ANEXO I

# ANEXO I DO EDITAL – TERMO DE REFERÊNCIA

**ANEXO I – TERMO DE REFERÊNCIA**

1. **OBJETO:** Aquisição de dispositivo appliance para armazenamento de backup, segurança WEB, licenças VMware, RedHat, Commvault, serviços especializados de implantação RedHat e VMware, e treinamentos Microsoft, Vmware e RedHat
2. **ESPECIFICAÇÕES E DESCRIÇÃO DE OBJETO:** Solução para armazenamento de backup, segurança WEB, expansão de armazenamento, licenças e treinamentos diversos

**LOTE 01 - ITEM 01 - Academic VMware vRealize Operations 8 Advanced**

|  |
| --- |
| ESPECIFICAÇÃO TÉCNICA: Licença perpétua de software - Academic VMware vRealize Operations 8 Advanced (Per CPU) - PN: VR8-OADC-A  Características mínimas:   * 1. Licença perpétua para 01 processador, independentemente da quantidade de servidores virtuais, containers ou aplicações instalados ou gerenciados;   2. Todas as especificações deverão ser atendidas, exclusivamente, por um único fabricante de software. Não serão admitidas propostas que incluam composição de softwares de fabricantes diversos ou variações semelhantes;   3. Serviço de subscrição e garantia de 60 meses com suporte Basic;   4. A garantia e serviço de subscrição deve englobar a manutenção corretiva de todos os componentes e software fornecidos, incluindo upgrades, updates ou patches de correção; |

**LOTE 01 - ITEM 02 - Academic VMware NSX-T Advanced**

|  |
| --- |
| ESPECIFICAÇÃO TÉCNICA: Licença perpétua de software - Academic VMware NSX-T Advanced per Processor - NX-T-ADV-A  Características mínimas:   * 1. Licença perpétua para 01 processador, independentemente da quantidade de servidores virtuais, containers ou aplicações instalados ou gerenciados;   2. Todas as especificações deverão ser atendidas, exclusivamente, por um único fabricante de software. Não serão admitidas propostas que incluam composição de softwares de fabricantes diversos ou variações semelhantes;   3. Serviço de subscrição e garantia de 60 meses com suporte Production;   4. A garantia e serviço de subscrição deve englobar a manutenção corretiva de todos os componentes e software fornecidos, incluindo upgrades, updates ou patches de correção; |

**LOTE 01 - ITEM 03 - Serviços técnicos especializados em VMWare NSX**

|  |
| --- |
| ESPECIFICAÇÃO TÉCNICA – Serviços técnicos especializados VMWare NSX. POR HORA  Características mínimas   * 1. Em até 5 (cinco) dias corridos após a assinatura do contrato, a contratada deverá agendar reunião com representante da Secretaria de Tecnologia da Informação e Comunicação – SETIC - da UDESC e combinar cronograma de instalação e configuração da solução;   2. Deverá ser entregue um cronograma à SETIC em até 5 (cinco) dias corridos após a realização da reunião;   3. O início das atividades deve ocorrer após a aprovação e agendamento do cronograma pela SETIC, e estas deverão ser concluídas no prazo máximo de 60 (sessenta) dias corridos;   4. Todos as configurações deverão ser realizadas seguindo-se obrigatoriamente documento de padronização de nomenclaturas e endereços que será fornecido pela UDESC em momento oportuno antes da instalação;   5. Os serviços de instalação compreendem a instalação e configuração de todos os softwares e componentes adquiridos, incluindo softwares necessários para o total funcionamento e gerenciamento da solução que não foram listados, como por exemplo, mas não se limitando a, os seguintes serviços:      1. Levantamento do ambiente e preparação para instalação nova da solução VMware NSX;      2. Design da solução;      3. Instalação da solução;      4. Instalação e configuração das Manager controllers;      5. Instalação e configuração dos Edge Appliances;      6. Configuração de Compute Managers;      7. Configuração das transport zones;      8. Configuração dos profiles (hosts, edge e network);      9. Configuração dos Segments;      10. Configuração de IP Pools;      11. Configuração dos Transport Nodes;      12. Configuração de roteamento T0 e/ou T1;      13. Configuração integração do Distribuited Firewall;      14. Configuração e integração entre os dois datacenters da UDESC através dos respectivos vCenters Servers, considerando as arquiteturas similares entre eles;      15. Configuração do balanceador de cargas para as camadas de rede L4 -L7 com off-load SSL, verificação de integridade, regras de aplicação com programabilidade e manipulação de tráfego via interface ou API      16. Testes;      17. Liberar para uso;   6. A equipe técnica que executará os serviços de instalação e configuração deverá sempre conter pelo menos um técnico, presente em todos os momentos da execução do serviço, treinado e capacitado nos produtos, serviços e tecnologias objetos do LOTE 01, que deverá possuir, no mínimo, as seguintes qualificações:      1. Certificado oficial, de nível profissional com comprovação da capacidade de implementação da solução ofertada, VMWARE NSX, emitido pelo fabricante em nome deste profissional nos produtos, serviços e tecnologia objetos desta contratação;   7. A CONTRATADA deverá apresentar atestado de capacidade técnica, emitido por pessoa jurídica de direito público ou privado, que comprove que a CONTRATADA tem experiência profissional, em projetos de implantação de VMWARE NSX (capacidade técnica);   8. Documentação      1. Ao término da implementação da solução, a Contratada deverá fornecer toda a documentação técnica dos softwares instalados, incluindo, mas não se limitando, a:         1. Documentação descritiva dos produtos, com todos os componentes e softwares que perfazem a solução;         2. Documentação técnica do ambiente contendo um report detalhado contendo a topologia, configurações realizadas, serviços ativados e escolhas técnicas realizadas durante o projeto com o embasamento e justificativas;   9. Endereço na Internet do fabricante, onde seja possível obtenção de literatura técnica e drivers atualizados; |

**LOTE 02 - ITEM 04 - Red Hat OpenShift Container Platform Premium**

|  |
| --- |
| ESPECIFICAÇÃO TÉCNICA: Licença perpétua de software - Red Hat OpenShift Container Platform Premium (2 Cores or 4 vCPUs) - MCT2735F5  Características mínimas:   * 1. Licença perpétua para 02 cores ou 4 vCPUs, independentemente da quantidade de servidores virtuais, containers ou aplicações instalados ou gerenciados;   2. Todas as especificações deverão ser atendidas, exclusivamente, por um único fabricante de software. Não serão admitidas propostas que incluam composição de softwares de fabricantes diversos ou variações semelhantes;   3. Serviço de subscrição e garantia de 60 meses;   4. A garantia e serviço de subscrição deve englobar a manutenção corretiva de todos os componentes de software fornecidos, incluindo upgrades, updates ou patches de correção; |

**LOTE 02 - ITEM 05 - Red Hat OpenShift Container Platform with Runtimes Premium**

|  |
| --- |
| ESPECIFICAÇÃO TÉCNICA: Licença perpétua de software - Red Hat Runtimes Premium (2 Cores or 4 vCPUs) - MW00277F5  Características mínimas:   * 1. Licença perpétua para 02 cores ou 4 vCPUs, independentemente da quantidade de servidores virtuais, containers ou aplicações instalados ou gerenciados;   2. Todas as especificações deverão ser atendidas, exclusivamente, por um único fabricante de software. Não serão admitidas propostas que incluam composição de softwares de fabricantes diversos ou variações semelhantes;   3. Serviço de subscrição e garantia de 60 meses;   4. A garantia e serviço de subscrição deve englobar a manutenção corretiva de todos os componentes de software fornecidos, incluindo upgrades, updates ou patches de correção; |

**LOTE 02 - ITEM 06 - Red Hat OpenShift Data Foundation Essentials Premium**

|  |
| --- |
| ESPECIFICAÇÃO TÉCNICA: Licença perpétua de software - Red Hat OpenShift Data Foundation Essentials Premium (2 Cores) - MCT4039F5  Características mínimas:   * 1. Licença perpétua para 02 cores ou 4 vCPUs, independentemente da quantidade de servidores virtuais, containers ou aplicações instalados ou gerenciados;   2. Todas as especificações deverão ser atendidas, exclusivamente, por um único fabricante de software. Não serão admitidas propostas que incluam composição de softwares de fabricantes diversos ou variações semelhantes;   3. Serviço de subscrição e garantia de 60 meses;   4. A garantia e serviço de subscrição deve englobar a manutenção corretiva de todos os componentes de software fornecidos, incluindo upgrades, updates ou patches de correção; |

**LOTE 02 - ITEM 07 - Serviços técnicos especializados em plataforma Red Hat**

|  |
| --- |
| ESPECIFICAÇÃO TÉCNICA – Serviços técnicos especializados em plataforma Red Hat - GPS-C. POR HORA  Características mínimas   * 1. Os serviços listados deverão ser realizados diretamente pelo fabricante da solução;   2. Em até 5 (cinco) dias corridos após a assinatura do contrato, a contratada deverá agendar reunião com representante da Secretaria de Tecnologia da Informação e Comunicação – SETIC - da UDESC e combinar cronograma de instalação e configuração da solução;   3. Deverá ser entregue um cronograma à SETIC em até 5 (cinco) dias corridos após a realização da reunião;   4. O início das atividades deve ocorrer após a aprovação e agendamento do cronograma pela SETIC, e estas deverão ser concluídas no prazo máximo de 45 (quarenta e cinco) dias corridos;   5. Todos as configurações deverão ser realizadas seguindo-se obrigatoriamente documento de padronização de nomenclaturas e endereços que será fornecido pela UDESC em momento oportuno antes da instalação;   6. Os serviços de instalação compreendem a instalação e configuração de todos os softwares e componentes adquiridos, incluindo softwares necessários para o total funcionamento e gerenciamento da solução que não foram listados, como por exemplo, mas não se limitando a, os seguintes serviços:      1. Instalação e configuração dos servidores;      2. Instalação e configuração da ferramenta de gerência e monitoramento do ambiente e integração desta ao Active Directory da UDESC (idUDESC);      3. Instalação, configuração e validação da ferramenta de provisionamento de containers;      4. Instalação, configuração e validação da ferramenta de orquestração de containers;      5. Criação, configuração e implantação de uma rotina de deploy de uma aplicação JAVA integrada à um repositório GIT que será fornecido pela UDESC;      6. Criação, configuração e implantação de uma rotina de deploy de uma aplicação PHP integrada à um repositório GIT que será fornecido pela UDESC;   7. A equipe técnica que executará os serviços de instalação e configuração deverá sempre conter pelo menos um técnico, presente em todos os momentos da execução do serviço, treinado e capacitado nos produtos, serviços e tecnologias objetos do LOTE 02, que deverá possuir, no mínimo, as seguintes qualificações:      1. Certificado oficial, de nível profissional com comprovação da capacidade de implementação da solução ofertada, emitido pelo fabricante em nome deste profissional nos produtos, serviços e tecnologia objetos desta contratação;   8. A CONTRATADA deverá apresentar atestado de capacidade técnica, emitido por pessoa jurídica de direito público ou privado, que comprove que a CONTRATADA tem experiência profissional, em projetos de implantação de RedHat OpenShift (capacidade técnica);   9. Documentação      1. Ao término da implementação da solução, a Contratada deverá fornecer toda a documentação técnica dos softwares instalados, incluindo, mas não se limitando, a:         1. Documentação descritiva dos produtos, com todos os componentes e softwares que perfazem a solução;         2. Documentação técnica do ambiente;         3. Endereço na Internet do fabricante, onde seja possível obtenção de literatura técnica e drivers atualizados; |

**LOTE 02 - ITEM 08 - Treinamento - Red Hat Container Adoption Boot Camp for Administrators Classroom Training - DO700**

|  |
| --- |
| ESPECIFICAÇÃO TÉCNICA - Treinamento técnico oficial do fabricante - Red Hat Container Adoption Boot Camp for Administrators Classroom Training - DO700.  Características mínimas:   * 1. Deverá ser ministrado por instrutor, online, estando disponível durante todo período do treinamento.   2. Não serão aceitos treinamentos gravados.   3. Deverá contemplar todos os itens descritos na ementa disponível em: https://www.redhat.com/pt-br/services/training/do700-container-adoption-boot-camp;   4. Deverá ser ministrado por empresa provedora de treinamento oficial autorizada pelo respectivo fabricante;   5. Deverão ser emitidos certificados de conclusão dos treinamentos para todos os participantes e enviados para o Fiscal do Contrato. O prazo para emissão e envio dos certificados aos alunos é de 30 (trinta) dias corridos após o término de cada curso;   6. Após a realização de cada treinamento e entrega dos certificados, será emitido um Termo de Aceite do Treinamento. |

**LOTE 03 - ITEM 09 - Treinamento - VMware vSphere: Optimize and Scale [V7]**

|  |
| --- |
| ESPECIFICAÇÃO TÉCNICA - Treinamento técnico oficial do fabricante - VMware vSphere: Optimize and Scale [V7].  Características mínimas:   * 1. Deverá ser ministrado por instrutor, online, estando disponível durante todo período do treinamento.   2. Não serão aceitos treinamentos gravados.   3. Deverá contemplar todos os itens descritos na ementa disponível em: https://mylearn.vmware.com/mgrReg/courses.cfm?ui=www\_edu&a=one&id\_subject=93065;   4. Deverá ser ministrado por empresa provedora de treinamento oficial autorizada pelo respectivo fabricante;   5. Deverão ser emitidos certificados de conclusão dos treinamentos para todos os participantes e enviados para o Fiscal do Contrato. O prazo para emissão e envio dos certificados aos alunos é de 30 (trinta) dias corridos após o término de cada curso;   6. Após a realização de cada treinamento e entrega dos certificados, será emitido um Termo de Aceite do Treinamento. |

**LOTE 03 - ITEM 10 - Treinamento - VMware vSphere: Troubleshooting [V7]**

|  |
| --- |
| ESPECIFICAÇÃO TÉCNICA - Treinamento técnico oficial do fabricante - VMware vSphere: Troubleshooting [V7].  Características mínimas:   * 1. Deverá ser ministrado por instrutor, online, estando disponível durante todo período do treinamento.   2. Não serão aceitos treinamentos gravados.   3. Deverá contemplar todos os itens descritos na ementa disponível em: https://mylearn.vmware.com/mgrReg/courses.cfm?ui=www\_edu&a=one&id\_subject=93070;   4. Deverá ser ministrado por empresa provedora de treinamento oficial autorizada pelo respectivo fabricante;   5. Deverão ser emitidos certificados de conclusão dos treinamentos para todos os participantes e enviados para o Fiscal do Contrato. O prazo para emissão e envio dos certificados aos alunos é de 30 (trinta) dias corridos após o término de cada curso;   6. Após a realização de cada treinamento e entrega dos certificados, será emitido um Termo de Aceite do Treinamento. |

**LOTE 03 - ITEM 11 - Treinamento - VMware NSX-T Data Center: Troubleshooting and Operations [V3.2]**

|  |
| --- |
| ESPECIFICAÇÃO TÉCNICA - Treinamento técnico oficial do fabricante - VMware NSX: Troubleshooting and Operations [V6.4].  Características mínimas:   * 1. Deverá ser ministrado por instrutor, online, estando disponível durante todo período do treinamento.   2. Não serão aceitos treinamentos gravados.   3. Deverá contemplar todos os itens descritos na ementa disponível em: https://mylearn.vmware.com/mgrReg/courses.cfm?ui=www\_edu&a=one&id\_subject=98675;   4. Deverá ser ministrado por empresa provedora de treinamento oficial autorizada pelo respectivo fabricante;   5. Deverão ser emitidos certificados de conclusão dos treinamentos para todos os participantes e enviados para o Fiscal do Contrato. O prazo para emissão e envio dos certificados aos alunos é de 30 (trinta) dias corridos após o término de cada curso;   6. Após a realização de cada treinamento e entrega dos certificados, será emitido um Termo de Aceite do Treinamento. |

**LOTE 03 - ITEM 12 - Treinamento - VMware NSX-T Data Center: Install, Configure, Manage [V3.2]**

|  |
| --- |
| ESPECIFICAÇÃO TÉCNICA - Treinamento técnico oficial do fabricante - VMware NSX: Install, Configure, Manage [V6.4].  Características mínimas:   * 1. Deverá ser ministrado por instrutor, online, estando disponível durante todo período do treinamento.   2. Não serão aceitos treinamentos gravados.   3. Deverá contemplar todos os itens descritos na ementa disponível em: https://mylearn.vmware.com/mgrReg/courses.cfm?ui=www\_edu&a=one&id\_subject=97477;   4. Deverá ser ministrado por empresa provedora de treinamento oficial autorizada pelo respectivo fabricante;   5. Deverão ser emitidos certificados de conclusão dos treinamentos para todos os participantes e enviados para o Fiscal do Contrato. O prazo para emissão e envio dos certificados aos alunos é de 30 (trinta) dias corridos após o término de cada curso;   6. Após a realização de cada treinamento e entrega dos certificados, será emitido um Termo de Aceite do Treinamento. |

**LOTE 04 - ITEM 13 - Treinamento - Administração da infraestrutura do núcleo híbrido do Windows Server (AZ-800)**

|  |
| --- |
| ESPECIFICAÇÃO TÉCNICA - Treinamento técnico oficial do fabricante - Administração da infraestrutura do núcleo híbrido do Windows Server (AZ-800)  Características mínimas:   * 1. Deverá ser ministrado por instrutor, presencial ou online, estando disponível durante todo período do treinamento.   2. Não serão aceitos treinamentos gravados.   3. Deverá contemplar todos os itens descritos na ementa disponível em: https://docs.microsoft.com/en-us/training/courses/az-800t00;   4. Deverá ser ministrado por empresa provedora de treinamento oficial autorizada pelo respectivo fabricante;   5. Deverão ser emitidos certificados de conclusão dos treinamentos para todos os participantes e enviados para o Fiscal do Contrato. O prazo para emissão e envio dos certificados aos alunos é de 30 (trinta) dias corridos após o término de cada curso;   6. Após a realização de cada treinamento e entrega dos certificados, será emitido um Termo de Aceite do Treinamento. |

**LOTE 04 - ITEM 14 - Treinamento - Configurar serviços avançados híbridos do Windows Server (AZ-801)**

|  |
| --- |
| ESPECIFICAÇÃO TÉCNICA - Treinamento técnico oficial do fabricante - Configurar serviços avançados híbridos do Windows Server (AZ-801)  Características mínimas:   * 1. Deverá ser ministrado por instrutor, presencial ou online, estando disponível durante todo período do treinamento.   2. Não serão aceitos treinamentos gravados.   3. Deverá contemplar todos os itens descritos na ementa disponível em: https://docs.microsoft.com/en-us/training/courses/az-800t01;   4. Deverá ser ministrado por empresa provedora de treinamento oficial autorizada pelo respectivo fabricante;   5. Deverão ser emitidos certificados de conclusão dos treinamentos para todos os participantes e enviados para o Fiscal do Contrato. O prazo para emissão e envio dos certificados aos alunos é de 30 (trinta) dias corridos após o término de cada curso;   6. Após a realização de cada treinamento e entrega dos certificados, será emitido um Termo de Aceite do Treinamento. |

**LOTE 05 - ITEM 15 – Appliance para armazenamento de backup**

|  |
| --- |
| ESPECIFICAÇÃO TÉCNICA: Appliance para armazenamento de backup  Características mínimas:   1. Descrição do Sistema    1. Deverá ser composto por um conjunto de nós provisionados em uma estrutura de controladora(s) (ou "appliances") e de gavetas de discos, integrados de forma a atender ao conjunto de requisitos técnicos exigidos nessa especificação em sua integralidade    2. Deverá possuir serviço de suporte e garantia de 60 meses;    3. Deverá permitir o monitoramento pró-ativo e reativo por meio de conexão baseada na rede mundial de computadores a uma central de assistência técnica do fabricante ou de um representante autorizado, que opere em regime de 24 (vinte e quatro) horas por dia, 7 (sete) dias por semana. O referido monitoramento deverá permitir a abertura automática de chamados de suporte para reposição de componentes defeituosos ou de componentes que apresentem indícios de falha iminente    4. Será de responsabilidade da contratada o fornecimento de todos os componentes de software e de hardware necessários ao pleno funcionamento do sistema. Caberá à contratada o fornecimento de todas as licenças de "software" necessárias para fins de provimento das funcionalidades exigidas nessa especificação    5. Deverá possuir sistema operacional desenvolvido pelo fabricante do hardware do equipamento (ou sistema computacional dedicado/embarcado), com propósito específico de operacionalizar todos os componentes de software e de hardware do sistema ofertado. De tal forma que caberá à contratada o fornecimento de "hardware" com arquitetura dedicada (ou "sistema embarcado"), em forma de "appliance", e o sistema operacional deverá estar embutido no "hardware" proposto, ou seja, "hardware" e "software" devem ser integrados em um único equipamento    6. Deverá ser fornecido na forma de conjuntos de componentes que deverão ser instalados no datacenter primário do contratante, devendo permitir a interconexão entre estes, possibilitando que estes operem de forma integrada e provendo funcionalidades advindas desta integração    7. Quando do uso de mais de uma controladora em forma de “cluster”, deverá prover a propriedade de redundância no contexto de todos os componentes físicos ("hardware") que sejam fundamentais para seu pleno funcionamento    8. Quando do uso de mais de uma controladora em forma de “cluster”, deverá assegurar o acionamento automático do mecanismo de redundância ("failover" automático) sem necessidade de intervenção humana, de forma que não haja um ponto único de falha que possa ocasionar a indisponibilidade de todos os componentes do sistema em caso de falha de um dado componente físico    9. Quando do uso de mais de uma controladora em forma de “cluster”, deverá assegurar a disponibilidade das informações armazenadas durante atividades de manutenção técnica, sem que faça necessária a parada de todos os componentes do sistema ou a interrupção no acesso às informações armazenadas no equipamento    10. Quando do uso de mais de uma controladora em forma de “cluster”, deverá permitir a atualização do software e do microcódigo (firmware) dos componentes de forma não disruptiva, sem que se faça necessária a parada total do sistema, via emprego de mecanismo de atualização e de reinicialização (reboot) escalonado de cada controladora    11. Deverá possuir funcionalidade de monitoramento pró-ativo que permita a detecção, o isolamento e o registro de falhas sem que faça necessária intervenção manual    12. Caberá à contratada o fornecimento dos dispositivos necessários à implementação dos mecanismos de monitoramento e abertura automática de chamados    13. A contratada deverá incluir todos os softwares necessários para viabilizar a execução do suporte remoto nos computadores dedicados a tal atividade, incluindo o sistema operacional    14. A contratada deverá detalhar no documento que descreve o projeto de implantação do sistema ofertado quais são os protocolos, portas de rede e endereços IP necessários para a comunicação na rede mundial de computadores, com as devidas justificativas técnicas para fins e análise da equipe técnica do contratante    15. Caso o suporte remoto seja feito por um computador externo ao equipamento, esse computador deverá se fixar em um rack de 19 polegadas padrão    16. Deverá permitir sua configuração básica e avançada por meio de conexão de rede Ethernet LAN para acesso à interface de configuração e administração do sistema    17. Deverá disponibilizar interface gráfica web (GUI - Graphical User Interface) para viabilizar seu gerenciamento centralizado    18. Todas as licenças de "software" deverão ser ofertadas na modalidade de licenciamento perpétuo, ou seja, não poderão ser cobrados quaisquer valores adicionais pelo uso das funcionalidades implementadas em "software" durante e após o término do contrato de suporte e manutenção do sistema    19. A solução ofertada deverá se integrar nativamente ao software de backup Commvault , devendo esta compatibilidade ser comprovada através de matriz de compatibilidade do fabricante    20. A solução ofertada e seus componentes (hardware e softwares) deverão ser novos, sem utilização anterior e em linha de fabricação na data da entrega. Esta comprovação deve fazer parte da proposta apresentada pela contratada para análise da equipe técnica da CONTRATANTE    21. Não serão aceitos equipamentos usados, remanufaturados ou de demonstração    22. A solução ofertada deverá suportar e estar completamente licenciada para realização de backups utilizando aceleradores fornecidos pelo fabricante do appliance e que operem de forma integrada com a solução de software proposta 2. Arquitetura    1. Deverá suportar expansões em sua arquitetura pelo acréscimo de novos componentes de hardware e de software    2. Deverá possuir componentes redundantes em sua arquitetura, tais como fonte de alimentação, de forma a se obter alta disponibilidade, facilidade de manutenção, modularidade, conectividade e capacidade de expansão da plataforma    3. Deverá viabilizar expansões futuras da sua capacidade de armazenamento por meio da instalação de novos componentes de "hardware" e por meio da ativação de novas licenças de "software"    4. Deverá ser implementado em "hardware" específico, via emprego de equipamento do tipo "appliance", dedicado exclusivamente a esta função visando prover suas funcionalidades    5. Deverá prover conectividade de forma concorrente e distribuída a todos os clientes do serviço de cópia e de restauração dos dados    6. A rede de "front-end" Ethernet LAN deverá prover velocidade mínima de 10 (dez) Gbps em regime de balanceamento de carga e de alta disponibilidade    7. A rede de "back-end" SAS deverá prover velocidade mínima de 6 (seis) Gbps em regime de alta disponibilidade    8. Deverá implementar o nível de proteção RAID 6 ou equivalente, permitindo a falha de no máximo 2 (dois) discos do mesmo grupo sem perda de dados    9. Em caso de falha de até 2 (dois) discos de um dado grupo RAID 6, a disponibilidade do sistema não deverá ser afetada, não podendo haver períodos de indisponibilidades devido a recuperações lógicas ou movimentações de dados (reordenamento) entre os discos    10. Deverá permitir a definição de VLANs 12 conforme padrão IEEE 802.1q ("Frame Tagging") e a criação de pelo menos 16 (dezesseis) interfaces lógicas associadas às respectivas VLANs    11. Deverá permitir a transmissão e a recepção de quadros que possuam o tamanho mínimo de 9.000 bytes (ou técnica de "jumbo frames") nas respectivas portas Ethernet LAN    12. Deverá implementar técnicas de agregação de tráfego na camada de rede Ethernet LAN por meio do emprego de pelo menos uma das seguintes técnicas: o padrão IEEE 802.3ad (LACP 13) ou via mecanismo de "port trunking" 14    13. Deverá implementar nativamente o protocolo IP ("Internet Protocol") v4    14. Deverá possibilitar a criação de rotas estáticas unicast IP v4 3. Capacidade    1. Deverá possuir a capacidade líquida de armazenamento local de pelo menos **100 (cem) TB**, descontadas todas as perdas com redundâncias, paridades, spares de proteção do arranjo de discos, desduplicação de dados e qualquer outro mecanismo de redução de dados. A volumetria é informada em base 10, onde 1 TB (um Terabyte) é igual a 1.000 GB (mil Gigabytes).    2. Complementarmente, não poderão ser considerados quaisquer ganhos de capacidade oriundos de desduplicação, compressão de dados ou outros algoritmos similares    3. A licença não deverá possuir limitações quanto à quantidade de dados armazenados    4. Deverá suportar o aumento da área de armazenamento local em pelo menos 250 (duzentos e cinquenta) TB líquidos    5. Deverá atingir sua capacidade máxima de expansão pela simples adição de discos e/ou gavetas de discos    6. Deverá implementar pelo menos 14 TB/hora de throughput sustentado nas interfaces de "front-end" do equipamento, desconsiderando qualquer taxa de desduplicação    7. Deverá implementar pelo menos 250 (duzentos e cinquenta) fluxos (sessões) de backups simultâneos 4. Controladoras    1. Deverão ser compatíveis com o sistema a ser fornecido    2. A controladora deverá empregar processadores com múltiplos núcleos (ou cores) visando o aumento de desempenho do sistema    3. No caso do fornecimento de múltiplas controladores, no funcionamento em modalidade ativo/passivo:       1. As controladoras deverão operar em modo ativo/passivo, com "failover" automático da controladora ativa (primária/"hot") para a controladora passiva (secundária/"standby") em caso de falha da controladora ativa       2. As controladoras deverão implementar mecanismo de "failover", sendo que no caso de ocorrência de falha da controladora primária, a controladora secundária deverá ser capaz de manter acessíveis todos os volumes de dados disponibilizados pelo sistema       3. As controladoras deverão ser conectadas entre si por meio de conexões dedicadas (ou rede exclusiva e dedicada para este fim). Todos os componentes necessários para essa conexão deverão estar inclusos e não será permitido o compartilhamento de recursos da rede de armazenamento de dados (Fibre Channel SAN) ou da rede de dados (Ethernet LAN) para tal finalidade       4. O sistema de armazenamento deverá possibilitar a substituição das controladoras de forma alternada em caso de falha       5. Deverá garantir que apenas um conjunto de licenças necessite ser empregado pela controladora primária do "cluster" independentemente do número de controladoras secundárias. De tal forma que no decorrer do chaveamento entre suas controladoras ("failover") o sistema permita que as licenças em uso na controladora primária sejam transferidas para a controladora secundária, e vice-versa quando o funcionamento da controladora primária for restabelecido. Deverá ser capaz de proporcionar o chaveamento dos serviços e dos endereços IP (endereço lógico) da controladora primária do "cluster" para a controladora secundária caso a controladora primária apresente defeito que resulte em sua indisponibilidade       6. Deverá assegurar a disponibilidade e a proteção dos dados no decorrer da execução de atividades de manutenção técnica, tais como substituição de componentes, "upgrade" de capacidade e alteração de características funcionais. Deverá permitir a substituição ou o acréscimo de discos nas gavetas de expansão e de controladoras ao "cluster" sem a necessidade de parada do sistema    4. A(s) controladora(s) deverá possuir no mínimo 2 (duas) conexões redundantes ao barramento de "back-end" SAS do sistema 5. Memória Cache    1. Deverá possuir no mínimo 192 (cento e noventa e dois) GB de memória instalada por controladora, não sendo aceita memória baseada em tecnologia flash ou SSD para tal finalidade    2. O mecanismo de memória cache de escrita deverá prover recurso nativo que garanta a integridade dos blocos de dados armazenados em sua área de endereçamento    3. Caso possua mais de uma controladora, deverá possuir mecanismo de proteção que garanta a integridade dos dados armazenados na memória cache de escrita, mitigando o risco de perda de dados em caso de falha no alimentador do sistema de distribuição de energia elétrica, seja por meio da utilização de baterias ou por meio da transferência dos dados para armazenamento persistente/não volátil ("cache destaging")    4. Deverá prover mecanismo de tolerância a falhas da memória cache de escrita implementado por meio de memória com suporte a códigos de correção de erro (ECC - "Error Correction Code")    5. Caso possua mais de uma controladora, deverá implementar mecanismo de espelhamento de escrita da memória cache ("Mirrored-Write-Cache"), para assegurar a proteção do conteúdo de escrita entre suas controladoras, de forma que, na ocorrência de falha em uma delas, a outra possa dar continuidade as tarefas que estavam sendo executadas sem interrupção do sistema ou perda de dados. Alternativamente, deverá implementar mecanismo que assegure que seja reiniciado o job disparado pelo software de backup visando a continuidade da operação de ingestão de imagem de backup no sistema 6. Interfaces de Conectividade de Front-End    1. Deverá prover acesso dos hosts autorizados a executar operações de leitura e de escrita em seus volumes de dados por meio de interfaces de "front-end" do tipo Ethernet LAN    2. Deverá ser fornecido com no mínimo 4 (quatro) interfaces 10Gbps, de acordo com o padrão IEEE 802.3ae, com conectores SFP+. deverão ser fornecidos transcievers e cordões de fibra ótica com conectores LC-LC para todas as interfaces disponíveis. Os transcievers deverão ser do tipo SR. O cordão de fibra ótica deverá possuir o comprimento mínimo de 10 metros.    3. Caberá à contratada o fornecimento de todos os conectores, cabos, e demais componentes que se façam necessários para o perfeito funcionamento das interfaces Ethernet LAN de cada controladora 7. Interfaces de Conectividade de Back-End    1. Deverá implementar mecanismo que assegure que os discos conectados ao barramento de "back-end" sejam acessados pela(s) controladora(s) do sistema de forma redundante    2. Deverá implementar caminhos de acesso redundantes aos discos contidos no barramento de "back-end"    3. Cada gaveta de discos deverá possuir pelo menos 2 (dois) conectores a fim de estar conectada simultaneamente a pelo menos 2 (duas) controladoras distintas, quando for utilizada mais de uma controladora    4. O quantitativo total de discos a ser fornecido pela proponente deverá estar distribuído homogeneamente entre os diversos canais de comunicação do equipamento    5. A comunicação entre a(s) controladora(s) e os discos deverá empregar interface SAS com velocidade de no mínimo 6 (seis) Gbps por canal de comunicação 8. Funcionalidades    1. Caberá à contratada o fornecimento de toda e qualquer licença de software necessária à implementação integral do conjunto de funcionalidades a seguir enumerado para a capacidade total de armazenamento líquida a ser fornecida    2. Deverá implementar algoritmos de desduplicação, permitindo eliminar segmentos redundantes e compactar os dados, de forma a reduzir a área de disco destinada ao armazenamento dos dados de backup    3. O mecanismo de desduplicação deverá ser nativo da solução, sem utilização de software externo instalado nos servidores ou clientes de backups    4. O mecanismo de desduplicação de dados deverá ser executado em tempo real (em linha ou "in line") dos dados recebidos para gravação em disco, ou seja, durante a ingestão (ou gravação) dos dados e replicação ocorrendo durante a cópia, de forma simultânea. Não serão aceitas soluções que realizem a desduplicação após a gravação do dado no disco (pós-processo) ou mesmo híbridas que realizem parte do processo antes e parte após a gravação do dado no disco    5. Deverá efetuar desduplicação global, ou seja, um único pool de desduplicação por sistema, desduplicando assim de forma global todos os dados oriundos de qualquer protocolo (CIFS, NFS, OST), cliente e/ou aplicação    6. Caso não suporte desduplicação global entre todos os shares e protocolos, deverá ser acrescida área adicional de 50% da área útil total solicitada, devendo ser entregue um equipamento com capacidade líquida de no mínimo 150TB, tendo em vista a menor eficiência no processo de redução de dados    7. A solução deve fazer uso de recursos dedicados para realizar a compressão dos dados via hardware antes ou após a desduplicação dos dados, de forma que este processo de compressão não deve impactar o desempenho do equipamento    8. Suportar criptografia do tipo DARE (Data At Rest Encryption) de no mínimo 256 bits com certificação FIPS 140-2    9. Os blocos de dados deverão ser criptografados quando ocorrer a execução de uma operação de escrita em disco enquanto que deverão ser descriptografados quando ocorrer a execução de uma operação de leitura em disco    10. Os blocos de dados deverão ser criptografados na(s) controladora(s) de origem e descriptografados na(s) controladora(s) de destino quando ocorrer sua replicação entre um dado sistema origem e um dado sistema destino    11. Deverá suportar mecanismo de apagamento seguro das imagens de backup armazenadas em seus volumes de dados, ou seja, os blocos de dados deverão ser efetivamente apagados por meio da gravação de 0s e 1s ou algum padrão aleatório com base em alguma função randômica após a deleção dos respectivos volumes de dados    12. O mecanismo de replicação deverá ser nativo da solução, sem necessidade de utilização de recursos externos    13. O mecanismo de replicação deverá permitir a adoção de uma topologia de replicação de pelo menos do tipo um-para-um, a qual consiste em uma ou mais controladora de origem e uma ou mais controladora de destino    14. O mecanismo de replicação deverá permitir o emprego de algoritmos de compressão, desduplicação e criptografia no tráfego trocado entre o "cluster" de controladoras de origem e o "cluster" de controladoras de destino    15. O mecanismo de replicação deverá empregar a pilha de protocolos TCP/IP para viabilizar a replicação dos blocos entre a(s) controladora(s) de origem e a(s) controladora(s) de destino    16. 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    17. REMOVER 9. Proteção contra Ransomware    1. O equipamento deve suportar enviar de forma desduplicada e criptografada os dados de backup para um armazenamento de objeto (S3), em nuvem pública ou privada. O licenciamento desta funcionalidade não faz parte deste certame    2. O equipamento deve fazer uso de API ou outros mecanismos de segurança 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    3. Possuir recurso de imutabilidade de dados utilizando WORM (Write Once Read Many) ou recurso similar 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    4. O recurso de imutabilidade WORM (Write Once Read Many) deve possuir proteção (System Clock Hardening Protection) caso o cibercriminoso altere/adiante a data do subsistema para poder alterar/excluir os arquivos protegidos    5. Possuir recurso de dupla autenticação (2FA – Two Factor Authentication) para executar atividades administrativas de exclusão no equipamento 10. Protocolos de Acesso aos Dados     1. Deverá suportar simultaneamente as seguintes formas de acesso para backup: CIFS, NFS e OST     2. Deverá permitir a criação e a deleção de CIFS "Shares"     3. Deverá permitir a integração com o serviço de diretório Microsoft Windows ADS 2019 de tal modo que seja possível a criação de políticas de segurança visando a implementação de listas de controle de acesso ("Access Control Lists - ACL") aos CIFS "Shares" publicados no sistema por meio do emprego das informações armazenadas no serviço de diretório supracitado (usuários e grupos)     4. Deverá permitir o emprego de endereços IP na criação de políticas de segurança visando à implementação de listas de controle de acesso aos NFS "Exports" publicados no sistema. Alternativamente, deverá permitir a criação de políticas de segurança com base nos nomes de hosts ou no respectivo FQDN visando à implementação de listas de controle de acesso aos NFS "Exports" publicados no sistema 11. Gerenciamento do Sistema     1. Deverá ser fornecido com no mínimo 1 (uma) interface Gigabit Ethernet 10/100/1000Base-T, conforme padrão IEEE 802.3ab, com conectores RJ-45 fêmea diretamente no equipamento, a qual será dedicada ao gerenciamento "out-of- band" para fins de operação, administração e atualização de firmware     2. Deverá possuir interface de linha de comando, a qual deverá ser acessada remotamente por meio do emprego do protocolo SSH     3. Deverá disponibilizar interface de administração gráfica centralizada baseada no protocolo HTTP ou no protocolo HTTPS para fins de configuração remota do equipamento via interface web     4. Deverá implementar cliente de atualização de data e hora por meio do emprego de pelo menos um dos protocolos a seguir enumerados: SNTP v3 (RFC 1769), NTP v3 (RFC 1305), SNTP v4 (RFC 2030) ou NTP v4 (RFC 5905)     5. Deverá implementar agente SNMP por meio do emprego de pelo menos um dos protocolos a seguir enumerados: SNMP v1 (RFC 1157), SNMP v2c (RFC 1901), SNMP v2 (RFC 1907) ou SNMP v3 (RFC 2571)     6. Deverá prover MIBs 18 que possam ser compiladas para o sistema de gerenciamento SNMP empregado pelo contratante 19     7. Deverá permitir o envio de SNMP traps para gerentes SNMP     8. Deverá possibilitar o envio de mensagens de notificação de eventos para servidores SYSLOG     9. Deverá possibilitar o envio de mensagens de notificação de eventos para servidores SMTP     10. Deverá possibilitar a criação de usuários, com atribuição a grupos e permissões específicas de acesso as funcionalidades     11. Deverá possibilitar a integração com o serviço de diretório Microsoft Windows "Active Directory System" (ADS) para fins de autenticação de usuários e grupos. Deverá implementar biblioteca baseada em REST API que disponibilize "web services" que viabilizem a administração do sistema via linguagem de script ou de programação     12. Deverá permitir executar as seguintes funções de administração do sistema de armazenamento:         1. Prover dados de medição sobre o consumo corrente de recursos do sistema: Número de requisições: totais, com sucesso e com falha         2. Capacidade em disco: total, usada e disponível         3. Desempenho: taxa de transferência na escrita e taxa de transferência na leitura         4. Replicação: tráfego de leitura e tráfego de escrita         5. Estado do sistema: controladoras, memória, portas de I/O, interfaces de rede, discos, fontes e ventiladores         6. Viabilizar a configuração dos mecanismos de criptografia e replicação         7. Monitorar o status do sistema, com recursos para definição de thresholds e geração de alertas         8. Registrar o histórico de eventos do sistema com possibilidade de análise remota e envio remoto de logs 12. Segurança     1. Deverá possibilitar a criação de usuários e de grupos de usuários (ou perfis/papéis) de usuários, com atribuição de permissões específicas de acesso as funcionalidades que forem necessárias     2. Deverá permitir o uso de listas de controle de acesso para permitir o acesso aos dados armazenados no sistema 13. Características Físicas e Elétricas     1. Cada sistema deverá vir acompanhado de rack de 19" do mesmo fabricante do equipamento, contemplando acomodação de todos os módulos e acessórios que se fizerem necessários ao seu perfeito funcionamento     2. Cada sistema deverá ser instalado em rack 19" a ser fornecido pela contratada, bem como todo o conjunto de ferragens (trilhos laterais, braços/trilhos de gerenciamento de cabos) e cabos originais e necessários ao seu perfeito funcionamento.     3. Cada rack do sistema deverá possuir pelo menos 2 (duas) fontes de energia elétrica (PDUs 24) redundantes e independentes por meio do emprego de alimentadores baseados em modalidade dual, sendo que o equipamento deverá continuar em funcionamento normal caso uma das fontes de alimentação venha a manifestar algum tipo de falha     4. Cada rack do sistema deverá ser fornecido com cabo de conexão ao sistema de aterramento de cada data center do contratante     5. As fontes de alimentação deverão operar com uma tensão monofásica nominal de 220 VCA e com uma frequência nominal de 60 Hz     6. Todos os módulos de potência elétrica de cada componente do sistema deverão empregar apenas as fontes de energia "hot-swap" redundantes para fins de energização     7. Deverá implementar mecanismo de refrigeração a ar por meio do emprego de unidades de ventilação redundantes e "hot-swap"     8. Caberá à contratada o fornecimento de tampas cegas para preenchimento integral dos espaços vazios dos racks do equipamento visando melhorar a eficiência do respectivo sistema de ventilação 14. Implementação     1. O equipamento deverá ser instalado e configurado pela CONTRATADA     2. Todos as configurações deverão ser realizadas seguindo-se obrigatoriamente documento de padronização de nomenclaturas e endereços que será fornecido pela UDESC em momento oportuno antes da instalação;     3. Os serviços de instalação compreendem a instalação e configuração de todos os softwares e componentes adquiridos, incluindo softwares necessários para o total funcionamento e gerenciamento da solução que não foram listados, como por exemplo, mas não se limitando a, os seguintes serviços:     4. Instalação e configuração do hardware;     5. Instalação e configuração da ferramenta de gerência e monitoramento e integração desta ao Active Directory da UDESC (idUDESC);     6. Criação de pools de armazenamento conforme orientações da UDESC;     7. Configuração da rede e VLANs;     8. Integração com a solução de backup hoje existente na UDESC - Commvault;     9. Realização de testes de backup e restore dos seguintes componentes:        1. Máquinas Virtuais        2. Bases de dados SQLServer        3. Filesystems EXT4 e NTFS     10. A equipe técnica que executará os serviços de instalação e configuração deverá sempre conter pelo menos um técnico, presente em todos os momentos da execução do serviço, treinado e capacitado nos produtos, serviços e tecnologias objetos do LOTE 05, que deverá possuir, no mínimo, as seguintes qualificações:     11. Certificado oficial, de nível profissional com comprovação da capacidade de implementação da solução ofertada, emitido pelo fabricante em nome deste profissional nos produtos, serviços e tecnologia objetos desta contratação;     12. O certificado deverá contemplar a instalação, configuração e gerenciamento da solução proposta; 15. Documentação     1. Ao término da implementação da solução, a Contratada deverá fornecer toda a documentação técnica dos softwares instalados, incluindo, mas não se limitando, a:     2. Documentação descritiva dos produtos, com todos os componentes e softwares que perfazem a solução;     3. Documentação técnica do ambiente;     4. Endereço na Internet do fabricante, onde seja possível obtenção de literatura técnica e drivers atualizados; |

**LOTE 05 - ITEM 16 - Treinamento - Appliance para armazenamento de backup**

|  |
| --- |
| ESPECIFICAÇÃO TÉCNICA - Treinamento técnico oficial do fabricante - Appliance para armazenamento de backup ofertado no LOTE 05 - ITEM 15.  Características mínimas:   * 1. Deverá ser ministrado por instrutor, online, estando disponível durante todo período do treinamento.   2. Não serão aceitos treinamentos gravados.   3. Deverá contemplar, no mínimo, as seguintes pautas:      1. Solução em Backup;      2. Monitoramento do sistema;      3. Configurar e gerenciar interfaces de rede;      4. Acessar e copiar dados para o sistema de Backup;      5. Personalizar e gerenciar sistema de arquivos de desduplicação;      6. Descrever e realizar replicação e recuperação de dados;      7. Descrever e configurar a solução de backup;      8. Descrever o planejamento de capacidade e rendimento;      9. Descrever e configurar multilocação segura;   4. Deverá ser ministrado por empresa provedora de treinamento oficial autorizada pelo respectivo fabricante;   5. Deverão ser emitidos certificados de conclusão dos treinamentos para todos os participantes e enviados para o Fiscal do Contrato. O prazo para emissão e envio dos certificados aos alunos é de 30 (trinta) dias corridos após o término de cada curso;   6. Após a realização de cada treinamento e entrega dos certificados, será emitido um Termo de Aceite do Treinamento. |

**LOTE 06 - ITEM 17 - Solução de balanceamento de carga e segurança para aplicações web**

|  |
| --- |
| ESPECIFICAÇÃO TÉCNICA - Solução de balanceamento de carga e segurança para aplicações web  Características mínimas:   1. Características gerais:    1. Deve ser fornecida em hardware com arquitetura dedicada, não podendo ser servidor de uso genérico, e o sistema operacional deve estar embutido no hardware proposto, ou seja, hardware e software devem ser integrados em cada equipamento (appliance);    2. Todas as funcionalidades deverão ser fornecidas pelo mesmo fabricante, de maneira integrada e em uma mesma arquitetura, com atualizações, dentro do período do contrato;    3. Um único appliance deve ser capaz de executar e suportar a totalidade das capacidades exigidas, não sendo aceitos somatórias para atingir os limites mínimos;       1. Não serão aceitos módulos adicionais de hardware para atingir a capacidade exigida;       2. Cada appliance deve possuir quantidade de memória e capacidade de processamento suficiente para atendimento de todas as funcionalidades operando simultaneamente, conforme desempenhos solicitados neste item;       3. Não serão aceitos módulos adicionais de hardware para prover as funcionalidades exigidas;       4. Todas as interfaces fornecidas nos appliances devem estar licenciadas e habilitadas para uso imediato;    4. A solução deverá permitir a instalação em ambientes de alta disponibilidade das seguintes formas:       1. Ativo/Standby, com equipamento da mesma marca e modelo;       2. Ativo/ativo, com equipamento da mesma marca e modelo, mantendo o status das conexões. Entende-se como ativo/ativo a utilização de dois endereços virtuais, onde cada endereço está ativo em um elemento e standby no outro ou a capacidade do mesmo endereço virtual ser respondido de forma controlada pelos dois elementos simultaneamente;    5. A solução deverá implementar, quando em alta disponibilidade, sincronismo de sessão entre os elementos onde a falha do equipamento principal não deverá causar a interrupção das sessões balanceadas;    6. Todos os recursos necessários (hardware, software, licenças, assinaturas, cabos, etc) para implementar alta-disponibilidade devem ser fornecidos sem custo adicional;    7. A solução deve permitir escalabilidade, podendo crescer na forma de cluster adicionando novos appliances inclusive de modelos diferentes;    8. O equipamento ofertado deverá possuir sistema operacional certificado na ICSA Labs podendo assim ser instalado na borda da rede antes de qualquer equipamento de segurança;    9. Deverá fornecer recurso de agregação de portas baseado no protocolo LACP:       1. Deverá possuir suporte a LACP em modo passivo e ativo;       2. Deverá fornecer recurso para suportar até 8 portas em um mesmo conjunto agregado;    10. Deverá possuir suporte a Spanning-Tree(802.1D), Fast Spanning-Tree (802.1w, 802.1t) e Multi Spanning-Tree (802.1s);    11. Deverá fornecer recurso para o transporte de múltiplas VLAN por uma única porta (ou por um conjunto agregado de portas) utilizando o protocolo 802.1q;    12. Deverá oferecer suporte a IPv6;    13. A solução deve suportar múltiplas tabelas de rotas independentes;    14. A solução, quando habilitada para mais de uma função (SLB, GSLB, Aceleração Web, etc), deverá permitir a definição da importância da função, determinando quanta CPU e memória será alocada para cada tipo de funcionalidade;        1. Deverá possuir capacidade para gerenciar os recursos disponíveis de acordo com as funções habilitadas;    15. A solução deve permitir múltiplos domínios de roteamento em IPv4 e IPv6;    16. Deverá suportar à funcionalidade de VXLAN, para integração com o ambiente de virtualização de redes (Software Defined Network);    17. Cada appliance deve possuir, no mínimo, as seguintes especificações de desempenho;        1. Possuir capacidade para tratar 350.000 (trezentas e cinquenta mil) requisições por segundo em camada 7;        2. Possuir capacidade para tratar 125.000 (cento e vinte e cinco mil) conexões por segundo em camada 4;        3. Possuir capacidade para sustentar pelo menos 14.000.000 (catorze milhões) de conexões simultâneas em camada 4;        4. Possuir capacidade mínima de throughput em camada 4 de 10 (dez) Gbps;        5. Ser capaz de tratar, pelo menos, 2.100 (duas mil e cem) transações SSL/TLS por segundo (TPS) considerando Elliptic Curve Digital Signature Algorithm (ECDSA) P-256;        6. Ser capaz de tratar, pelo menos, 2.500 (duas mil e quinhentas) transações SSL/TLS por segundo (TPS) considerando Rivest-Shamir-Adleman (RSA) com chaves de 2048 bits;        7. Possuir capacidade de criptografar com throughput mínimo de 5 (cinco) Gbps;    18. Cada appliance deverá possuir, no mínimo, 4 (quatro) interfaces de 1 Gigabit Ethernet SFP e 2 (duas) interfaces de 10G SFP+;        1. Todas as interfaces já devem ser fornecidas com os respectivos transcievers SR e com cordões de fibra ótica LC-LC;    19. Cada appliance deverá possuir fontes de alimentação redundantes 100-240V com seleção automática de tensão; 2. Gerenciamento:    1. Deverá ser possível realizar a configuração de endereçamento IP estático ou dinâmico (DHCP/BOOTP) para o gerenciamento;    2. Deve suportar o protocolo SNTP (Simple Network Time Protocol) ou NTP (Network Time Protocol) para a sincronização do relógio com outros dispositivos de rede, garantindo a alta efetividade e segurança na troca de mensagens com os servidores de tempo;    3. Deve permitir administração remota através de SSH;    4. Deverá permitir manter internamente múltiplos arquivos de configurações do sistema;    5. Deverá suportar transferência de arquivos de configuração e Sistema Operacional utilizando SCP ou HTTPS;    6. Permitir acesso por Interface de linha de comando (CLI – Command Line Interface) que possibilite a configuração dos equipamentos com acesso via porta de console e SSH com as seguintes facilidades:       1. Possuir função de auto completar de comandos na CLI;       2. Possuir ajuda contextual dos comandos na CLI;       3. Possuir comando para visualizar o tráfego de utilização das interfaces em bits/segundo (bps) e pacotes/segundo (pps);       4. Reinicialização do equipamento por comando na CLI;       5. Possuir ferramentas para identificação de problemas (debugging) através da CLI;    7. Permitir a criação de no mínimo, três níveis de usuários na GUI – administrador, usuário com permissões reduzidas e usuário somente leitura;    8. Deverá permitir a autenticação dos usuários de gerência em bases remotas e suportar no mínimo RADIUS, LDAP e TACACS+;    9. Deverá permitir a autenticação dos usuários em bases Microsoft Active Directory;    10. Possuir interface de gerência gráfica web com acesso seguro utilizando HTTP sobre TLS;    11. Deverá ser possível realizar a atualização do sistema operacional e/ou a instalação de patches ou Hotfixes através da interface Gráfica sem o uso da linha de comando;    12. Deverá suportar a restauração de forme simples (rollback) de configuração e sistema operacional;    13. Possuir e fornecer geração de mensagens de syslog para eventos relevantes ao sistema;    14. Possuir a possibilidade de configuração de múltiplos syslog servers para os quais o equipamento irá enviar as mensagens de syslog;    15. Possuir armazenamento de mensagens de syslog em dispositivo interno ao equipamento;    16. A interface gráfica deverá permitir a reinicialização do equipamento;    17. Possuir recurso de gerência via SNMP e implementar SNMPv1, SNMPv2c e SNMPV3;    18. Implementar envio de notificações (traps) via SNMP;    19. Possui suporte a monitoração utilizando RMON através de pelo menos 4 grupos: statistics, history, alarms e events    20. Implementar Link Layer Discovery Protocol (LLDP);    21. A Solução deve implementar exportação de informações de fluxo através de Netflow ou sFlow; 3. Características do balanceamento e carga e cache de dados:    1. A solução deverá suportar todas as aplicações comuns de um Switch Layer 7, como:       1. Server Load-Balancing;       2. Firewall Load-Balancing;       3. Proxy Load-Balancing;    2. Deverá permitir balanceamento apenas em direção ao servidor, onde a resposta do servidor real é enviada diretamente ao cliente;    3. A solução deve permitir o encapsulamento, em camada 3, do tráfego entre o balanceador e o servidor para tráfego IPv4 e IPv6, quando o balanceamento é realizado apenas em direção ao servidor, onde a resposta do servidor real é enviada diretamente ao cliente;    4. Permitir a clonagem de fluxos, de forma que a solução envie uma cópia do tráfego para um pool/porta adicional, como por exemplo um pool de IDSs ou sniffers, para fins de análise de tráfego de rede ou mesmo para identificação de padrões de acesso não permitidos ou indicações de atividade maliciosas ou ataques de rede;    5. Possuir recursos para balancear servidores com qualquer hardware, sistema operacional e tipo de aplicação;    6. A solução deve possuir recurso de ativação de grupo prioritário, no qual o administrador pode especificar a quantidade mínima de servidores que devem estar disponíveis em cada grupo e a prioridade dos grupos;    7. Caso o número de servidores disponíveis fique menor do que o estipulado pelo administrador, a solução deve automaticamente distribuir o tráfego para o próximo grupo com maior prioridade não afetando o serviço.    8. Caso o número de servidores disponíveis volte ao valor mínimo estipulado pelo administrador, a solução deve automaticamente retirar o grupo com menor prioridade de balanceamento, voltando ao estado original.    9. Possuir capacidade de abrir um número reduzido de conexões TCP com o servidor e inserir os HTTP requests gerado pelos clientes nestas conexões, reduzindo a necessidade de estabelecimento de conexões nos servidores e aumentando a performance do serviço;    10. Suportar os seguintes métodos de balanceamento:        1. Round Robin;        2. Least Connections;        3. Weighted Percentage (por peso);        4. Servidor ou equipamento com resposta mais rápida baseado no tráfego real;        5. Weighted Percentage dinâmico (baseado no número de conexões);        6. Dinâmico, baseado em parâmetros de um determinado servidor ou equipamento, coletados via SNMP ou WMI;    11. A solução deve permitir aplicar criptografia de cookies para a proteção dos cookies utilizados pela aplicação web;    12. Possuir recursos para balancear as sessões novas, mas preservar sessões existentes no mesmo servidor, implementando persistência de sessão dos seguintes tipos:        1. Por cookie: inserção de um novo cookie na sessão;        2. Por cookie: utilização do valor do cookie da aplicação, sem adição de cookie;        3. Por endereço IP destino;        4. Por endereço IP origem;        5. Por sessão SSL;        6. Através da análise da URL acessada.;        7. Através da análise de qualquer parâmetro no header HTTP;        8. Através da análise do MS Terminal Services Session (MSRDP);        9. Através da análise do SIP Call ID ou Source IP;        10. Através da análise de qualquer informação da porção de dados (camada 7);    13. A solução deve utilizar Cache Array Routing Protocol (CARP) no algoritmo de HASH;    14. O equipamento oferecido deverá suportar os seguintes métodos de monitoramento dos servidores reais:        1. Layer 3 – ICMP;        2. Conexões TCP e UDP pela respectiva porta no servidor;    15. Devem existir monitores predefinidos para, no mínimo, os seguintes protocolos: ICMP, HTTP, HTTPS, FTP, SMB, RADIUS, MSSQL, NNTP, RPC, LDAP, IMAP, SMTP, POP3, SIP, SOAP, SNMP e WMI;    16. Possuir recursos para balanceamento de carga de servidores SIP para VoIP (equipamento SIP PROXY);    17. Possuir recursos para limitar o número de sessões estabelecidas com cada servidor real;    18. Possuir recursos para limitar o número de sessões estabelecidas com cada servidor virtual;    19. Possuir recursos para limitar o número de sessões estabelecidas com cada grupo de servidores;    20. Possuir recursos para limitar o número de sessões estabelecidas com cada servidor físico:        1. Realizar Network Address Translation (NAT);        2. Realizar Proteção contra Denial of Service (DoS);        3. Realizar Proteção contra SYN flood;        4. Realizar Limpeza de cabeçalho HTTP;    21. A solução deve permitir o controle da resposta ICMP por servidor virtual;    22. Possuir recursos para que a configuração seja baseada em perfis, permitindo uma fácil administração;    23. Possuir capacidade de geração e gestão de perfis hierarquizados, permitindo maior facilidade na administração de políticas similares;    24. Permitir a criação de servidores virtuais com endereço IPv4 e os servidores reais com endereços IPv6;    25. Possuir recursos para executar compressão de conteúdo HTTP, para reduzir a quantidade de informações enviadas ao cliente;        1. Permitir definir qual tipo de compressão será habilitada (gzip1 a gzip9, deflate);        2. Possuir capacidade para definir compressão especificamente para certos tipos de objetos;    26. Possuir recursos para fazer aceleração de SSL, onde os certificados digitais são instalados no equipamento e as requisições HTTP são enviadas aos servidores sem criptografia;    27. A solução deverá garantir que na aceleração de SSL, tanto a troca de chaves quanto a criptografia dos dados sejam realizadas com aceleração em hardware, para não onerar o sistema;    28. Deve possuir capacidade de importação dos certificados e chaves criptográficas, para transações seguras entre cliente/servidor, podendo assim operar em modo “man in the middle”, ou seja, descriptografar, otimizar e re-criptografar o tráfego SSL sem comprometer a segurança da conexão SSL estabelecida previamente entre cliente/servidor. Caso haja falha na leitura da conexão SSL, esta deverá, se assim definido, prosseguir em regime de passthrough;    29. A solução deve possuir a funcionalidade de espelhamento de conexões SSL.    30. Possuir recursos para configurar o equipamento para recriptografar em SSL a requisição ao enviar para o servidor, permitindo as demais otimizações em ambiente 100% criptografado;    31. Todas as funcionalidades de inspeção, proteção e aceleração de tráfego criptografado através de SSL/TLS especificadas neste termo de referência devem estar disponíveis quando a conexão segura for estabelecida usando:        1. Autenticação do servidor por parte do cliente, através da verificação da validade do certificado digital fornecido pelo lado servidor durante o processo de estabelecimento do túnel SSL/TLS;        2. Autenticação do cliente por parte do servidor, através da solicitação e verificação da validade do certificado digital fornecido pelo cliente durante o processo de estabelecimento do túnel SSL/TLS;        3. Ambas as autenticações acima mencionadas ocorrendo de forma simultânea;    32. Ao realizar inspeção, proteção, offLoad e aceleração de tráfego criptografado através de SSL/TLS, a solução deverá ser capaz de:        1. Encaminhar ao servidor real via cabeçalho HTTP ou de forma transparente, todo o certificado digital utilizado pelo lado cliente para se autenticar perante o servidor durante o processo de estabelecimento do túnel SSL/TLS;        2. Encaminhar ao servidor real via cabeçalho HTTP campos específicos do certificado digital utilizado pelo cliente para se autenticar perante o servidor durante o processo de estabelecimento do túnel SSL/TLS;    33. A solução deve permitir aplicar criptografia de cookies para a poteção dos cookies utilizados pela aplicação web;    34. Possuir recursos para fazer aceleração de SSL, onde os certificados digitais são instalados no equipamento e as requisições POP3S, IMAPSe SMTPS são enviadas aos servidores sem criptografia;    35. A solução deve possuir diversos recursos relacionados ao uso de criptografia com o objetivo de otimizar e minimizar o impacto na performance das aplicações. Dentre eles deve ser possível configurar parâmetros como:        1. SSL session cache Timeout;        2. Session Ticket;        3. OCSP (Online Certificate Status Protocol) Stapling;        4. Dynamic Record Sizing;        5. ALPN (Application Layer Protocol Negotiation);        6. Perfect Forward Secrecy;    36. Suportar a utilização de memória RAM como cache de objetos HTTP, para responder às requisições dos usuários sem utilizar recursos dos servidores;    37. Possuir capacidade, no uso do recurso de cache, em definir quais tipos de objeto serão armazenados em cache e quais nunca devem ser cacheados;    38. Garantir que o recurso de cache possa ajustar quanta memória será utilizada para armazenar objetos;    39. Suporte a otimização do protocolo TCP para ajustes a parâmetros das conexões clientes e servidor;    40. A solução deve suportar Internet Content Adaptation Protocol (ICAP);    41. Deve ser capaz de realizar DHCP relay;    42. Deve possuir relatórios das aplicações, com pelos menos os seguintes gráficos:        1. Tempo de resposta da aplicação;        2. Latência;        3. Conexões para conjunto de servidores, servidores individuais;        4. Por URL;    43. A ferramenta de relatórios deve possuir pelo menos os seguintes filtros para a geração dos gráficos:        1. Servidores virtuais;        2. Servidores balanceados;        3. URLs;        4. Países de origem, baseados em geolocalização (GEOIP);        5. Dispositivos de origem do cliente (user agent);    44. Deve possuir framework unificado para configuração da aplicação;    45. Deve possuir criptografia IPSEC para comunicação entre os balanceadores;    46. Quando licenciada, a solução deve ter a capacidade de realizar cache transparente das respostas DNS;    47. A solução deve permitir que cada domínio de roteamento utilize BGP, OSPF e RIP em IPv4 e IPv6;    48. A solução deve suportar Equal Cost Multipath (ECMP);    49. A solução deve realizar Bidirectional Forward Detection (BFD);    50. A solução deve ter suporte a Stream Control Transmission Protocol (SCTP);    51. Deve ter suporte a Transport Layer Security (TLS) Server Name Indication (SNI);    52. A solução deve possuir monitor HTTP/HTTPS com autenticação NTLM embutida, que permita verificar se o HTTP/HTTPS está operando assim como a plataforma de autenticação;    53. A solução deve realizar SSL Forward Proxy;    54. A solução deve ter suporte a TLS 1.2, SHA 2 Cipher e SHA256 hash;    55. A solução deve ter suporte a criptografia Perfect Forward Secrecy não apenas para troca de chaves RSA.    56. A solução deve ser capaz de colocar em fila as requisições TCP que excedam a capacidade de conexões do grupo de servidores ou de um servidor. O balanceador não deverá descartar as conexões que excedam o número de conexões do servidor ou do grupo de servidores:        1. Deve ser possível configurar o tamanho máximo da fila;        2. Deve ser possível configurar o tempo máximo de permanência na fila;    57. A solução deve realizar Controle de Banda Estático para grupos de aplicações e rede;    58. A solução deve realizar Controle de Banda Dinâmico por aplicação e usuário;    59. A solução deve realizar Controle de Banda baseado em domínio de roteamento;    60. Permitir tráfego por parâmetros de QoS (Quality of Service) ou rate-shaping, com pelo menos 2 (duas) filas para priorização de tráfego baseada na camada de aplicação;        1. Através dessa priorização de tráfego e restrição de largura de banda deverá ser possível permitir um melhor nível de serviço para clientes preferenciais em detrimento dos demais clientes.    61. A solução deve permitir a priorização de tráfego de entrada para determinadas aplicações.    62. A solução deve permitir a criação de túneis IP por domíno de roteamento utilizando GRE, IPIP, PPP;    63. A solução deve permitir a criação de túneis IP transparente utilizando GRE e IPIP;    64. Fornecer recursos para o uso de servidores (reals) no mesmo Virtual Server;    65. Possuir suporte ao protocolo SPDY e HTTP 2.0;    66. O equipamento deve possuir suporte ao espelhamento de conexões FTP, HTTP, UDP, SSL.    67. O equipamento deverá permitir a sincronização das configurações de forma automática e manualmente, forçando a sincronização apenas no momento desejado;    68. Permitir a configuração das interfaces de comunicação (heartbeat) em alta-disponibilidade do cluster através da mesma interface de dados e a através de interface dedicada para comunicação;    69. Permitir a criação de regras customizadas através de linguagem aberta para modificar a distribuição dinâmica de tráfego e aumentar a proteção contra ataques;    70. Permita a manipulação do tráfego de entrada e saída, viabilizando assim a alteração de parâmetros no cabeçalho e no corpo das mensagens;    71. Permitir a criação de políticas através de interface gráfica web para manipulação de tráfego através de lógica para, pelo menos, os operadores GEOIP, http-basic-auth, http-cookie, http-header, http-host, http-method, http-referer, http-set-cookie, http-status, http-uri e http-version    72. Deve ser possível tomar as seguintes ações através dessas políticas:        1. Bloqueio de tráfego;        2. Reescrita e manipulação de URL;        3. Registro de tráfego (log);        4. Adição de informação no cabeçalho HTTP;        5. Redirecionamento do tráfego para um membro específico;        6. Selecionar uma política específica para Aplicação Web;    73. A solução deverá ser capaz de fazer log de todas as sessões, onde os registros deverão conter:        1. Endereço IP de origem;        2. Porta TCP ou UDP de origem;        3. Endereço IP de destino;        4. Porta TCP ou UDP de destino;        5. Protocolo de camada 4 (TCP ou UDP);        6. Data e hora da mensagem;        7. URL acessada;    74. A solução deve possuir políticas de uso de senhas administrativas tais como: nível de complexidade, período de validade e travamento de conta devido a erros múltiplos de login de forma nativa ou no mínimo integrado a uma base Active Directory;    75. A solução deve suportar controle de versão da política de configuração de forma a permitir a restauração (rollback) de qualquer versão de políticas;    76. A solução deve ser capaz de analisar a performance de aplicações web;    77. A solução deve possuir relatórios das aplicações;    78. Deve prover métricas de aplicações como:        1. Transações por Segundo;        2. Tempo de latência do cliente e servidor;        3. Throughput de requisição e resposta;    79. A solução deverá gerar informações para permitir análises históricas e auxiliar nos processos de manutenções preventivas, de troubleshooting, de planejamento de capacidade e de análise da experiência dos usuários finais no acesso das aplicações;    80. As informações coletadas deverão permitir a análise dos dados por aplicações, por URL’s, por clientes e por servidores, permitindo assim a identificação mais precisa dos eventuais ofensores do tráfego suportado pela solução;    81. A solução deverá gerar informações estatísticas de acesso identificando para cada aplicação os métodos de acesso HTTP (GET e Post), o tipo de sistema operacional utilizado pelos clientes, e os browsers utilizados;    82. A geração de informações históricas deverá permitir:        1. O detalhamento do tempo de resposta total de carregamento de uma URL e ou Página;        2. Permitir a correlação de métricas de uso de rede com o comportamento das aplicações; 4. Características de Segurança WEB:    1. O equipamento oferecido deverá proteger a infraestrutura web de ataques contra a camada de aplicação (Camada 7);    2. Deve possuir tecnologia para mitigação de DDoS em camada 7 baseado em análise comportamental, usando o aprendizado;    3. Deve possuir proteção contra ataques DDoS, através da análise de comportamento de trafego usando técnicas de análise de dados e Machine Learning;    4. Deve aprender automaticamente o comportamento da aplicação e combinar o comportamento heurístico do tráfego com o stress do servidor de aplicação para determinar uma condição de DDoS;    5. Ao detectar uma condição de DDoS, assinaturas dinâmicas devem ser automaticamente criadas e implementadas em tempo real para proteção da aplicação;    6. Não deve haver a necessidade de intervenção de usuário para configurar limiares de DoS pois esses valores devem ser auto ajustáveis e adaptativos de acordo com mudanças;    7. Através da análise continua de carga e monitoração de saúde de servidores, deve ser possível identificar anomalias e mitiga-las;    8. Deve ajudar a prevenir contra ataques de Credential Stuffing, onde bases de credenciais expostas na Internet são usados para tentativa de acesso de outras aplicações Web;    9. A solução deve possuir a capacidade de automaticamente capturar tráfego no formato TCP Dump relativos aos ataques de DoS L7, Web Scraping e força bruta permitindo uma análise mais aprofundada por parte do administrador;    10. A solução deve suportar o uso de firewall camada 3-4 junto com firewall camada 7 no mesmo equipamento/appliance para evitar problemas com o aumento da latência;    11. O equipamento oferecido deverá possuir a certificação ICSA para Firewall de Aplicação (Web Application Firewall);    12. Permitir a utilização de um modelo positivo de segurança para proteger contra ataques conhecidos aos protocolos HTTP e HTTPS e às aplicações web acessíveis através destes;    13. Possuir política de segurança de aplicações web predefinidas na solução;    14. Permitir a criação de políticas diferenciadas por aplicação e por URL, onde cada aplicação e URL poderão ter políticas totalmente diferentes;    15. Permitir a criação de políticas diferenciadas por aplicação;    16. Permite configurar de forma granular, por aplicação protegida, restrições de métodos HTTP permitidos, tipos ou versões de protocolos, tipos de caracteres e versões utilizadas de cookies;    17. A solução deverá se integrar a soluções de análise de vulnerabilidade compatíveis com DAST (Dynamic Application Security Testing). O resultado desta análise deve ser utilizado para configurar as políticas do equipamento;    18. A solução deve permitir a inspeção de upload de arquivos para os servidores de aplicação;        1. Essa inspeção pode ser feito via integração ICAP. Deve ser possível integrar com diferentes softwares de Antivírus;    19. Permitir que regras customizadas em linguagem aberta possam ser utilizadas para customizar e aumentar a proteção contra ataques recentes;    20. A solução deve se integrar com outras soluções de segurança e análise de logs de outros fabricantes;    21. Deve possuir tecnologia de detecção de anomalias baseada em rastreamento de identificação de dispositivos, permitindo a detecção de DoS, ataques de força bruta e ataques de sequestro de sessão. Deve ser possível filtrar relatórios por identificação de dispositivos;    22. A solução deve permitir incluir em blacklist os endereços IPs que repetidamente falharem a desafios no browser. Portanto o sistema não precisa usar recursos para mitigar tráfego enviado por esses endereços IP. Ao entrar em Blacklist o sistema automaticamente bloqueia os pacotes enviados por esse endereço por um período de tempo;    23. A solução deve prover suporte e fazer a proteção do tráfego em cima de protocolo WebSocket;    24. A solução deve possibilitar o uso de múltiplas formas de logging remoto ao mesmo tempo para a mesma aplicação. Portanto dever ser possível por exemplo registrar os requests válidos num servidor de SIEM e os requests inválidos em outro servidor de SIEM de outra marca e modelo;    25. A solução deverá possuir funcionalidade de proteção positiva e segura contra ataques, incluindo pelo menos:        1. Acesso por Força Bruta;        2. Ameaças Web AJAX/JSON;        3. DoS e DDoS camada 7;        4. Buffer Overflow;        5. Cross Site Request Forgery (CSRF);        6. Cross-Site Scripting (XSS);        7. SQL Injection;        8. Parameter tampering;        9. Cookie poisoning;        10. HTTP Request Smuggling;        11. Manipulação de campos escondidos;        12. Manipulação de cookies;        13. Roubo de sessão através de manipulação de cookies;        14. Sequestro de sessão;        15. Força bruta no browser;        16. XML bombs/DoS;        17. Checagem de consistência de formulários;        18. Checagem do cabeçalho do “user-agent” para identificar clientes inválidos.    26. A solução deve suportar o uso de páginas de login AJAX/JSON tanto com configuração manual como descoberta automática;    27. Deverá ser capaz de identificar e bloquear ataques através de:        1. Assinaturas, com atualização periódica da base pelo fabricante;           1. As assinaturas devem ser atualizadas durante o período do contrato de suporte e garantia sem que seja necessário nenhum custo a mais por parte da CONTRATANTE na aquisição de novas licenças ou subscrições. Deve fazer parte da solução ofertada;        2. Regras de verificação personalizadas – política de segurança configurada.    28. Prevenir contra vazamento de dados sensíveis (mensagens de erro HTTP, códigos das aplicações, entre outros) dos servidores de aplicação, retirando os dados ou mascarando a informação nas páginas enviadas aos usuários;    29. Permitir a customização da resposta de bloqueio;    30. Permitir a liberação temporária ou definitiva (whitelist) de endereços IP bloqueados por terem originados ataques detectados pela solução;    31. Deve permitir limitar o número de conexões e requisições por IP de origem para cada endereço IP Virtual;    32. Deve permitir adicionar, automaticamente e manualmente, em uma lista de bloqueio, os endereços IP de origem que ultrapassarem o limite estabelecido, por um período determinado através de configuração;    33. Deve permitir criar lista de exceção (whitelist) por endereço IP específico ou faixa de sub-rede;    34. A solução deve suportar o modelo de segurança positiva definido pelo OWASP, pelo menos o que consta no TOP 10;    35. Permitir o uso do parâmetro HTTP X-Forwarded-For como parte da política de controle;    36. Deverá implantar, no mínimo, as seguintes funcionalidades:        1. Proteção contra Buffer Overflow;        2. Checagem de URL;        3. Checagem de métodos HTTP utilizados (GET, POST, HEAD, OPTIONS, PUT, TRACE, DELETE, CONNECT);        4. Proteção contra envios de comandos SQL escondidos nas requisições enviadas a bases de dados (SQL Injection);        5. Proteção contra Cross-site Scripting;        6. Funcionalidade de Cookie Encryption;        7. Checagem de consistência de formulários;        8. Checagem do cabeçalho “user-agent” para identificar clientes inválidos;    37. Implementar funcionalidades para proteção contra exposição de informações do ambiente e servidores internos, incluindo pelo menos:        1. Informações que identifique o sistema operacional e o servidor web através de “impressão digital” dos sistemas;        2. Esconder qualquer mensagem de erro HTTP dos usuários;        3. Remover as mensagens de erro às páginas que serão enviadas aos usuários;    38. Permitir a utilização de uma página HTML informativa e personalizável como HTTP Response aos bloqueios;    39. Deve ser possível verificar o endereço de origem do pacote IP no cabeçalho IP e no parâmetro X-forwarded-for (XFF);    40. Deve suportar a criação de políticas por geolocalização, permitindo que o tráfego de determinado(s) país/países seja(m) bloqueado(s);    41. Possuir mecanismo de aprendizado automático capaz de identificar todos os conteúdos das aplicações, incluindo URLs, parâmetros URLs, campos de formulários, o que se espera de cada campo (tipo de dado, tamanho de caracteres), cookies, arquivos XML e elementos XML;    42. O equipamento oferecido deverá possuir uma funcionalidade de criação automática de políticas, onde a política de segurança é criada e atualizada automaticamente baseando-se no tráfego real observado à aplicação;    43. O perfil aprendido de forma automatizada pode ser ajustado, editado ou bloqueado;    44. O equipamento oferecido deverá possuir proteção baseada em assinaturas para prover proteção contra ataques conhecidos. Deverá ser possível desabilitar algumas assinaturas específicas em determinados parâmetros, como uma exceção a regra geral;    45. A atualizações de assinaturas deverão passar por um período configurável de testes, ondes nenhuma requisição que viole a assinatura será bloqueada, apenas informada no relatório. Este processo deve ser automatizado, não sendo necessário criar regras específicas a cada atualização de assinatura;    46. O equipamento oferecido deverá permitir o bloqueio de ataques DoS na camada 7, possuindo também a opção de apenas registrar o ataque, sem tomar nenhuma ação de bloqueio;    47. O equipamento oferecido deverá possuir as seguintes formas de detecção de ataques DoS na camada de aplicação:        1. Número de requisições por segundo enviados a uma URL específica;        2. Número de requisições por segundo enviados de um IP específico;        3. Detecção através de código executado no cliente com o objetivo de detectar interação humana ou comportamento de robôs (bots);        4. Número máximo de transações por segundo (TPS) de um determinado IP;        5. Aumento de um determinado percentual do número de transações por segundo (TPS);        6. Aumento do stress do servidor de aplicação;    48. O equipamento oferecido deverá permitir o bloqueio de ataques de força bruta de usuário/senha em páginas de acesso (login) que protegem áreas restritas. Este bloqueio deve limitar o número máximo de tentativas e o tempo do bloqueio deverá ser configurável;    49. O equipamento oferecido deverá permitir o bloqueio de determinados endereços IPs que ultrapassarem um número máximo de violações por minuto. O período de bloqueio deverá ser configurável e durante este período todas as requisições do cliente serão bloqueadas automaticamente;    50. O equipamento oferecido deverá permitir o bloqueio de robôs (bots) que acessam a aplicação através de detecção automática, não dependendo de cadastros manuais. Robôs conhecidos do mercado, como Google, Yahoo e Microsoft Bing deverão ser liberados por padrão;    51. O equipamento oferecido deverá permitir o cadastro de robôs que podem acessar a aplicação;    52. A solução deverá proteger a aplicação Web contra robôs sofisticados através da combinação de desafios enviados ao browser do usuário e técnicas avançadas de analise comportamental;    53. A solução deverá possuir proteção proativa contra ataques automatizados por robôs e outras ferramentas de ataque;    54. A solução deverá encriptar dados e credenciais na camada de aplicação, sem ter a necessidade de atualizar a aplicação;        1. Essas informações devem ser encriptadas para proteger o login e as credenciais dos usuários e com isso os dados da aplicação;    55. Deve proteger informações sensíveis e confidenciais da interceptação por terceiros, através da criptografia de dados quando ainda no browser do usuário;        1. Deve proteger esses dados criptografados de malwares e keyloggers;    56. O equipamento oferecido deverá implementar proteção ao JSON (JavaScript Object Notation);    57. Possuir firewall XML integrado com suporte a filtro e validação de funções XML específicas da aplicação;    58. Implementar a segurança de web services, através dos seguintes métodos:        1. Criptografar/Decriptografar partes das mensagens SOAP;        2. Assinar digitalmente partes das mensagens SOAP;        3. Verificação de partes das mensagens SOAP;    59. Prevenir o vazamento de informações, permitindo o bloqueio ou a remoção dos dados confidenciais;    60. Prevenir que erros de aplicação ou infra-estrutura sejam mostrados ao usuário;    61. Deverá ter integração, via ICAP, com servidor de anti-vírus para verificação dos arquivos a serem carregados nos servidores;    62. Permitir o uso do parâmetro HTTP X-Forwarded-For como parte da política de controle;    63. Deverá proteger o protocolo FTP com pelo menos os seguintes métodos:        1. Determinar os comandos FTP permitidos;        2. Requests FTP anônimos;        3. Checar conformidade com o protocolo FTP;        4. Proteger contra ataques de força bruta nos logins;    64. Deverá proteger o protocolo SMTP com pelo menos os seguintes métodos:        1. A comunicação deve ser aderente a RFC 2821;        2. Limitar o número de mensagens;        3. Validar registro SPF do DNS;        4. Determinar quais métodos SMTP podem ser utilizados;    65. Deverá armazenar os registros (logs) localmente ou exportar para Syslog server;    66. Deverá proteger contra atraques CSRF (Cross-Site Request Forgery), podendo ser possível especificar quais URLs serão examinadas;    67. Deverá possuir controle de fluxo por aplicação permitindo definir o fluxo de acesso de uma URL para outra da mesma aplicação. Dessa forma qualquer tentativa de acesso a um determinado site que não siga o fluxo passando pelas URLs pré-definidas deverá ser bloqueado como uma tentativa de acesso ilegal;    68. A solução deve fornecer relatórios consolidados de ataques com pelo menos os seguintes dados:        1. Resumo geral com as políticas ativas;        2. Anomalias e estatísticas de tráfego;        3. Ataques de DoS, força bruta e robôs;        4. Informações sobre violações, URL, endereços IP, países, severidade e PCI Compliance;    69. Deverá permitir o agendamento de relatórios a serem entregues por e-mail;    70. Fornecer os seguintes Gráficos de alertas por:        1. Política de segurança;        2. Tipos de ataques;        3. Violações;        4. URL;        5. Endereços IP;        6. Países;        7. Severidade;        8. Código de resposta;        9. Métodos;        10. Protocolos;        11. Vírus;        12. Usuário;        13. Sessão;    71. Deverá exportar as requisições que contém os ataques, pelo menos no formato PDF;    72. Deve possuir relatório em tempo real sobre ataques de DoS L7, atualizado automaticamente;    73. A solução deve mostrar o impacto de ataques de DoS L7 na performance e memória do servidor;    74. Os logs devem indicar o momento de início e final de um ataque de DoS L7;    75. Possuir método de mitigação de DoS L7 baseado em:        1. CAPTCHA;        2. Descarte de todas as requisições de um determinado IP e/ou país suspeito;        3. Geolocalização, incluindo a prevenção com CAPTCHA para países suspeitos que ultrapassarem limiares;        4. Defesa proativa contra bot, através da injeção de um desafio JavaScript para detectar se é um usuário legítimo ou robô;    76. A solução deve permitir que ao detectar um falso positivo, o administrador aceite a requisição e atualize a política automaticamente;    77. A solução ao se integrar com um Scanner de vulnerabilidade deve mostrar quais a vulnerabilidades podem ser resolvidas automaticamente (pela própria solução de WAF) e quais podem ser resolvidas manualmente, pelo próprio administrador. No caso de resolução manual, deve ainda mostrar um guia com os passos necessários para resolver aquela vulnerabilidade, inclusive com a avisos de possíveis consequências na aplicação Web;    78. A solução deve classificar o nível de violação de uma requisição, possuindo pelo menos 5 níveis, onde o nível 5 é referente a violação mais grave e, portanto, deve ter prioridade;    79. A solução deve possuir proteção de DDoS L7 baseado em análise comportamental, sem precisar de nenhuma configuração manual; 5. Características de alta disponibilidade global    1. A solução deve operar, no mínimo, das seguintes formas:       1. DNS autoritativo;       2. DNS secundário;       3. DNS resolver;       4. DNS cache;       5. Balanceamento de DNS servers;       6. DNSSec;    2. A solução deve ser capaz de realizar transferência de zonas para múltiplos servidores DNS Primários responsáveis por diferentes zonas;    3. A solução deverá ter a capacidade de uso de chave criptográfica TSIG para comunicação segura entre servidores DNS, obedecendo no mínimo os padrões: HMAC MD5, HMAC SHA-1 ou HMAC SHA-256;    4. A solução deve realizar o offload dos servidores de DNS, funcionando como o DNS secundário;    5. A solução deve possuir certificação ICSA;    6. A solução deve possuir proteções contra ataques DNS, de no mínimo dos seguintes tipos:       1. Inspeção de protocolo;       2. Validação de protocolo;       3. UDP flood;       4. Pacotes mal formados;       5. Ataque Teardrop;       6. Ataque ICMP;    7. Permitir que regras customizadas em linguagem aberta possam ser utilizadas para customizar a distribuição dinâmica de tráfego e aumentar a proteção contra ataques;    8. A solução deve ser capaz de realizar balanceamento dos servidores DNS;    9. A solução deve ser capaz de realizar filtragem de pacotes;    10. A solução deve prover segurança do protocolo DNS, protegendo contra ataques de negação de serviço, NXDOMAIN e reflexão e amplificação de DNS;    11. A solução deve prover segurança do protocolo DNS, protegendo contra ataques de Cache Poisoning;    12. A solução deve realizar stateful inspection;    13. A solução deve possuir base de Geolocalização IP;    14. A solução deve implementar DNS64;    15. A solução deve suportar pelo menos os seguintes tipos de requisição DNS: SOA, A, AAAA, CNAME, DNAME, HINFO, MX, NS, PTR, SRV, TXT;    16. Deve ser capaz de gerar estatísticas sobre consultas de DNS por: Aplicação, nome da query, tipo da query, endereço IP do cliente;    17. Deve ser possível configurar a solução de modo inline a estrutura de DNS existente e transparente sem requerer grandes mudanças na infraestrutura;    18. Deve prover as respostas as queries DNS da própria RAM CACHE;    19. A solução deve ser capaz de realizar IP Anycast;    20. A solução deve ser capaz de realizar DNSSec, independente da estrutura dos servidores DNS em uso;    21. A solução de alta disponibilidade não deve depender de BGP ou outro protocolo de roteamento;    22. A solução de alta disponibilidade será realizada baseada em respostas a requisições DNS. A resposta a requisições DNS devem conter apenas endereços que estejam disponíveis no momento, e balanceadas por usuário, de acordo com as políticas definidas;    23. A solução deverá aceitar resolução de nomes baseada em topologia, onde requisições de DNS são respondidas baseado no país, continente, ou endereço IP de onde veio a requisição;    24. Deve ser possível ajustar quantos endereços são enviados em uma única resposta;    25. Suporte a monitoração de estado de saúde de servidores, serviços e links de conexão a provedor de serviço, garantindo a disponibilidade do serviço oferecido;    26. Suportar pelo menos os seguintes algoritmos de balanceamento:        1. Round Robin;        2. Global Availability;        3. Ratio;        4. LDNS Persist;        5. Geografia;        6. Disponibilidade da Aplicação;        7. Capacidade do Virtual Server;        8. Least Connections;        9. Pacotes por segundo;        10. Round trip time;        11. Hops;        12. Packet Completion Rate;        13. QoS definido pelo usuário;        14. Kilobytes per Second;    27. A solução deverá ser capaz de implementar persistência da conexão do usuário entre aplicações ou data centers;    28. A solução deverá suportar o controle de grupos de aplicações, e permitir que um usuário seja redirecionado para outro datacenter quando houver falha em qualquer das aplicações de um mesmo grupo;    29. A solução deverá permitir que as políticas sejam configuradas individualmente por aplicação sendo balanceada;    30. A solução deverá permitir que a contingência seja automática, mas que o retorno seja manual;    31. A solução deve ser capaz de atender clientes IPv6 quando o site atende apenas com IPv4 (requests AAAA ou A6);    32. Possuir suporte a IPv6 no balanceamento global entre datacenters.    33. Ter capacidade de tratar informações das camadas L4-L7 (FTP, SMTP, URL, HTTP Header, TCP e UDP) para a tomada de decisão de encaminhamento a servidor real, em IPv4 e IPv6;    34. Deverá possuir a funcionalidade de resposta rápida a queries DNS permitindo respostas mais rápidas para zonas que seja autoritativo;    35. A solução deve possuir suporte a Response Policy Zones (RPZ), mecanismo de firewall usado por DNS recursivo para permitir o tratamento customizado da resolução de nomes. Portanto a solução deve ser capaz de filtrar queries DNS para domínios considerados maliciosos e retornar respostas customizadas; 6. Garantia e Atualização    1. Deverá possuir serviço de suporte e garantia DO FABRICANTE de 60 meses;    2. Será de responsabilidade da contratada o fornecimento de todos os componentes de software e de hardware necessários ao pleno funcionamento do sistema. Caberá à contratada o fornecimento de todas as licenças de "software" necessárias para fins de provimento de TODAS as funcionalidades exigidas nessa especificação    3. A contratada deverá disponibilizar, na vigência do contrato, todas as atualizações dos softwares e firmwares dos equipamentos, concebidas em data posterior ao seu fornecimento, pelo período especificado no termo de referência, sem qualquer ônus adicional para o contratante;    4. As atualizações incluídas devem ser do tipo “minor release” e “major release”, permitindo manter os equipamentos atualizados em sua última versão de software/firmware; 7. Implantação    1. O equipamento deverá ser instalado e configurado pela CONTRATADA    2. Entende-se por instalação, configuração e transferência de conhecimento todos os serviços pertinentes ao completo funcionamento da nova solução, compreendendo inicialmente a elaboração do projeto executivo que deverá nortear a interconexão física e lógica dos equipamentos fornecidos e a realização do repasse de conhecimento pertinente às tecnologias empregadas;       1. Instalação de todos os componentes da solução fornecidos como softwares;       2. Componentes em softwares poderão ser instalados em servidores/equipamentos do parque tecnológico da CONTRATANTE, quando compatíveis e de acordo com as especificações técnicas, sendo da CONTRATANTE a responsabilidade pela disponibilização dos recursos necessários à sua instalação;       3. Ativação de todas os componentes da solução fornecidos como assinaturas (subscription);       4. Disposição e conectorização de hardwares no rack que os acomodarão;       5. Instalação dos transceivers em seus módulos/slots;       6. Interconexão a outros switches, roteadores e servidores de rede, entre outros;       7. Configurações de interfaces, endereçamento e serviços de rede, além das configurações das políticas de segurança da informação e de outras configurações necessárias ou constantes no Projeto Executivo;       8. Ajuste dos demais parâmetros de configuração, conforme Projeto Executivo;       9. Configuração relativa ao balanceamento de carga:          1. Configuração de alta disponibilidade;          2. Configuração de interfaces virtuais para balanceamento de servidores;          3. Configuração de perfis de otimização de trafego;          4. Configuração de políticas de acesso;          5. Configuração de regras de manipulação de trafego;       10. Configuração relativa à solução de segurança de aplicações web:           1. Configurações de bloqueios de máscara contra violações, técnicas de invasão, compliance de protocolos HTTP e segurança de web services;           2. Configuração de assinaturas de ataques;           3. Configuração de ataques baseados em assinatura com base nas requisições do cliente;           4. Configuração de parâmetros para uma aplicação específica;           5. Configuração de segurança de aplicação baseada em DoS Protection;       11. Configuração relativas a alta disponibilidade de sites e DNS:           1. Configuração de até 2 (dois) data centers;           2. Configuração de até 4 (quatro) links de dados;           3. Configuração de até 8 (oito) Wide-IPs (hosts dns alto disponível);           4. Configuração de até 4 zonas DNS com DNSSEC;           5. Configuração de forwarding e recursividade;    3. A equipe técnica que executará os serviços de instalação e configuração deverá sempre conter pelo menos um técnico, presente em todos os momentos da execução do serviço, treinado e capacitado nos produtos, serviços e tecnologias objetos do LOTE 06, que deverá possuir, no mínimo, as seguintes qualificações:       1. Certificado oficial, de nível profissional com comprovação da capacidade de implementação da solução ofertada, emitido pelo fabricante em nome deste profissional nos produtos, serviços e tecnologia objetos desta contratação;       2. A CONTRATADA deverá apresentar atestado de capacidade técnica, emitido por pessoa jurídica de direito público ou privado, que comprove que a CONTRATADA tem experiência profissional em projetos que envolvam appliances de segurança conforme ofertados(capacidade técnica);    4. Todos os parâmetros a serem configurados deverão ser alinhados entre as partes em reuniões de pré-projeto, podendo estas ser realizadas presencialmente, por telefone ou via conferência web, devendo a CONTRATADA sugerir as configurações de acordo com normas e práticas recomendadas, cabendo à CONTRATANTE a sua aceitação expressa ou recusa, ambas por escrito nos casos de não atendimento das condições estabelecidas;    5. As configurações deverão seguir fielmente a padronização previamente estabelecida pela CONTRATANTE;    6. É parte integrante do escopo de transferência do conhecimento a disponibilização de toda a documentação técnica, incluindo manuais de instalação, configuração e de usuário, relativa aos componentes integrantes da solução;       1. A transferência de conhecimento deverá ser realizada em Florianópolis-SC, preferencialmente nas dependências da CONTRATANTE, por técnicos com certificação(ões) técnica(s) emitida(s) pelo(s) fabricante(s) dos equipamentos, e poderá ser realizada durante as semanas de operação assistida contratadas;       2. A carga horária deverá ser de, no mínimo, 8 (oito) horas e contar com até 5 (dez) participantes indicados pela CONTRATANTE;       3. A CONTRATADA assumirá todas as despesas e encargos inerentes à transferência de conhecimento, compreendendo as despesas com hospedagem, transporte e alimentação dos técnicos responsáveis pelo repasse e demais despesas/custos indiretos que incidirem sobre esta contratação;       4. Durante a transferência de conhecimento deverão ser fornecidos aos técnicos da CONTRATANTE todo material e documentação, preferencialmente em português, necessários à perfeita compreensão da solução instalada (slides, exemplos de implementação, documentação do projeto executado na CONTRATANTE, etc.) bem como alimentação compatível com a quantidade de pessoas envolvidas; 8. Documentação    1. 15.1 Ao término do serviço deve ser fornecido um relatório detalhado (as-built) contendo todas as configurações realizadas, com comentários sobre os principais comandos e as justificativas das opções de parametrização de modo a facilitar a posterior administração da solução e a continuidade de seu funcionamento; a critério da CONTRATANTE, poderá ser elaborado um único as-built contendo todas as informações de todos os equipamentos e módulos instalados/configurados, incluindo, mas não se limitando, a:       1. Documentação descritiva dos produtos, com todos os componentes e softwares que perfazem a solução;       2. Documentação técnica do ambiente; 9. 8.1.3. Endereço na Internet do fabricante, onde seja possível obtenção de literatura técnica e drivers atualizados; |

**LOTE 06 - ITEM 18 - Treinamento - Solução de balanceamento de carga e segurança para aplicações web**

|  |
| --- |
| ESPECIFICAÇÃO TÉCNICA - Treinamento técnico oficial do da solução ofertada no LOTE 06 – ITEM 17.  Características mínimas:   * 1. Deverá ser ministrado por instrutor, online, estando disponível durante todo período do treinamento.   2. Não serão aceitos treinamentos gravados.   3. Deverá ser ministrado por empresa provedora de treinamento oficial autorizada pelo respectivo fabricante;   4. O treinamento deverá englobar, no mínimo, os seguintes tópicos:      1. Configuração relativa ao balanceamento de carga:      2. Configuração de alta disponibilidade;      3. Configuração de interfaces virtuais para balanceamento de servidores;      4. Configuração de perfis de otimização de trafego;      5. Configuração de políticas de acesso;      6. Configuração de regras de manipulação de trafego;      7. Configuração relativa a solução de segurança de aplicações web:      8. Configurações de bloqueios de máscara contra violações, técnicas de invasão, compliance de protocolos HTTP e segurança de web services;      9. Configuração de assinaturas de ataques;      10. Configuração de ataques baseados em assinatura com base nas requisições do cliente;      11. Configuração de parâmetros para uma aplicação específica;      12. Configuração de segurança de aplicação baseada em DoS Protection;      13. Configuração relativas a alta disponibilidade de sites e DNS:      14. Configuração de data centers;      15. Configuração de links de dados;      16. Configuração de Wide-IPs (hosts dns alto disponível);      17. Configuração de zonas DNS com DNSSEC;      18. Configuração de forwarding e recursividade;   5. Caso seja necessário mais de um treinamento, cabe a CONTRATADA o fornecimento de proposta que englobe todos;   6. Deverão ser emitidos certificados de conclusão dos treinamentos para todos os participantes e enviados para o Fiscal do Contrato. O prazo para emissão e envio dos certificados aos alunos é de 30 (trinta) dias corridos após o término de cada curso;   7. Após a realização de cada treinamento e entrega dos certificados, será emitido um Termo de Aceite do Treinamento. |

**LOTE 07 - ITEM 19 – Licenças Commvault para backup do Microsoft365**

|  |
| --- |
| ESPECIFICAÇÃO TÉCNICA – Licenciamento para backup do Microsoft365 integrado ao software Commvault Complete Data Protection  Características mínimas:   * 1. Licença perpétua para backup de 1(uma) conta do Microsoft365, independentemente da volumetria utilizada, incluindo a possibilidade de fazer backup as seguintes ferramentas:      1. Exchange;      2. One Drive;      3. SharePoint;      4. Microsoft Teams;   2. Todas as especificações deverão ser atendidas, exclusivamente, pelo fabricante Commvault. Não serão admitidas propostas que incluam composição de softwares de fabricantes diversos ou variações semelhantes;   3. Garantia e suporte técnico, com direito à atualização de software, na modalidade Production (24x7) atendido diretamente pela Commvault   4. O período de garantia deverá ser compatibilizado para finalizar juntamente com período já existente no registro do Commcell ID 100398; |

**LOTE 08 - ITEM 20 – Cage para Discos (Backplane/ Drive Cage)**

|  |
| --- |
| ESPECIFICAÇÃO TÉCNICA – Cage para Discos (Backplane/ Drive Cage)  REFERÊNCIA: HPE DL380 Gen 10 Box 1/2 Cage BACKPLANE KIT 8XSFF - Part Number 826691-B21  Características mínimas:   * 1. Painel Traseiro para Servidor Hp Dl380 Gen10 para acomodação da expansão de discos;   2. Suportar oito unidades SAS / SAFA SFF 2,5” na caixa;   3. Acompanhar cabos de energia;   4. Deve ser totalmente compatível com o servidor Hp Dl380 Gen10(Part Number 19720-B21);   5. Deve possuir garantia de 12 meses; |

**LOTE 08 - ITEM 21 – Controlador modular HPE Smart Array P816i-a SR Gen10**

|  |
| --- |
| ESPECIFICAÇÃO TÉCNICA – Controlador modular HPE Smart Array P816i-a SR Gen10  REFERÊNCIA: HPE Smart Array P816i-a SR Gen 10 Ctrlr - Part Number 804338-B21  Características mínimas:   * 1. Controlador modular para expansão da capacidade de armazenamento;   2. Suporte para 12 Gb/s SAS e PCIe 3.0;   3. Deve possuir 16 portas internas SAS, compatível com níveis avançados de RAID com cache de gravação garantido por flash de 4GB (FBWC);   4. Deve ser totalmente compatível com o servidor Hp Dl380 Gen10(Part Number 19720-B21);   5. Deve possuir garantia de 12 meses; |

**LOTE 08 - ITEM 22 –** **Capacitores híbridos**

|  |
| --- |
| ESPECIFICAÇÃO TÉCNICA – Capacitores híbridos  REFERÊNCIA: HPE Smart Hybrid Capacitor w 145mm - Part Number P02377-B21  Características mínimas:   * 1. Capacitores híbridos de armazenamento inteligente HPE com kit de cabo de 145 mm   2. Deve ser totalmente compatível com o servidor Hp Dl380 Gen10(Part Number 19720-B21);   3. Deve possuir garantia de 12 meses; |

**LOTE 08 - ITEM 23 – Discos SAS HDD**

|  |
| --- |
| ESPECIFICAÇÃO TÉCNICA – Discos SAS HDD  REFERÊNCIA: HPE 2,4TB SAS 12G 10K SFF SC 512e MV HDD - Part Number: 881457-B21  Características mínimas:   * 1. Disco SAS do tipo hard drive HDD;   2. Capacidade de no mínimo 2.4 TB;   3. Interface SAS 12GB/S, tipo HOT-SWAP;   4. Formato de tamanho 2,5” SFF;   5. Taxa de transferência de dados de 1.2 GBPS;   6. Velocidade de rotação de 10000 RPM;   7. Formato avançado 512E;   8. Deve ser totalmente compatível com o servidor Hp Dl380 Gen10(Part Number 19720-B21);   9. Deve possuir garantia de 12 meses; |

**LOTE 08 - ITEM 24 – Discos SAS SSD**

|  |
| --- |
| ESPECIFICAÇÃO TÉCNICA – Discos SAS SSD  REFERÊNCIA: HPE 1,92TB SAS RI SFF SC VS MV SSD – Part Number: P36999-B21  Características mínimas:   * 1. Disco SAS do tipo Drive de Estado Sólido SSD;   2. Capacidade de no mínimo 1.9 TB;   3. Interface SAS 12GB/S;   4. Formato de tamanho 2,5” SFF;   5. Leitura randômica de 4K com 155000IOPS;   6. Deve ser totalmente compatível com o servidor Hp Dl380 Gen10(Part Number 19720-B21);   7. Deve possuir garantia de 12 meses; |

**LOTE 08 - ITEM 25 – Serviço de Implementação/Instalação**

|  |
| --- |
| ESPECIFICAÇÃO TÉCNICA – Serviço de Implementação/Instalação  Características mínimas:   * 1. Instalação/Implantação do itens presentes no LOTE 08;   2. O escopo da instalação consiste em 01 (um) servidor HP Dl380 Gen10(Part Number: 19720-B21) de propriedade da contratante;   3. O serviço deverá ser realizado pelo fabricante do equipamento ou seu representante autorizado;   4. A instalação consiste no pleno funcionamento dos itens contratados; |

1. **CONDIÇÕES GERAIS**
   1. Licenciamento para o Lote 01, Lote 02 e Lote 07:
      1. Será admitido o fornecimento de licenças acadêmicas desde que as mesmas não estejam restritas somente para uso acadêmico. Ou seja, estas licenças devem permitir o uso dos softwares fornecidos no âmbito da administração da Universidade.
   2. Garantia e Suporte:
      1. Todos os softwares e equipamentos, salvo quando descrito o contrário no Termo de Referência, devem possuir suporte e garantia de 60 meses do fabricante por meio de uma Central de Suporte Técnico;
      2. Em caso de software a garantia deve englobar a atualização de versões de software, incluindo upgrades, updates ou patches de correção;
      3. Em caso de hardware, a garantia deve englobar a manutenção corretiva de todos os componentes de hardware e software fornecidos, incluindo peças, upgrades, updates ou patches de correção;
      4. O atendimento da Central de Suporte Técnico deverá ser prestado diretamente pelo fabricante, por especialistas e/ou analistas, para a abertura de chamados técnicos de software.
      5. Salvo quando descrito o contrário no termo de referência, o tempo máximo de atendimento para problemas de hardware não poderá ser superior a 8 (oito) horas após a abertura do chamado na Central de Suporte Técnico do fabricante onde, após diagnóstico por telefone, poderá ser deslocado um técnico de campo para ir ao local e realizar o reparo/substituição dos componentes defeituosos;
      6. Para problemas técnicos que não podem ser resolvidos rapidamente de forma remota, no julgamento da Contratada, a mesma deverá enviar um técnico nas dependências da Contratante para fornecer suporte técnico aos produtos de hardware cobertos e devolvê-los à condição operacional.
      7. A garantia deverá abranger todo e qualquer defeito de projeto, fabricação, transporte, softwares e acessórios envolvidos;
      8. A Contratada deverá disponibilizar acesso ao site do(s) fabricante(s) da solução para que seja possível efetuar o download gratuito de todas as atualizações de softwares, drivers de dispositivos, bem como dispor dos manuais do usuário, com informações detalhadas e atualizadas sobre: instalação, configuração, operação e administração dos sistemas, além dos manuais técnicos de todos os componentes da solução;
   3. Abertura de Chamados:
      1. A abertura de chamados técnicos poderá ser realizada no fabricante da solução ofertada. Os chamados poderão ser abertos através dos seguintes canais:
         1. Telefone 0800;
         2. Página web mantida pela Contratada e pelo fabricante do equipamento.
   4. Para comprovação das especificações exigidas, a licitante deverá apresentar em formato digital (disponível no site do fabricante ou fornecido em mídia), sob pena de desclassificação da proposta, os prospectos técnicos e/ou catálogos do fabricante do(s) item(ns) cotados, informando marca, o modelo e o fabricante do item, não sendo aceita a simples cópia da especificação geral do edital;
   5. Todos os itens deste edital deverão constar no portfólio de produtos do fabricante, sendo que eles não deverão estar na lista de produtos à serem descontinuados (End-of-Life, End-of-Sale, End-of-Market e End-of-Support), com exceção aos casos onde o modelo de licenciamento perpétuo de software esteja em revisão/descontinuidade pelo fabricante;
   6. Todos os equipamentos deste edital deverão ser novos e sem uso. Não serão aceitos equipamentos usados, re-manufaturados ou de demonstração. Os equipamentos deverão ser entregues nas caixas lacradas pelo fabricante, não sendo aceitos equipamentos com caixas violadas;
   7. Deverá ser fornecido, **obrigatoriamente**, no **formato abaixo**, um documento que faça a associação do item especificado neste Termo de Referência com o documento técnico que comprove a validação do mesmo referenciando o local exato no documento em que essa comprovação se encontra:

|  |  |
| --- | --- |
| 10.10.1 – Característica x | Datasheet X, página Y, item N |
| 10.10.2 – Característica z | Site: [www.fabricante.com/](http://www.fabricante.com/xxxxx)zzzzz |

1. **LOCAL, PRAZOS E CONDIÇÕES DE FORNECIMENTO:**
   1. **Locais** – Os produtos serão entregues e/ou executados pelo(s) Contratado(s), conforme a necessidade e mediante Autorização de Fornecimento – AF/Contrato.
      1. **CAMPUS I – GRANDE FLORIANÓPOLIS:**
         1. **Reitoria:** Av. Madre Benvenuta, 2007, Itacorubi, Florianópolis/SC, CEP 88035-001. **Horário de funcionamento: 13h às 19h.**
      2. **CAMPUS II – Norte Catarinense:**
         1. **CCT - Centro de Ciências Tecnológicas**. Rua Paulo Malschitzki, Zona Industrial Norte - Joinville, SC, CEP: 89.219-710.
   2. As solicitações serão expedidas somente pelo Fiscal de Contrato de cada Centro ou substituto legal, discriminando os materiais a serem adquiridos, fornecendo os dados do objeto e a quantidade desejada, por e-mail.
   3. As solicitações só poderão ser atendidas se houver saldo do item na Autorização de Fornecimento (AF)/Contrato vigente.
   4. O prazo de entrega dos materiais e/ou serviços constantes nas solicitações será de até 60 dias após a Autorização formal para entrega do material, por escrito pelo Fiscal do Contrato de cada Centro, podendo ser prorrogado por igual prazo mediante justificativa devidamente apresentada com antecedência e aceita pela Contratante, devendo, esta entrega, ser realizada, obrigatoriamente até o dia 31/12/2022 caso o prazo ultrapasse o ano de 2022.
   5. A Contratada receberá por e-mail a AF, a qual começará a contar o prazo para entrega dos materiais ou será convocada para assinatura do Contrato, conforme o caso.
   6. A Contratante não aceitará, sob nenhum pretexto, a transferência de responsabilidade da Contratada para terceiros.
   7. A Contratante reserva-se o direito de a qualquer tempo, previamente ao aceite, ou durante o prazo de validade do produto, proceder a analise técnica e de qualidade do mesmo, através de Parecer Técnico, realizado diretamente ou por intermédio de terceiros.
      1. Caso o Parecer Técnico rejeite o produto analisado este deverá ser substituído imediatamente pela Contratada, sem qualquer ônus para a Contratante.
   8. A Contratada, mesmo não sendo a fabricante, responderá inteira e solidariamente pela qualidade e autenticidade destes, obrigando-se a substituir, as suas expensas, no todo ou em parte, o(s) produto(s) em que se verificar(em) vícios, defeitos, incorreções, resultantes da fabricação ou transporte, constatado visualmente ou em laboratório, respondendo por todos os custos.
      1. O aceite dos produtos pela Contratante, não exclui a responsabilidade civil da Contratada por vícios de quantidade ou qualidade do produto ou disparidade com as especificações técnicas exigidas no edital ou atribuídas pela Contratada, verificados posteriormente, garantindo-se à Contratante as faculdades previstas no Art. 18 da Lei Federal 8.078/90 (Código de Defesa do Consumidor).
   9. Para efeitos de garantia, será suficiente à UDESC a apresentação de cópia da Nota Fiscal de compra.
   10. Em caso de manutenção, a contratada deverá fornecer todos os recursos necessários à perfeita execução dos serviços, em quantidade, qualidade e tecnologia adequada aos padrões recomendados pelos fabricantes ou padrões determinado no edital.

ANEXO II

**ANEXO II DO EDITAL – QUANTITATIVOS E PROPOSTA DE PREÇOS**

1. **QUANTITATIVO DOS ITENS**

O quantitativo dos itens está especificado conforme a tabela abaixo:

|  |  |  |  |
| --- | --- | --- | --- |
| **LOTE** | **ITEM** | | **QTDE** |
| 1 | 1 | ACADEMIC VMWARE VREALIZE OPERATIONS 8 ADVANCED | 32 |
| 2 | ACADEMIC VMWARE NSX-T ADVANCED | 32 |
| 3 | SERVIÇOS TÉCNICOS ESPECIALIZADOS EM VMWARE NSX | 1 |
| 2 | 4 | RED HAT OPENSHIFT CONTAINER PLATFORM PREMIUM | 6 |
| 5 | RED HAT RUNTIMES PREMIUM | 6 |
| 6 | RED HAT OPENSHIFT DATA FOUNDATION ESSENTIALS PREMIUM | 6 |
| 7 | SERVIÇOS TÉCNICOS ESPECIALIZADOS EM PLATAFORMA RED HAT | 500 |
| 8 | TREINAMENTO - RED HAT CONTAINER ADOPTION BOOT CAMP FOR ADMINISTRATORS CLASSROOM TRAINING - DO700 | 7 |
| 3 | 9 | TREINAMENTO - VMWARE VSPHERE: OPTIMIZE AND SCALE [V7] | 3 |
| 10 | TREINAMENTO - VMWARE VSPHERE: TROUBLESHOOTING [V7] | 3 |
| 11 | TREINAMENTO - VMWARE NSX-T DATA CENTER: TROUBLESHOOTING AND OPERATIONS [V3.2] | 3 |
| 12 | TREINAMENTO - VMWARE NSX-T DATA CENTER: INSTALL, CONFIGURE, MANAGE [V3.2] | 3 |
| 4 | 13 | TREINAMENTO - ADMINISTRAÇÃO DA INFRAESTRUTURA DO NÚCLEO HÍBRIDO DO WINDOWS SERVER (AZ-800) | 5 |
| 14 | TREINAMENTO - CONFIGURAR SERVIÇOS AVANÇADOS HÍBRIDOS DO WINDOWS SERVER (AZ-801) | 5 |
| 5 | 15 | APPLIANCE PARA ARMAZENAMENTO DE BACKUP | 2 |
| 16 | TREINAMENTO - APPLIANCE PARA ARMAZENAMENTO DE BACKUP | 3 |
| 6 | 17 | SOLUÇÃO DE BALANCEAMENTO DE CARGA E SEGURANÇA PARA APLICAÇÕES WEB | 2 |
| 18 | TREINAMENTO - SOLUÇÃO DE BALANCEAMENTO DE CARGA E SEGURANÇA PARA APLICAÇÕES WEB | 3 |
| 7 | 19 | LICENÇAS COMMVAULT PARA BACKUP DO MICROSOFT365 | 2500 |
| 8 | 20 | CAGE PARA DISCOS (BACKPLANE/ DRIVE CAGE) | 3 |
| 21 | CONTROLADOR MODULAR HPE SMART ARRAY P816I-A SR GEN10 | 3 |
| 22 | CAPACITORES HÍBRIDOS | 3 |
| 23 | DISCOS SAS HDD | 27 |
| 24 | DISCOS SAS SSD | 12 |
| 25 | SERVIÇO DE IMPLEMENTAÇÃO/INSTALAÇÃO | 3 |

1. **FORMATAÇÃO DA PROPOSTA DE PREÇOS**

A formatação da proposta de preços para a proposta deve seguir conforme a tabela abaixo:

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **LOTE** | **ITEM** | **QTDE** | **DESCRIÇÃO** | **VALOR**  **UNITÁRIO** | **VALOR**  **TOTAL** |
| 1 | 1 | 32 |  |  |  |
| 2 | 32 |  |  |  |
| 3 | 1 |  |  |  |
| 2 | 4 | 6 |  |  |  |
| 5 | 6 |  |  |  |
| 6 | 6 |  |  |  |
| 7 | 500 |  |  |  |
| 8 | 7 |  |  |  |
| 3 | 9 | 3 |  |  |  |
| 10 | 3 |  |  |  |
| 11 | 3 |  |  |  |
| 12 | 3 |  |  |  |
| 4 | 13 | 5 |  |  |  |
| 14 | 5 |  |  |  |
| 5 | 15 | 2 |  |  |  |
| 16 | 3 |  |  |  |
| 6 | 17 | 2 |  |  |  |
| 18 | 3 |  |  |  |
| 7 | 19 | 2500 |  |  |  |
| 8 | 20 | 3 |  |  |  |
| 21 | 3 |  |  |  |
| 22 | 3 |  |  |  |
| 23 | 27 |  |  |  |
| 24 | 12 |  |  |  |
| 25 | 3 |  |  |  |