipamentos: instalação física; ligar, desligar e reiniciar; cabos e transceivers; portas e conexões de componentes; operação de substituição de fontes, sistemas de ventilação e unidades de armazenamento; componentes do equipamento; controles visuais (LEDs, LCDs e outros monitores); configurações iniciais; acesso à interface de gerenciamento diretamente no equipamento; configurações avançadas do equipamento pela interface; procedimentos de recuperação com substituição de nós e todos os seus componentes (unidades de armazenamento, memória, bateria, placas expansoras, etc.); configurações de VLANs, agregação de links, e uso de demais protocolos de rede nos switches e interfaces dos equipamentos;

10.8.2. Configuração e operação do software de hiperconvergência e hypervisor: acesso para gerenciamento; configurações iniciais e avançadas; configuração e manutenção de nós; configuração e manutenção de rede lógica; configuração e manutenção de unidades de armazenamento, storage e datastores; manutenção, conversão e configuração de máquinas virtuais (incluindo alocação de recursos e configurações de rede); procedimentos de backup e recuperação com manutenção de nós; gestão de logs;

10.8.3. Configuração e operação do ambiente de gestão centralizada: acesso ao ambiente; monitoramento de uso e capacidade de recursos; monitoramento em tempo real de processamento, uso de memória, uso de rede e I/O; monitoramento em nível de informações, alertas e erros; configurações de protocolos de monitoramento; ações diversas de gestão da solução; gestão de logs; planejamento de capacidade; avaliação de saúde (health check);

10.8.4. Gestão administrativa: verificação e atualização de licenças; verificação e atualização de certificados (auto assinados ou externos - Wildcard); gestão de usuários; gestão de logs;

10.8.5. WAF: utilizando a interface gráfica de administração do WAF e conhecimento das funções gerenciais;

10.8.5.1. O instrutor dos produtos mencionados no item 10.8.5 deverá ser certificado pelo fabricante da solução;

10.9. A ementa, abrangendo os tópicos mínimos, deverá ser proposta pela CONTRATADA e enviada para a CONTRATANTE pelo menos 2 (dois) dias úteis antes do início do treinamento, em meio eletrônico. A CONTRATANTE se reserva o direito de sugerir a inclusão ou exclusão de tópicos relevantes, antes do início do treinamento;

10.10. O conteúdo do material e das ações de treinamento deverão ser entregues em formato eletrônico aberto (docx, odt, etc.), devendo ainda:

10.10.1. Ser construído em linguagem dialogada, favorecendo a interatividade;

10.10.2. Ser atualizado e preciso - oferecer uma representação fidedigna de fatos, princípios, procedimentos de segurança, e operação das tecnologias, entre outros;

10.10.3. Apresentar claramente os objetivos de cada módulo, resumo, atividades de aplicação e verificação do conhecimento;

10.10.4. Apresentar os módulos de maneira clara e ordenada, de tal forma que se estabeleça uma relação lógica entre eles;

10.10.5. Conter as referências bibliográficas;

10.10.6. Levar em consideração as melhores práticas indicadas pelo fabricante da solução.

10.11. A qualidade do treinamento será avaliada pelos participantes ao final de sua realização e, caso sua qualidade seja considerada insuficiente, a CONTRATADA deverá reformular sua metodologia e providenciar realização de nova turma, até o alcance dos objetivos do repasse, sem ônus adicional para a CONTRATANTE;

10.12. O profissional da CONTRATADA deverá acompanhar e aferir o funcionamento da solução implantada, apoiar a equipe técnica da CONTRATANTE nas adequações da solução às necessidades e especificidades, responder dúvidas, bem como prover suporte durante o período de prestação do treinamento;

10.13. Durante a operação assistida, o profissional deverá prover relatórios técnicos diários, apresentando dados quantitativos e qualitativos do funcionamento da solução, para a devida aferição da sua correta operação em produção;

10.14. O profissional deverá ser capaz de operar todas as funcionalidades de todos os componentes e softwares da solução, físicos ou lógicos, bem como orientar os funcionários da CONTRATANTE nestas atividades;

10.15. O profissional deverá ser capaz de reconfigurar a solução para realizar possíveis ajustes necessários, identificados durante a operação assistida, com o devido repasse de conhecimento para os funcionários da CONTRATANTE;

10.16. Toda a operação assistida deverá levar em consideração as melhores práticas indicadas pelo fabricante da solução;

10.17. Os treinamentos serão considerados aceitos quando atestados pelo fiscal e gestor do contrato, por parte da CONTRATANTE, observados, necessariamente, os seguintes critérios:

10.17.1. Aprovação pela CONTRATANTE da ementa do treinamento;

10.17.2. Cumprimento integral do disposto neste capítulo;

10.17.3. Avaliação positiva de, no mínimo, 75% por parte dos participantes, em formulário próprio, a ser elaborado pela CONTRATADA, contendo as seguintes questões:

10.17.3.1. Conteúdo apresentado e estrutura do treinamento:

- Clareza na definição do conteúdo do treinamento;
- Adequação do conteúdo programático do treinamento;
- Adequação da sequência de apresentação do conteúdo;
- Adequação da dinâmica de treinamento;
- Disponibilidade e qualidade do material.

10.17.3.2. Desempenho do Instrutor:

- Uso de estratégias para motivar os participantes;
- Uso das estratégias instrucionais (estudo de caso, atividades, exemplos);
- Nível de conhecimento sobre os temas e assuntos abordados;
- Segurança na transmissão dos conteúdos do treinamento;
- Disposição para esclarecer dúvidas e reações às ideias e questões dos participantes acerca dos temas abordados.

10.17.4. As questões da avaliação receberão notas de 1 a 5 (1-Muito insatisfeito, 2-Insatisfeito, 3-Neutro, 4-Satisfeito, 5-Muito satisfeito);

10.17.5. Deverão existir dois campos para respostas abertas, um para comentários gerais sobre o treinamento e outro para comentários gerais sobre o instrutor;

10.17.6. Caso a avaliação total não seja superior ou igual a 75% (setenta e cinco por cento) da nota máxima possível (não satisfatório), o treinamento deverá ser melhorado e aplicado novamente, sem ônus adicional para a CONTRATANTE, em data e horário a serem definidos pela CONTRATANTE.

11. **DA SUBCONTRATAÇÃO**

11.1. Será permitida a subcontratação para o item de segurança (item 4 - Web Application Firewall), mantendo-se a CONTRATADA obrigada a fornecer suporte técnico único e com ponto único de contato para toda a solução.

Rafael Henrique de Souza Pereira, Cap PM

Chefe da Seção de Infraestrutura - CTS

Documento assinado eletronicamente por **Rafael Henrique de Souza Pereira**, **Capitão**, em 07/08/2025, às 15:51, conforme horário oficial de Brasília, com fundamento no art. 6º, § 1º, do Decreto nº 47.222, de 26 de julho de 2017.

A autenticidade deste documento pode ser conferida no site http://sei.mg.gov.br/sei/controlador_externo.php?acao=documento_conferir&id_orgao_acesso_externo=0, informando o código verificador **119979215** e o código CRC **ABF9DAE1**.