	adaptadores, softwares, licenças, itens de acabamento, etc. **SUPORTE E GARANTIA** Para viabilizar a execução do serviço de suporte de forma a minimizar períodos de indisponibilidade, deverá ser disponibilizado software de gestão de suporte de Hardware com as seguintes características: Monitoramento ativo do ambiente. Identifica problemas que afetem o funcionamento e o desempenho dos equipamentos; Abertura automática de chamados junto ao fabricante; As características do serviço são as seguintes: Período do serviço: 5 anos; Tempo de atendimento contato a partir da abertura do chamado, o qual ocorre via 0800 Intervalo de cobertura: 24 x 7 (24 horas por dia, 7 dias por semana); Suporte remoto Assistência remota para solução de problemas comuns de suporte.		
Solução de Backup	**CARACTERÍSTICAS GERAIS:** A solução de armazenamento Appliance integrado de backup em disco a ser ofertada deverá atender integralmente os requisitos especificados neste Termo, devendo ser fornecida com todas as licenças que forem necessárias para entrega totalmente funcional da solução. A solução de armazenamento de backup a ser proposta pela proponente deverá obrigatoriamente fazer uso de sistemas inteligentes de armazenamento de backup em disco, baseado em appliance, que se entende como subsistema composto de hardware e software com o propósito específico de ingestão dos dados de backup, desduplicação e replicação dos dados desduplicados. O appliance deverá ser novo, sem uso, e integrar a linha de produção atual do fabricante. O appliance deverá fazer parte do catálogo atual de produtos comercializados pelo fabricante e não ter sido descontinuado, pelo menos, até a data da entrega. O appliance deverá constar no site do fabricante (documento oficial e público). O appliance composto de hardware e software integrado, deverá ser do mesmo fabricante, não sendo aceito regime de OEM no fornecimento da solução e todo o suporte seja prestado pela mesma engenharia. A solução ofertada deverá permitir a utilização de todas as funcionalidades, tecnologias e recursos especificados, de maneira perpétua e irrestrita. Direito e permissão de atualização para novas versões durante a vigência do contrato, sem ônus para a CONTRATANTE. O appliance deverá ser composto, de processamento e armazenamento integrado, dedicado única e exclusivamente, à execução das atividades de console de gerenciamento, catálogo, gerenciadores das rotinas de proteção, ingestão, desduplicação e replicação dos dados, sem a necessidade de servidores adicionais de backup para seu funcionamento. O appliance deverá prover uma solução de gerenciamento das atividades de backup, restore, monitoração de sistema de software e hardware e gerenciamento de falhas e alarmes. O	Und	01

	appliance deverá possuir a funcionalidade de desduplicação: Entende-se por desduplicação dos dados, a funcionalidade que permite eliminar segmentos redundantes e compactar os dados, de forma a reduzir a capacidade de disco destinada ao armazenamento dos dados de backup. A desduplicação deverá segmentar os dados em blocos de tamanho variável, ajustados automaticamente pelo próprio algoritmo do appliance de forma a atingir as melhores taxas de desduplicação. A desduplicação deverá ser global, considerando e comparando todos os dados armazenados no sistema em sua total capacidade. A funcionalidade de desduplicação de dados em blocos deverá ser executada concomitantemente com a ingestão dos dados (data ingestion) e replicação, eliminando a necessidade de armazenamento intermediário para cache dos dados. Não serão aceitas soluções que realizem a desduplicação após a gravação do dado no disco (pós-processo/paralelo) ou mesmo híbridas que realizem parte do processo antes e parte após a gravação em disco. A desduplicação de blocos deverá acontecer na origem dos dados (cliente-side deduplication), ou seja, no cliente de backup, antes dos dados serem enviados e gravados nos discos do appliance. Deverá possuir uma taxa de transferência mínima de 14TB/h(quatorze terabyte por hora). O appliance deverá possuir funcionalidade de replicação de dados: A solução de armazenamento de backup em disco deverá possuir licença para replicação dos dados armazenados no dispositivo de armazenamento para outro dispositivo de mesma natureza em formato desduplicado. Os dados replicados pelo sistema de armazenamento devem ser refletidos no catálogo do aplicativo de backup. O appliance deverá permitir a replicação assíncrona dos dados que devem ocorrer em horários ajustáveis e pré-determinados. A solução de armazenamento de backup em disco deverá permitir múltiplas políticas de disaster recovery para prevenir perda de dados tais como: cópia automática do catálogo do backup, sincronização entre as cópias do catálogo do backup e suporte para replicação para cloud pública AWS e Azure. Deverá possuir interface de administração gráfica (Graphical User Interface – GUI). Todo o tráfego de conexão entre os clientes e o appliance integrado deve ser criptografado. Permitir executar múltiplos processos de backup em paralelo. A solução de armazenamento de backup em disco deverá ser capaz de suportar falhas de até dois discos simultâneos, devendo ser fornecido com proteção RAID-6, RAID-DP ou similar. A área de armazenamento da solução deverá ser disponibilizada em discos rígidos com capacidade máxima de 12TB (doze Terabytes) com tecnologia SAS ou NL-SAS. Deve permitir no mesmo equipamento a expansão da área de armazenamento a no mínimo, 24TB (Vinte e quatro		

	Terabytes) úteis, considerando BASE10 como cálculo de capacidade(1TB=1000GB), em uma única área de armazenamento global e deve ser atingida somente com discos e/ou licença de software de todas os recursos especificados. A solução deve ter no mínimo 2 processadores multi-core. A solução deve fazer uso de discos do tipo SSD (Solid State Drive) ou NVMe para aceleração de metadados. Será facultada a oferta do dobro (2x) de memória cache solicitada neste certame para as soluções que não fazem uso de discos SSD ou NVMe para aceleração, de forma a compensar a menor eficiência deste tipo de equipamento. A solução de armazenamento de backup deverá possuir no mínimo 384 GB (trezentos e oitenta e quatro gigabytes) de memória RAM. Deverá suportar as seguintes interfaces de interconexão: Interfaces 10GbE e 25Gb Ethernet: A solução de armazenamento de backup deverá suportar as seguintes interfaces de interconexão para integração com os clientes de backup, replicação e gerência: No mínimo, 04 (quatro) portas Ethernet de 10 Gbps SFP+ (Dez gigabit por segundo). Os componentes de power supply (fontes de alimentação) e fan (ventiladores) devem ser redundantes. As rotinas internas de manutenção dos dados de backup armazenados tais como: Processo de limpeza (Garbage Collector ou housekeeping) e Validação de integridade (data integrity), devem ser executados em paralelo com as rotinas de backup e recuperação, ou seja, a solução ofertada não deve exigir parada ou interrupção (blackout window) das atividades de backup/restore para tarefas internas do equipamento. Deve prover “software” de administração e gerenciamento, que permitam a análise de desempenho e implementação das políticas de backup e de acesso de usuários. O APPLIANCE DEVERÁ ENTREGAR AS SEGUINTES CARACTERÍSTICAS DE SEGURANÇA: Deverá suportar criptografia de no mínimo 256-SHA, possuindo gerenciamento de chave de segurança nativo do appliance, sem depender de qualquer gerenciador de chave externa. A solução deve possuir recurso de mídia WORM (Write Once Read Many) SEC 17a-4 (f) de proteção contra alteração/regravação e exclusão dos dados armazenados, permitindo somente uma única escrita e múltiplas leituras, garantindo integridade e autenticidade, deste modo a solução não deverá permitir que usuários consigam alterar ou apagar dados protegidos, até que o tempo de retenção configurado tenha expirado. Não serão aceitas soluções que não possuam SEC 17a-4 (f) a fim de garantir a imutabilidade dos dados. Deverá possuir acesso seguro com 2FA suportando Google Auth ou Microsoft Authenticator. Deve suportar nativamente enviar de forma desduplicada e criptografada os dados de backup para um armazenamento em nuvem pública ou privada para dados de longa retenção, sem a necessidade de aquisição		

	de dispositivos e softwares de terceiros. Deverá possuir mecanismo inteligente que verifique continuamente de forma automática a integridade lógica dos dados, "ponteiros" e índices armazenados (fim-a-fim) no hardware com correção automática das falhas encontradas, de forma a garantir a consistência de todo o conteúdo em sua total capacidade, sem a utilização de scripts e/ ou composições feitas exclusivamente para atendimento a esse item. O equipamento deve fazer uso de API para permitir que os backups sejam acessados e enviados para o repositório de backup sem que o volume esteja montado no servidor de backup, eliminando qualquer risco de propagação Ransomware e acesso aos dados de backups armazenados. Deverá utilizar padrão de criptografia AES-256 para replicação dados em trânsito (in-flight) e em repouso (at-rest). Deverá realizar a criptografia dos dados no agente de backup no cliente, na transmissão dos dados através da rede IP e no armazenamento em disco do backup. Possuir capacidade de estabelecer níveis de acesso e perfis diferenciados e configuráveis para atividades de administração e operação do software de backup. A solução deve possibilitar gerenciar múltiplos equipamentos em uma única console de gerenciamento central. **ESPECIFICAÇÕES TÉCNICAS DO LICENCIAMENTO:** Deve estar licenciada para permitir a utilização de no mínimo 12TB (Doze Terabytes) úteis e disponíveis para gravação, considerando BASE10 como cálculo de capacidade(1TB=1000GB), descontadas todas as perdas com redundâncias, paridades e os ganhos com compactação e desduplicação de dados ou qualquer outro mecanismo de redução de dados para efeito de cálculo de capacidade disponível. O Sistema Operacional do equipamento deverá ser licenciado e nativo do produto. Não serão aceitas as modalidades OEM de sistemas operacionais de propósito geral, tal como Windows ou qualquer distribuição do Linux. Deverá possuir catálogo ou banco de dados centralizado contendo as informações sobre todos os dados e informações do ambiente protegido. Esse banco de dados ou catálogo deverá ser próprio e fornecido em conjunto com o produto. Os softwares necessários para execução do software de backup, tais como, Sistema Operacional, Banco de Dados e qualquer outro necessário para o perfeito funcionamento do software de backup devem ser inclusos. O licenciamento de software deverá permitir que seja efetuado backup em quantidades ilimitadas, sem limite de capacidade e número de clientes, até que se extingue a área de armazenamento liquida livre solicitada. Para as soluções onde o licenciamento de software é calculado a partir da capacidade em TB (Terabytes) de origem dos dados (Front End), o licenciamento de software de backup deverá permitir que seja efetuado backup de no mínimo 10 (dez) vezes a capacidade de		

	armazenamento solicitada. Não serão permitidos outros tipos de licenciamento. Deverá permitir utilizar um armazenamento em nuvem pública e suportar AWS, Azure e Google para fins de longa retenção, sem a necessidade de aquisição de softwares de terceiros. O licenciamento desta funcionalidade deve permitir a utilização de até 02 x (duas vezes) capacidade total solicitada deste certame. A área de armazenamento em nuvem pública não faz parte deste certame. Deverá possuir mecanismos que verifique o atendimento de SLA (service-level agreement) das políticas de backup e o Appliance deverá emitir alertas caso algum nível de serviço não esteja sendo atendido. Possuir mecanismo de reconstrução do catálogo ou banco de dados centralizado em caso de perda do mesmo. Possuir função de agendamento do backup. Possuir interface web para gerenciamento, monitoramento e criação de políticas de backup e restore. Permitir a programação de tarefas de backup automatizadas em que sejam definidos prazos de retenção dos arquivos e/ou imagens. Deverá permitir o agendamento de jobs de backup nativamente no software controlador, sem a necessidade de usar utilitários externos (softwares de terceiros). Permitir a realização do backup completo de servidor para recuperação de desastres. Possuir capacidade de estabelecer níveis de acesso diferenciados e configuráveis para atividades de administração e operação do software de backup. A solução de backup deverá, a partir de uma única interface, gerenciar operações de backup e restore de diferentes sistemas operacionais (clientes). Deverá prover monitoramento e gerenciamento via interface gráfica e em tempo real dos jobs sendo executados. Deverá suportar operações de backup e restore em paralelo. Deverá prover relatórios gerenciais de backup com no mínimo as seguintes informações: Quantidade e relação dos Backups com sucesso. Volume de backup transferido. Quantidade e relação dos restores. Relação de clientes de backup configurados. Ocupação do backup. Deverá permitir exportar relatórios em alguns dos formatos: PDF, XML, HTML ou CSV. **POSSUIR SUPORTE A BACKUP E RESTORE DE MÁQUINAS VIRTUAIS VMWARE COM AS SEGUINTES CARACTERÍSTICAS:** Deve possuir a capacidade de realizar backup das máquinas virtuais Windows e Linux. Suportar o mecanismo de proteção para máquinas virtuais sendo totalmente integrado ao ESXi e sem a necessidade de VMs para execução da função de proxies/agents/data movers/media server. Caso a proponente não possua tal característica, será facultado a integração com o VADP, desde que, a proponente inclua infraestrutura/servidor adicional necessário em sua proposta, para executar a função de "proxies/data movers/media server" incluindo todo hardware e licenciamento necessário para seu perfeito funcionamento. O servidor deverá atender com as		

	seguintes características mínimas ou mais recursos a depender das boas práticas do fabricante: Deverá possuir licenciamento VMWARE para permitir virtualização dos proxies. Caso necessite de sistema operacional, o mesmo deverá estar licenciado e com suporte do fabricante. Deverá possuir no mínimo 2 (dois) processadores para servidores corporativos das famílias Intel Xeon ou AMD EPYC, de terceira geração ou superior, sendo que cada processador deverá ter no mínimo 16 núcleos de processamento e frequência mínima de 2,00GHz. O processador deverá estar em linha de produção pelo fabricante do processador e a época de lançamento deve ser igual ou superior ao primeiro quadrimestre de 2021, não sendo aceitos processadores descontinuados. Deverá possuir no mínimo 192GB (cento e noventa e dois Gigabytes) de memória RAM DDR4 ou superior, com tecnologia de correção ECC (Error Correcting Code), provisionados por módulos de mesmo tamanho e na velocidade máxima suportada pelo processador. A memória RAM deverá ser fornecida pelo FABRICANTE do equipamento, devendo ser compatível e homologada para o processador e para o modelo de servidor físico. Os módulos deverão ser distribuídos de forma a proporcionar maior desempenho. Deverá possuir 2 (dois) discos SSD de no mínimo 240GB, conectados a uma controladora RAID configurada em RAID-1. Deverá possuir capacidade para pelo menos 4 (quatro) discos de 2,5 polegadas hot-swap e hot-pluggable, permitindo a troca de disco sem a necessidade de abrir o gabinete, e sem a necessidade de desligar o servidor. Deverá possuir módulo de gerenciamento, com suporte a gerenciamento remoto da solução e suporte a IPMI-over-LAN. Deverá permitir a recuperação de máquinas virtuais através de plugin integrado ao VMWare. Deverá possuir funcionalidade nativa para descoberta automática das máquinas virtuais VMWare conforme são criadas no ambiente virtual para que através de filtros possam ser incluidas nas políticas/rotinas de backup, sem a utilização de scripts e/ ou composições feitas exclusivamente para atendimento a esse item. Possui funcionalidade de replicação dos backups de máquinas virtuais VMWARE para um armazenamento em nuvem pública para fins de disaster recovery, sem a necessidade de aquisição de softwares de terceiros. O licenciamento desta funcionalidade deverá ser igual a capacidade total solicitada neste edital. A área de armazenamento em nuvem pública não faz parte deste certame. Permitir integração nativa através de API com vRealize Automation**.** Possuir suporte a backup e restore de máquinas virtuais VMware 6.5 ou superior. Deve permitir que através de uma única rotina de Backup seja possível recuperar a imagem completa da máquina virtual Windows e Linux (VMDK), somente o VMDK desejado de forma seletiva e os arquivos de maneira granular sem a		

	necessidade de scripts, ou área temporária. Deve suportar o uso da funcionalidade CBT (Change Block Tracking) para as operações de backup e restore. Deve permitir a identificação de aplicações Microsoft SQL que residem nas máquinas virtuais, através de integração VADP, permitindo o backup, recuperação integral ou granular. Deverá permitir o "instant recovery", ou seja, iniciar de maneira imediata a execução de base de dados SQL virtualizadas, diretamente a partir do seu repositório de backup. Deve permitir restaurar e iniciar de maneira imediata a execução de múltiplas máquinas virtuais instantaneamente, diretamente a partir do seu repositório de backup. Deve permitir a recuperação granular de arquivos (FLR) a partir do backup da imagem completa (VMDK). Deve possuir a capacidade de balanceamento de carga automático dos backups. Deve possuir capacidade de realizar backup de maneira off-host, sem a necessidade de instalação de agentes nas máquinas virtuais. Deve possuir a capacidade de recuperação da imagem da máquina virtual, para máquinas que possuam discos VMFS ou RDM. A solução deve disponibilizar recurso de busca e indexação dos dados de backup copiados, de forma a buscar de forma granular os arquivos protegidos nos servidores utilizando apenas o nome do arquivo desejado. **POSSUIR SUPORTE A BACKUP E RESTORE DE AMBIENTE KUBERNETES COM AS SEGUINTES CARACTERÍSTICAS:** Deve possuir integração nativa com Kubernetes no nível de namespaces e PVCs, não sendo aceitos scripts ou backups no nível de sistema de arquivos para atendimento a esse item. Deve suportar volumes contidos em armazenamento tipo CSI-based. Deve realizar o backup completo do Namespace e seus objetos como: Pods, Secrets, Services, Deployments, Replica set, Certificates, ConfigMaps e Persistent Volumes. Deve ser capaz de realizar a descoberta automática de namespaces dentro de um cluster. Possuir políticas de backup dinâmicas onde através de filtros e regras um novo Namespace pode ser protegido em uma determinada política de maneira automática, sem intervenção do administrador. Permitir o restore do Namespace nos seguintes formatos: Restore para o Namespace original. Restore para um Namespace existente. Restore para um novo Namespace. Restore do Namespace em um outro cluster Kubernetes diferente da origem**.** Suportar diferentes distribuições de Kubernetes em ambientes VMWare, Red Hat OpenShift, Rancher, Google Anthos, Microsoft Azure Kubernetes Service (AKS), Google Kubernetes Engine (GKE) e Amazon Elastic Kubernetes Service (EKS). Serão aceitas composições com softwares de terceiros para prover as funcionalidades solicitadas, desde que o nível de suporte atenda ao solicitado desde que centralizado e total integrado a solução de appliance. **SUPORTE E GARANTIA:** Para viabilizar a execução do serviço de suporte de forma a minimizar períodos de		

	indisponibilidade, deverá ser disponibilizado software de gestão de suporte de Hardware com as seguintes características: Monitoramento ativo do ambiente. Identifica problemas que afetem o funcionamento e o desempenho dos equipamentos; Abertura automática de chamados junto ao fabricante; As características do serviço são as seguintes: Período do serviço: 5 anos; Tempo de atendimento contato a partir da abertura do chamado, o qual ocorre via 0800 Intervalo de cobertura: 24 x 7 (24 horas por dia, 7 dias por semana); Suporte remoto Assistência remota para solução de problemas comuns de suporte.		
Switch 48 L2	**SWITCH DE ACESSO 48 PORTAS:** Deve possuir 48 (quarenta e oito) interfaces do tipo 1000Base-T para conexão de cabos de par metálico UTP com conector RJ-45. Deve implementar a auto-negociação de velocidade e duplex destas interfaces, além de negociar automaticamente a conexão de cabos crossover (MDI/MDI-X); Adicionalmente, deve possuir 4 (quatro) slots SFP+ para conexão de fibras ópticas do tipo 10GBase-X operando em 1GbE e 10GbE. Estas interfaces não devem ser do tipo combo e devem operar simultaneamente em conjunto com as interfaces do item anterior; Deve possuir porta console para acesso à interface de linha de comando (CLI) do equipamento através de conexão serial. O cabo e eventuais adaptadores necessários para acesso à porta console deverão ser fornecidos; Deve possuir 1 (uma) interface USB; Deve possuir capacidade de comutação de pelo menos 176 Gbps e ser capaz de encaminhar até 260 Mpps (milhões de pacotes por segundo); Deve suportar 4000 (quatro mil) VLANs de acordo com o padrão IEEE 802.1Q; Deve possuir tabela MAC com suporte a 32.000 endereços; Deve operar com latência igual ou inferior à 1us (microsegundo); Deve implementar Flow Control baseado no padrão IEEE 802.3X; Deve permitir a configuração de links agrupados virtualmente (link aggregation) de acordo com o padrão IEEE 802.3ad (Link Aggregation Control Protocol – LACP); Deve suportar a comutação de Jumbo Frames; Deve suportar a criação de rotas estáticas em IPv4 e IPv6; Deve suportar IGMP snooping para controle de tráfego de multicast; Deve permitir o espelhamento do tráfego de uma porta para outra porta do mesmo switch (port mirroring / SPAN); Deve implementar Spanning Tree conforme os padrões IEEE 802.1w (Rapid Spanning Tree) e IEEE 802.1s (Multiple Spanning Tree). Deve implementar pelo menos 15 (quinze) instâncias de Multiple Spanning Tree; Deve implementar recurso conhecido como PortFast ou Edge Port para que uma porta de acesso seja colocada imediatamente no status "Forwarding" do Spanning Tree após sua conexão física; Deve possuir mecanismo conhecido como Loop Guard para identificação de loops	Und	05

	na rede. Deve desativar a interface e gerar um evento quando um loop for identificado; Deverá possuir controle de broadcast, multicast e unicast nas portas do switch. Deve suportar a criação de listas de acesso (ACLs) para filtragem de tráfego. Deverá implementar priorização de tráfego baseada nos valores do campo "Differentiated Services Code Point" (DSCP) do cabeçalho IP, conforme definições do IETF; Deve possuir ao menos 8 (oito) filas de priorização (QoS) por porta; Deverá implementar mecanismo de proteção contra ataques do tipo man-in-the-middle que utilizam o protocolo ARP; Deve implementar controle de acesso por porta através do padrão IEEE 802.1X com assinalamento dinâmico de VLAN por usuário com base em atributos recebidos através do protocolo RADIUS; Deve suportar MAC Authentication Bypass (MAB); Deve implementar RADIUS CoA (Change of Authorization); Deve implementar Guest VLAN para aqueles usuários que não autenticaram nas interfaces em que o IEEE 802.1X estiver habilitado; Deve suportar o envio de mensagens de log para servidores externos através de syslog; Deve suportar o protocolo SNMP (Simple Network Management Protocol) nas versões v1, v2c e v3; Deve suportar o protocolo HTTPS para configuração e administração remota através de interface web; Deve permitir upload de arquivo e atualização do firmware (software) do switch através da interface web (HTTPS); Deve permitir ser gerenciado através de IPv6; Deve permitir a criação de perfis de usuários administrativos com diferentes níveis de permissões para administração e configuração do switch; Deve suportar o protocolo LLDP e LLDP-MED para descoberta automática de equipamentos na rede de acordo com o padrão IEEE 802.1ab; Deverá ser capaz de executar testes nas interfaces para identificar problemas físicos nos cabos de par trançado (UTP) conectados ao switch. Deverá suportar ser configurado e monitorado através de REST API; Deve suportar o padrão IEEE 802.3az (Energy Efficient Ethernet - EEE); Deve possuir LEDs que indiquem o status de atividade de cada porta; Deve suportar temperatura de operação de até 45º Celsius; Deve possuir MTBF (Mean Time Between Failures) igual ou superior a 10 (dez) anos; Deve ser fornecido com fonte de alimentação interna com capacidade para operar em tensões de 110V e 220V; Deve permitir a sua instalação física em rack padrão 19" com altura máxima de 1U. Todos os acessórios para montagem e fixação deverão ser fornecidos; Deve possuir garantia e suporte pelo período de 36 (trinta e seis) meses.		
Switch 48 POE L3	**SWITCH DE ACESSO 48 PORTAS POE -** Deve possuir 48 (quarenta e oito) interfaces do tipo 1000Base-T para conexão de cabos de par metálico UTP com conector RJ-45. Deve implementar a auto-negociação de velocidade e duplex destas interfaces, além de negociar	Und	01

	automaticamente a conexão de cabos crossover (MDI/MDI-X); Adicionalmente, deve possuir 4 (quatro) slots SFP+ para conexão de fibras ópticas do tipo 10GBase-X operando em 1GbE e 10GbE. Estas interfaces não devem ser do tipo combo e devem operar simultaneamente em conjunto com as interfaces do item anterior; Deve possuir porta console para acesso à interface de linha de comando (CLI) do equipamento através de conexão serial. O cabo e eventuais adaptadores necessários para acesso à porta console deverão ser fornecidos; Deve possuir 1 (uma) interface USB; Deve possuir capacidade de comutação de pelo menos 176 Gbps e ser capaz de encaminhar até 260 Mpps (milhões de pacotes por segundo); Deve suportar 4000 (quatro mil) VLANs de acordo com o padrão IEEE 802.1Q; Deve possuir tabela MAC com suporte a 32.000 endereços; Deve operar com latência igual ou inferior à 1us (microsegundo); Deve implementar Flow Control baseado no padrão IEEE 802.3X; Deve permitir a configuração de links agrupados virtualmente (link aggregation) de acordo com o padrão IEEE 802.3ad (Link Aggregation Control Protocol – LACP); Deve suportar a comutação de Jumbo Frames; Deve implementar roteamento (camada 3 do modelo OSI) entre as VLANs; Deve suportar a criação de rotas estáticas em IPv4 e IPv6; Deve implementar serviço de DHCP Relay; Deve suportar IGMP snooping para controle de tráfego de multicast; Deve permitir o espelhamento do tráfego de uma porta para outra porta do mesmo switch (port mirroring / SPAN); Deve implementar Spanning Tree conforme os padrões IEEE 802.1w (Rapid Spanning Tree) e IEEE 802.1s (Multiple Spanning Tree). Deve implementar pelo menos 15 (quinze) instâncias de Multiple Spanning Tree; Deve implementar recurso conhecido como PortFast ou Edge Port para que uma porta de acesso seja colocada imediatamente no status "Forwarding" do Spanning Tree após sua conexão física; Deve possuir mecanismo conhecido como Loop Guard para identificação de loops na rede. Deve desativar a interface e gerar um evento quando um loop for identificado; Deverá possuir controle de broadcast, multicast e unicast nas portas do switch. Quando o limite for excedido, o switch deve descartar os pacotes ou aplicar rate limit; Deve suportar a criação de listas de acesso (ACLs) para filtragem de tráfego. Deve permitir a definição de dias e horários que a ACL deverá ser aplicada na rede; Deverá implementar priorização de tráfego baseada nos valores do campo “Differentiated Services Code Point” (DSCP) do cabeçalho IP, conforme definições do IETF; Deve possuir ao menos 8 (oito) filas de priorização (QoS) por porta; Deverá implementar mecanismo de proteção contra ataques do tipo man-in-the-middle que utilizam o protocolo ARP; Deve implementar DHCP Snooping para mitigar problemas com servidores DHCP que não estejam autorizados na rede;		

	Deve implementar controle de acesso por porta através do padrão IEEE 802.1X com assinalamento dinâmico de VLAN por usuário com base em atributos recebidos através do protocolo RADIUS; Deve suportar MAC Authentication Bypass (MAB); Deve implementar RADIUS CoA (Change of Authorization); Deve implementar Guest VLAN para aqueles usuários que não autenticaram nas interfaces em que o IEEE 802.1X estiver habilitado; Deve suportar o envio de mensagens de log para servidores externos através de syslog; Deve suportar o protocolo SNMP (Simple Network Management Protocol) nas versões v1, v2c e v3; Deve suportar o protocolo HTTPS para configuração e administração remota através de interface web; Deve permitir ser gerenciado através de IPv6; Deve permitir a criação de perfis de usuários administrativos com diferentes níveis de permissões para administração e configuração do switch; Deve suportar o protocolo LLDP e LLDP-MED para descoberta automática de equipamentos na rede de acordo com o padrão IEEE 802.1ab; Deverá ser capaz de executar testes nas interfaces para identificar problemas físicos nos cabos de par trançado (UTP) conectados ao switch. Deverá suportar ser configurado e monitorado através de REST API; Deve suportar o padrão IEEE 802.3az (Energy Efficient Ethernet - EEE); Deve possuir LEDs que indiquem o status de atividade de cada porta; Deve suportar temperatura de operação de até 45º Celsius; Deve possuir MTBF (Mean Time Between Failures) igual ou superior a 10 (dez) anos; Deve ser fornecido com fonte de alimentação interna com capacidade para operar em tensões de 110V e 220V; Deve permitir a sua instalação física em rack padrão 19" com altura máxima de 1U. Todos os acessórios para montagem e fixação deverão ser fornecidos; Deve possuir garantia e suporte pelo período de 36 (trinta e seis) meses.		
Next Generation Firewall (NGFW)	**CARACTERÍSTICAS DO EQUIPAMENTO:** Throughput de, no mínimo, 10 Gbps; Suporte a, no mínimo, 700.000 conexões simultâneas; Suporte a, no mínimo, 35.000 novas conexões por segundo**;** Throughput de, no mínimo, 6,5 Gbps de VPN IPSec**;** Estar licenciado para, ou suportar sem o uso de licença, 200 túneis de VPN IPSEC Site-to-Site simultâneos**;** Estar licenciado para, ou suportar sem o uso de licença, 500 túneis de clientes VPN IPSEC simultâneos**;** Throughput de, no mínimo, 900 Mbps de VPN SSL**;** Suportar no mínimo 1,4 Gbps de throughput de IPS**;** Suportar no mínimo 630 Mbps de throughput de Inspeção SSL**;** Deverá ser entregue com no mínimo as seguintes interfaces de conexão: 02 portas RJ45 GE WAN; 05 portas RJ45 GE Internal; 02 Portas RJ45 GE; 01 porta RJ45 DMZ; 01 USB; 01 porta RJ45 console. **REQUISITOS MÍNIMOS DE FUNCIONALIDADE:** A solução deve consistir em plataforma de proteção de rede baseada em appliance com funcionalidades de Next Generation	Und	01

	Firewall (NGFW) e monitoração; Por funcionalidades de NGFW entende-se: reconhecimento de aplicações, prevenção de ameaças, identificação de usuários e controle granular de permissões; A plataforma deve oferecer recursos de rede avançados que se integram com domínios virtuais e de segurança de camada 7; A gestão do equipamento deve ser compatível através da interface de gestão Web no mesmo dispositivo de proteção da rede; Os dispositivos de proteção de rede devem possuir suporte a 4094 VLAN Tags 802.1q; Os dispositivos de proteção de rede devem possuir suporte a agregação de links 802.3ad e LACP; Os dispositivos de proteção de rede devem possuir suporte a Policy base drouting ou policy based forwarding; Os dispositivos de proteção de rede devem possuir suporte a roteamento multicast; Os dispositivos de proteção de rede devem possuir suporte a DHCP Relay; Os dispositivos de proteção de rede devem possuir suporte a DHCP Server; Os dispositivos de proteção de rede devem suportar sFlow; Os dispositivos de proteção de rede devem possuir suporte a Jumbo Frames; Os dispositivos de proteção de rede devem suportar sub-interfaces ethernet logicas; Deve suportar NAT64 e NAT46; Deve implementar o protocolo ECMP; Deve suportar SD-WAN de forma nativa; Deve implementar balanceamento de link por hash do IP de origem e destino; Deve implementar balanceamento de link por peso. Nesta opção deve ser possível definir o percentual de tráfego que será escoado por cada um dos links. Deve suportar o balanceamento de, no mínimo, dois links; Deve permitir monitorar via SNMP; Enviar log para sistemas de monitoração externos, simultaneamente; Deve haver a opção de enviar logs para os sistemas de monitoração externos via protocolo TCP e SSL; Para IPv4, deve suportar roteamento estático e dinâmico (RIP, BGP e OSPF); Para IPv6, deve suportar roteamento estático e dinâmico (OSPFv3); Suportar OSPF graceful restart; Deve suportar Modo Sniffer, para inspeção via porta espelhada do tráfego de dados da rede; Deve suportar Modo Camada – 2 (L2), para inspeção de dados em linha e visibilidade do tráfego; Suporte a configuração de alta disponibilidade Ativo/Passivo, Ativo/Ativo; A configuração em alta disponibilidade deve sincronizar: Sessões; Deve possuir suporte a criação de sistemas virtuais no mesmo appliance; Deve permitir a criação de administradores independentes, para cada um dos sistemas virtuais existentes, de maneira a possibilitar a criação de contextos virtuais que podem ser administrados por equipes distintas; O gerenciamento da solução deve suportar acesso via SSH e interface WEB (HTTPS), incluindo, mas não limitado a exportar configuração dos sistemas virtuais (contextos) por ambas as interfaces; Deve fornecer uma solução de segurança holística abrangendo toda a rede;		

	Deve ser capaz de identificar potenciais ataques e destacar as melhores práticas que poderiam ser usadas para melhorar a segurança e o desempenho geral de uma rede; Deve existir um Serviço de Suporte que oferece aos clientes uma verificação de saúde recorrente com um relatório de auditoria mensal personalizado de seus appliances NGFW; O console de administração deve suportar pelo menos inglês, espanhol e português. A solução deve suportar integração nativa de equipamentos de proteção de e-mail, firewall de aplicativo, proxy, cache e ameaças avançadas. **CONTROLE POR POLÍTICA DE FIREWALL**: Deverá suportar controles por zona de segurança; Controles de políticas por porta e protocolo; Controle de políticas por aplicações, grupos estáticos de aplicações, grupos dinâmicos de aplicações (baseados em características e comportamento das aplicações) e categorias de aplicações; Controle de políticas por usuários, grupos de usuários, IPs, redes e zonas de segurança; Firewall deve ser capaz de aplicar a inspeção UTM (Application Control e Webfiltering no mínimo) diretamente às políticas de segurança versus via perfis; Além dos endereços e serviços de destino, objetos de serviços de Internet devem poder ser adicionados diretamente às políticas de firewall; Deve suportar automatização de situações como detecção de equipamentos comprometidos, estado do sistema, mudanças de configuração, eventos específicos, e aplicar uma ação que possa ser notificação, bloqueio do equipamento, execução de scripts ou funções em nuvem pública. Deve suportar o padrão de indústria 'syslog' protocol para armazenamento usando o formato Common Event Format (CEF); Deve haver uma maneira de assegurar que o armazenamento dos logs em tempo real não supera a velocidade de upload; Deve suportar o protocolo padrão da indústria VXLAN; Em SD-WAN deve suportar QoS, modelamento de tráfego, rotas por políticas, VPN IPSec; A solução deve suportar a integração nativa com soluções de sandboxing, proteção de correio eletrônico, cache e firewall de aplicação Web. **CONTROLE DE APLICAÇÕES**: Os dispositivos de proteção de rede deverão possuir a capacidade de reconhecer aplicações, independente de porta e protocolo; Reconhecer pelo menos as seguintes aplicações: bittorrent, gnutella, skype, facebook, linked-in, twitter, Citrix Services, logmein, teamviewer, rdp, vnc, gmail, youtube, proxy http, http-tunnel, Facebook_Chat, gmail_chat, whatsapp, 4shared, dropbox, google drive, ibm db2, mysql, oracle TNS, activedirectory, kerberos, ldap, radius, itunes, dhcp, ftp, dns, wins, MS RPC, ntp, snmp, gotomeeting, webex, evernote, googledocs; Para tráfego criptografado SSL, deve de-criptografar pacotes a fim de possibilitar a leitura de payload para checagem de assinaturas de aplicações conhecidas pelo fabricante; Limitar a banda		

	(download/upload) usada por aplicações (trafficshaping), baseado no IP de origem, usuários e grupos; Permitir nativamente a criação de assinaturas personalizadas para reconhecimento de aplicações proprietárias na própria interface gráfica da solução, sem a necessidade de ação do fabricante; O fabricante deve permitir a solicitação de inclusão de aplicações na base de assinaturas de aplicações; Deve ser possível a criação de grupos estáticos de aplicações baseados em características das aplicações como: Categoria da aplicação; Deve ser possível configurar ApplicationOverride permitindo selecionar aplicações individualmente. **PREVENÇÃO DE AMEAÇAS**: Para proteção do ambiente contra ataques, os dispositivos de proteção devem possuir módulo de IPS, Antivírus e Anti-Spyware integrados no próprio appliance de firewall; Deve incluir assinaturas de prevenção de intrusão (IPS) e bloqueio de arquivos maliciosos (Antivírus e Anti-Spyware); As funcionalidades de IPS, Antivírus e Anti-Spyware devem operar em caráter permanente, podendo ser utilizadas por tempo indeterminado, mesmo que não subsista o direito de receber atualizações ou que não haja contrato de garantia de software com o fabricante; Deve permitir o bloqueio ataques baseados em rede; Deve incluir proteção contra ataques de negação de serviços; Deverá possuir o seguinte mecanismo de inspeção de IPS: Análise de decodificação de protocolo; Deverá possuir o seguinte mecanismo de inspeção de IPS: Análise para detecção de anomalias de protocolo; Ser imune e capaz de impedir ataques básicos como: TCP/UDP/ICMP session flooding; Detectar e bloquear a origem de portscans; Deverá possibilitar a criação de assinaturas customizadas pela interface gráfica do produto; Identificar e bloquear comunicação com botnets; Deve suportar a captura de pacotes (PCAP), por assinatura de IPS ou controle de aplicação; Deve ser possível a configuração de diferentes políticas de controle de ameaças e ataques baseado em políticas do firewall considerando Usuários, Grupos de usuários, origem, destino, zonas de segurança, etc, ou seja, cada política de firewall poderá ter uma configuração diferentes de IPS, sendo essas políticas por Usuários, Grupos de usuário, origem, destino, zonas de segurança; **FILTRO DE URL**: Suportar a capacidade de criação de políticas baseadas no controle por URL e categoria de URL; Possuir pelo menos 60 categorias de URLs; Deve possuir a função de exclusão de URLs do bloqueio, por categoria; Permitir a customização de página de bloqueio; Permitir o bloqueio e continuação (possibilitando que o usuário acesse um site potencialmente bloqueado informando o mesmo na tela de bloqueio e possibilitando a utilização de um botão Continuar para permitir o usuário continuar acessando o site); Além do Explicit Web Proxy, suportar proxy Web transparente; Deverá permitir a definição de cota diária pelos seguintes critérios: Por		

	categoria, Por grupo de categorias, ou por classificação. As cotas devem ser definidas para as ações: Monitor, Aviso ou Autenticação; Quando a cota é atingida, o tráfego deverá ser bloqueado e uma página de mensagem de substituição deverá ser exibida. As cotas poderão ser definidas por tempo ou por trafego. **IDENTIFICAÇÃO DE USUÁRIOS**: Deve possuir integração com Microsoft Active Directory para identificação de usuários e grupos permitindo granularidade de controle/politicas baseadas em usuários e grupos de usuários; Deve possuir integração com Radius para identificação de usuários e grupos permitindo granularidade de controle/politicas baseadas em usuários e grupos de usuários; Deve possuir integração com LDAP para identificação de usuários e grupos permitindo granularidade de controle/politicas baseadas em Usuários e Grupos de usuários; Permitir integração com tokens para autenticação dos usuários, incluindo, mas não limitado a acesso à internet e gerenciamento da solução; QOS E TRAFFIC SHAPING Com a finalidade de controlar aplicações e tráfego cujo consumo possa ser excessivo, (como Youtube, Ustream, etc) e ter um alto consumo de largura de banda, se requer que a solução, além de poder permitir ou negar esse tipo de aplicações, deve ter a capacidade de controlá-las por políticas de máxima largura de banda quando forem solicitadas por diferentes usuários ou aplicações, tanto de áudio como de vídeo streaming; Suportar a criação de políticas de QoS e TrafficShaping por endereço de origem; Suportar a criação de políticas de QoS e TrafficShaping por endereço de destino; Suportar a criação de políticas de QoS e TrafficShaping por usuário e grupo; Suportar a criação de políticas de QoS e TrafficShaping por aplicações, incluindo, mas não limitado a Skype, Bittorrent, YouTube e Azureus; Suportar a criação de políticas de QoS e TrafficShaping por porta; O QoS deve possibilitar a definição de tráfego com banda garantida; O QoS deve possibilitar a definição de tráfego com banda máxima; O QoS deve possibilitar a definição de fila de prioridade; Suportar marcação de pacotes Diffserv, inclusive por aplicação; Suportar modificação de valores DSCP para o Diffserv; Suportar priorização de tráfego usando informação de Typeof Service; **FILTRO DE DADOS**: Permitir a criação de filtros para arquivos e dados pré-definidos; Os arquivos devem ser identificados por extensão e tipo; Permitir identificar e opcionalmente prevenir a transferência de vários tipos de arquivos (MS Office, PDF, etc) identificados sobre aplicações (HTTP, FTP, SMTP, etc); Permitir identificar e opcionalmente prevenir a transferência de informações sensíveis, incluindo, mas não limitado a número de cartão de crédito, possibilitando a criação de novos tipos de dados via expressão regular; **GEO LOCALIZAÇÃO:** Suportar a criação de políticas por		

	geolocalização, permitindo o tráfego de determinado País/Países sejam bloqueados; Deve possibilitar a visualização dos países de origem e destino nos logs dos acessos; Deve possibilitar a criação de regiões geográficas pela interface gráfica e criar políticas utilizando as mesmas; **VPN**: Suportar VPN Site-to-Site e Cliente-To-Site; Suportar IPSec VPN; Suportar SSL VPN; A VPN IPSEc deve suportar Autenticação MD5 e SHA-1; A VPN IPSEc deve suportar Diffie-Hellman Group 1, Group 2, Group 5 e Group 14; A VPN IPSEc deve suportar Algoritmo Internet Key Exchange (IKEv1 e v2); A VPN IPSEc deve suportar AES 128, 192 e 256 (Advanced Encryption Standard); Deve permitir habilitar e desabilitar túneis de VPN IPSEC a partir da interface gráfica da solução, facilitando o processo de throuble shooting; O agente de VPN SSL ou IPSEC client-to-site deve ser compatível com pelo menos: Windows, Mac OS, iOS e Android; **SD-WAN**: Deve implementar balanceamento de link por IP de origem; Deve implementar balanceamento de link por IP de destino; Deve implementar balanceamento de link por peso. Nesta opção deve ser possível definir o percentual de tráfego que será escoado por cada um dos links; Deve suportar SD-WAN de forma nativa Deve suportar o balanceamento de links de interfaces físicas, agregação, VLAN e túneis IPSec; Em SD-WAN deve suportar QoS, modelamento de tráfego, rotas por políticas, VPN IPSec; Possuir checagem do estado de saúde do Link baseando-se em critérios mínimos de: Latência, Jitter e Perda de Pacotes; Deve ser possível configurar a porcentagem de perda de pacotes e o tempo de latência e jitter, na medição de estado de link; A checagem de estado de saúde deve suportar teste com Ping, HTTP ou DNS; A solução deve permitir modificar o intervalo de tempo de checagem, em segundos; As regras de escolha do link SD-WAN devem suportar o reconhecimento de aplicações. Deve suportar a configuração de nível mínimo de qualidade (latência, jitter e perda de pacotes) para que determinado link seja escolhido pelo SD-WAN; Deve suportar envio de BGP route-map para BGP neighbors, caso a qualidade mínima de um link não seja detectada pela checagem de saúde do link; A solução deverá ser capaz de monitorar e identificar falhas mediante a associação de healthcheck, permitindo testes de resposta por ping, http, tcp/udpecho, dns, tcp-connect e twamp; O SD-WAN deverá balancear o tráfego das aplicações entre múltiplos links simultaneamente, inclusive 4G; Deve possuir recurso para correção de erro (FEC), possibilitando a redução das perdas de pacotes nas transmissões; Deve ainda possibilitar a marcação de DSCP, a fim de que essa informação possa ser utilizada ao longo do backbone para fins de reserva de banda; A solução de SD-WAN deve prover estatísticas em tempo real a respeito da ocupação de banda e performance do healthcheck (packetloss, jitter e latência); A solução de SD-		