

## **PREGÃO ELETRÔNICO EDITAL Nº 1204/2022.**

A **FUNDAÇÃO UNIVERSIDADE DO ESTADO DE SANTA CATARINA**, com sede na Av. Madre Benvenuta, nº 2007, Itacorubi, Florianópolis/SC, inscrita no CNPJ sob o nº 83.891.283/0001-36, por intermédio da Coordenadoria de Compras e Licitações da Reitoria, torna público que fará realizar licitação na modalidade Pregão Eletrônico, com critério de julgamento de menor preço por lote, para selecionar proposta objetivando o **REGISTRO DE PREÇOS**, nos termos da Lei Federal nº 10.520, de 17 de julho de 2002, Lei Estadual nº 12.337, de 05 de julho de 2002, com aplicação subsidiária da Lei Federal nº 8.666, de 21 de junho de 1993, Lei Complementar nº 123, de 14 de dezembro de 2006, Decreto Estadual nº 2.617, de 16 de setembro de 2009, alterações posteriores, e demais normas legais federais e estaduais vigentes.

**OBJETO: AQUISIÇÃO DE DISPOSITIVO APPLIANCE PARA ARMAZENAMENTO DE BACKUP, SEGURANÇA WEB, LICENÇAS VMWARE, REDHAT, COMMVAULT, SERVIÇOS ESPECIALIZADOS DE IMPLANTAÇÃO DE REDHAT, VMWARE E TREINAMENTOS MICROSOFT, VMWARE E REDHAT**, conforme especificações constantes do **Anexo I e II**.

**LOTE 4 DO PROCESSO É EXCLUSIVO PARA MICROEMPRESAS E EMPRESAS DE PEQUENO PORTE.**

### **FORMALIZAÇÃO DE CONSULTAS:**

site: <http://e-lic.sc.gov.br/>

e-mail: [licita@udesc.br](mailto:licita@udesc.br)

### **1 – DISPOSIÇÕES PRELIMINARES**

**1.1 – Envio de proposta: a partir das 14h do dia 03/10/2022.**

**1.2 – Abertura da sessão: a partir das 14h do dia 18/10/2022.**

**1.3 – Início da disputa: a partir das 14h15min do dia 18/10/2022.**

**1.4 – O pregão eletrônico será realizado via Sistema Integrado de Licitações do Estado de Santa Catarina (LIC), módulo eletrônico (e-LIC, <http://e-lic.sc.gov.br/>).**

**1.5 – Os trabalhos serão conduzidos por servidores da Udesc, denominados pregoeiro e equipe de apoio, conforme atribuições normatizadas pela Resolução nº 060/2010 - Consuni.**

**1.6 – Todas as referências de tempo no Edital, no Aviso e durante a sessão pública observarão obrigatoriamente o horário de Brasília – DF.**

**1.7 – Os documentos relacionados a seguir fazem parte integrante desta licitação:**

**Anexo I – Termo de Referência;**

**Anexo II – Quadro de Quantitativo(s) e Especificação(ões) Mínima(s) do(s) Item(s);**

**Anexo III – Minuta da Ata de Registro de Preços;**

**Anexo IV – Minuta de Contrato;**

**Anexo V – Modelo de Autorização de Fornecimento/Ordem de Serviço;**

**Anexo VI – Informações da empresa vencedora para contratação**

### **2 – DA LICITAÇÃO**

**2.1 – A presente licitação destina-se a selecionar proposta(s) objetivando o **REGISTRO DE PREÇOS** para futura e eventual aquisição/contratação, conforme Anexo I e Anexo II deste edital.**

**2.1.1 – As quantidades licitadas e informadas no Anexo II são **estimativas**, podendo a contratante requisitar conforme a efetiva necessidade, respeitando-se os limites estabelecidos pela legislação.**

**2.2 – Do Convênio ICMS nº 26/03**

**2.2.1 – De acordo com o Convênio ICMS nº 26/03, aprovado pelo CONFAZ - Conselho Nacional de Política Fazendária, o benefício da isenção do ICMS às empresas catarinenses está condicionado ao desconto no preço ao valor equivalente ao imposto dispensado e a indicação do valor do desconto no**

respectivo documento fiscal de venda ou prestação de serviços; e à comprovação de inexistência de similar produzido no país, na hipótese de qualquer operação com mercadorias importadas do exterior, conforme previsto no parágrafo 1º da Cláusula Primeira do Convênio CONFAZ nº 26/2003, ficando ressalvadas as hipóteses em que a isenção mencionada não se aplica, nos termos previstos no Decreto Estadual nº 255, de 21/05/2003.

**2.2.2** - Nos termos do Convênio ICMS 26/03, por se tratar de operação interna relativa à aquisição de bens, as licitantes beneficiadas com a respectiva isenção fiscal devem apresentar as suas propostas de preços já com o valor líquido, ou seja, sem a carga tributária do ICMS.

**2.2.3** - Nos casos em que for aplicável a isenção do ICMS, o licitante deverá, obrigatoriamente, informar a respectiva alíquota via comunicação "CHAT", caso seja o primeiro colocado, depois de encerrada a disputa de lances.

**2.2.4** - A isenção supracitada não se aplica a licitante vencedora, quando:

- a) dispensa de licitação nos termos do art. 24, inciso II, da Lei Federal nº 8.666, de 21 de junho de 1993;
- b) saída promovida por contribuinte enquadrado no simples nacional;
- c) saída de bens ou mercadorias sujeitas ao regime de substituição tributária;

**2.2.5** – Eventuais dúvidas quanto ao benefício citado podem ser dirimidas junto à qualquer das Gerências Regionais da Fazenda Estadual – GERG, da Diretoria de Administração Tributária – DIAT, da Secretaria de Estado da Fazenda ou, ainda, no site [www.sef.sc.gov.br](http://www.sef.sc.gov.br);

### **2.3 – Da Execução da Licitação**

**2.3.1** – O processamento da licitação será pela Udesc na qualidade de Órgão Gerenciador, destinando-se o objeto licitado a atender as necessidades da Universidade.

**2.4** Da Lei Geral de Proteção de Dados - LGPD, as partes devem acordar o seguinte:

**I** – A UDESC e a licitante vencedora declaram que tem ciência da existência da Lei nº 13.709/2018 (Lei Geral de Proteção de Dados - LGPD) e se comprometem a adequar todos os procedimentos internos ao disposto na legislação, com o intuito de proteger os dados pessoais que lhe forem repassados, cumprindo, a todo momento, as normas de proteção de dados pessoais, jamais colocando, por seus atos ou por sua omissão, em situação de violação de tais regras.

**II** – A UDESC e a licitante vencedora se comprometem no sentido de que somente poderão tratar dados pessoais dos usuários dos serviços contratados, nos limites e finalidades exclusivas do cumprimento de suas obrigações com base na presente avença/instrumento e jamais para qualquer outra finalidade.

**III** – A UDESC e a licitante vencedora assumem o compromisso de confidencialidade e de não compartilhar e/ou garantir acesso aos dados pessoais, que detenha por força do presente contrato, sendo, em regra, vedada a transferência das informações a outras pessoas físicas ou jurídicas, salvo aquelas decorrentes de obrigações legais ou para viabilizar o cumprimento do próprio contrato; se a solicitação for realizada por autoridade de proteção de dados, deverá haver deliberação conjunta sobre tal pedido e suas decorrências.

**IV** - A UDESC e a licitante vencedora ficam obrigadas a denunciar eventual incidente de acessos não autorizados aos dados pessoais, situações acidentais ou ilícitas de destruição, perda, alteração, comunicação ou qualquer forma de tratamento inadequado ou ilícito, bem como adotar as providências dispostas no art. 48 da Lei Geral de Proteção de Dados Pessoais.

### **2.5 – Do acordo anticorrupção:**

**2.5.1** – De acordo com a Instrução Normativa CGE/SEA Nº 1 DE 26/03/2020, as Partes contratante e contratada:

**I** - Declaram que têm conhecimento das normas previstas na legislação sobre anticorrupção, entre as quais nas Leis nºs 8.429/1992 e 12.846/2013, seus regulamentos e eventuais outras aplicáveis;

**II** - Comprometem-se em não adotar práticas ou procedimentos que se enquadrem nas hipóteses previstas nas leis e regulamentos mencionados no inciso acima e se comprometem em exigir o mesmo pelos terceiros por elas contratados;

**III** - Comprometem-se em notificar à Controladoria-Geral do Estado qualquer irregularidade que tiverem conhecimento acerca da execução deste contrato;

**IV** - Declaram que têm ciência que a violação de qualquer das obrigações previstas na Instrução Normativa, além de outras, é causa para a rescisão unilateral do contrato, sem prejuízo da cobrança das perdas e danos, inclusive danos potenciais, causados à parte inocente e das multas pactuadas.

### **3 – DAS CONDIÇÕES DE PARTICIPAÇÃO**

**3.1** – Poderão participar desta licitação as empresas interessadas que atenderem às exigências estabelecidas neste Edital.

**3.2** – Não será admitida a participação de:

**3.2.1** – Empresas punidas com o impedimento do direito de licitar ou contratar com a Administração do Estado de Santa Catarina – SEA, durante o prazo estabelecido para a penalidade;

**3.2.2** – Empresas declaradas inidôneas para licitar ou contratar com a Administração Pública;

**3.2.3** – Empresas cujos diretores, gerentes, sócios e empregados sejam servidores da Udesc.

**3.3** – A participação na licitação implica automaticamente na aceitação integral e irretratável do edital e seus anexos, a observância dos preceitos legais e regulamentos em vigor; e a responsabilidade pela fidelidade e legitimidade das informações e dos documentos apresentados nesta licitação.

**3.4** – O e-mail servirá para comunicados e notificações relacionados ao procedimento licitatório devendo-se considerar como data de recebimento a data de envio da comunicação pela Udesc.

**3.4.1** – Será considerado e-mail cadastrado o informado no sistema E-lic e/ou o informado no Anexo VI;

### **4 – DO CREDENCIAMENTO PARA PARTICIPAR DO CERTAME**

**4.1** – O interessado em participar do pregão eletrônico deve dispor de chave de identificação e senha pessoal e intransferíveis emitidas pelo Cadastro Geral de Fornecedores do Estado de Santa Catarina.

**4.1.1** – Os interessados deverão estar previamente qualificados para fornecimento do objeto referente ao grupo-classe indicado no **Anexo II**.

**4.1.2** – O procedimento para inscrição e alterações do Cadastro encontra-se disponível no site do Portal de Compras, pelo endereço <http://portaldecompras.sc.gov.br>.

**4.2** – A licitante credenciada responsabiliza-se legalmente, independente da fase do certame, por seus atos praticados e por declarações falsas. Ainda, assume como verdadeiras suas propostas/lances, presumindo-se a legitimidade de seu representante para realização das transações no pregão eletrônico, já que é a única responsável pelo sigilo da senha.

### **5 – PARTICIPAÇÃO**

**5.1** – A participação no Pregão Eletrônico se dará por meio do encaminhamento da proposta eletrônica de preços, por meio do sistema eletrônico, observada data e horário limite estabelecidos.

**5.2** – Como requisito para a participação no Pregão, o licitante deverá manifestar, em campo próprio do sistema eletrônico, o pleno conhecimento e atendimento às exigências previstas no Edital.

**5.3** – Quando o licitante for beneficiário da Lei Complementar nº 123, de 14 de dezembro de 2006, deverá manifestar o pleno conhecimento em campo próprio do sistema eletrônico.

**5.3.1** – A declaração falsa relativa ao cumprimento dos requisitos de habilitação, proposta e enquadramento da empresa sujeitará o licitante às sanções previstas na legislação vigente.

**5.4** – Caberá à licitante acompanhar a sessão pública do Pregão, ficando responsável pela perda de negócios diante da inobservância de mensagens do sistema ou de sua desconexão.

### **6 – DA PROPOSTA DE PREÇOS**

**6.1** – Da proposta on-line:

**6.1.1** – Após a divulgação do edital, os licitantes deverão encaminhar proposta e, se for o caso, o respectivo anexo, até a data e hora marcadas para abertura da sessão, exclusivamente por meio do sistema eletrônico, quando, então, não poderá ser mais retirada ou substituída.

**6.1.2** – Os licitantes receberão, por e-mail, comprovante de recebimento das suas propostas eletrônicas enviadas, com a indicação do dia e respectivo horário de registro.

**6.1.3** – A proposta on-line, para cada item, deverá ser preenchida, obrigatoriamente, conforme as especificações abaixo, sob pena de desclassificação:

**a)** Indicando o valor unitário de cada item, expresso em reais, com no máximo 02 (duas) casas decimais, no campo “valor da proposta”;

**b)** Indicando a Marca/Modelo/Procedência do objeto cotado no campo correspondente a cada item, somente as informações solicitadas pelo sistema para cada item/lote.

**6.1.4** – As licitantes deverão ofertar preços para todos os itens do lote cotado, sob pena de Desclassificação.

**6.1.5** – Qualquer documentação que identifique a licitante deve ser inserida como anexo ou enviado por e-mail, conforme determinação do Pregoeiro, somente após à fase de lances

**6.1.6** – Nos preços cotados devem estar inclusos todos os custos relacionados com a remuneração e encargos sociais e outros, pertinentes ao fornecimento do objeto, bem como taxas, impostos, fretes, e demais despesas diretas e indiretas incidentes sobre o mesmo.

**6.1.7** – A proposta entregue não poderá ter prazo de validade inferior a 60 (sessenta) dias, sendo este o prazo considerado em caso de omissão.

**6.1.8** – O prazo de entrega do(s) produto(s) cotado(s) não poderá ser superior ao estabelecido no Anexo I, contados da data do recebimento da Autorização de Fornecimento/Contrato.

#### **6.1.9 – FORMATAÇÃO DA PROPOSTA DE PREÇO DO VENCEDOR:**

**6.1.9.1** - 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.

**6.1.9.2** - Todos itens deste edital deverão constar no portfólio de produtos do fabricante, sendo que 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;

**6.1.9.3** - Deverá ser fornecido, obrigatoriamente, no formato abaixo, um documento que faça a associação do item especificado no Anexo I 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: <a href="http://www.fabricante.com/zzzzz">www.fabricante.com/zzzzz</a>

**6.1.9.4** - A comprovação para atendimento as especificações dos itens, caso solicitado, deverá ser enviada por meio eletrônico, pelo endereço [licita@udesc.br](mailto:licita@udesc.br), em até 1 (um) dia útil a contar da data da convocação do pregoeiro, somente da empresa melhor classificada no lote.

**6.1.9.5** - Será desclassificada no item, a proposta da licitante vencedora que não atender (no prazo de 1 (um) dia útil, a contar da data da convocação do pregoeiro para a apresentação dos documentos), as exigências prescritas neste Edital, ou estejam fora das exigências previstas, estando sujeita às penalidades previstas.

**6.1.9.6** - Enquanto não houver licitante classificada, no que tange às exigências deste item, as demais licitantes serão convocadas para apresentarem, conforme o caso, a documentação, em até 1 (um) dia útil a contar da convocação, pela ordem de classificação na etapa de lances, sucessivamente, até se

obter uma licitante classificada, desde que o lance ofertado e registrado por esta, seja igual ou inferior ao limite estabelecido pelo valor de referência, e, caso este seja ultrapassado, os itens resultarão frustrados.

**6.1.9.7 - A Contratante reserva-se o direito de solicitar, também, na entrega do objeto, os documentos mencionados neste item.**

## **6.2 – Da proposta on-line readequada:**

**6.2.1 –** Quando houver cotação de proposta por lote, a vencedora do lote deverá readequar sua proposta no próprio e-Lic, após a adjudicação, com os respectivos valores unitários readequados ao valor total do lance vencedor, no prazo de 60 (sessenta) minutos, contados a partir da convocação do pregoeiro, podendo este prazo ser prorrogado, a critério da Administração.

**6.2.2 –** Quando por lote, o valor unitário readequado não poderá ser superior àquele oferecido na primeira proposta e nem superior ao preço máximo dos itens, conforme Anexo II.

**6.2.3 –** A empresa vencedora deverá enviar por e-mail as informações constantes do Anexo VI, no prazo de 1 (um) dia útil, contado a partir do encerramento da sessão.

**6.2.3.1 –** O endereço eletrônico (e-mail) fornecido no Anexo VI (Informações da Empresa Vencedora para Contratação) será considerado como legítimo canal de comunicação entre a UDESC e a licitante para quaisquer fins.

**6.2.3.2 –** A verificação rotineira das mensagens encaminhadas a tal e-mail é de inteira responsabilidade da licitante, não podendo invocar qualquer falha ocorrida em tal sistema - ainda que por fato imputável a terceiro - ou a negligência na sua checagem como razão para eximir-se de obrigação eventualmente imposta em tais comunicações, especialmente em relação ao cumprimento de prazos que venham a ser estipulados pela Administração.

**6.2.3.3 –** É de responsabilidade exclusiva da licitante manter atualizado o endereço eletrônico a que se refere o item 6.2.3.1. Eventual troca desse deverá ser imediatamente comunicado à UDESC pelo e-mail da primeira página deste Edital.

## **7 – DA ABERTURA DA SESSÃO E ETAPA DE LANCES**

**7.1 –** Iniciada a sessão pública do Pregão, esta não será suspensa ou transferida, salvo motivo excepcional assim caracterizado pelo Pregoeiro.

**7.1.1 –** Verificando-se o adiamento da sessão pública do Pregão, o Pregoeiro determinará nova data para continuação dos trabalhos, ficando intimadas as licitantes.

**7.1.2 –** O Pregoeiro poderá interromper a sessão, temporariamente, para determinar alguma providência administrativa para o bom andamento dos trabalhos (diligências).

**7.1.3 –** No caso de desconexão do Pregoeiro, no decorrer dos lances, se o sistema permanecer acessível aos licitantes, os lances continuarão sendo recebidos, sem prejuízo dos atos realizados.

**7.1.4 –** Quando a desconexão do Pregoeiro persistir por tempo mais de dez minutos, a sessão será suspensa e reiniciada somente após comunicação aos participantes por e-mail do cadastro no e-Lic.

**7.2 –** A partir do horário previsto no Edital terá início a sessão pública do Pregão com a abertura das propostas de preços recebidas, passando o Pregoeiro a avaliar a aceitabilidade das propostas.

**7.3 –** A desclassificação de proposta será sempre fundamentada e registrada no Sistema, com acompanhamento em tempo real por todos os participantes.

**7.3.1 –** O fornecedor que tiver a sua proposta desclassificada, terá o tempo de 3 (três) minutos para solicitar reconsideração.

**7.4 –** O Sistema ordenará automaticamente, fazendo sorteio quando tiver valores iguais, as propostas classificadas pelo pregoeiro, sendo que somente estas participarão da fase de lance.

**7.5 –** Aberta a etapa de lances, não serão aceitos dois ou mais lances de mesmo valor, prevalecendo aquele que for recebido e registrado primeiro.

**7.5.1 –** Os licitantes deverão encaminhar lances somente por meio do sistema eletrônico, sendo imediatamente computado e visualizado seu horário de registro e valor no link “histórico de lances”.

**7.5.2** – Somente o licitante de menor lance dentre os ofertados, e enquanto mantiver esta situação, visualiza em tempo real o ícone “troféu”.

**7.5.3** – Os lances aceitos ofertados serão no valor unitário do item (quando da cotação por item) ou valor total do lote (quando da cotação por lote).

**7.5.4** – Só serão aceitos lances cujos valores forem inferiores ao último lance da própria licitante, registrado anteriormente no sistema.

**7.5.5** – Durante o transcurso da sessão pública, os participantes serão informados, em tempo real, do valor do menor lance registrado. O sistema não identificará os autores dos lances.

**7.5.6** – A etapa de lances da sessão pública que terá o tempo de duração mínima de 5 (cinco) minutos, será encerrada mediante aviso de fechamento iminente dos lances, emitido pelo sistema eletrônico, após o que transcorrerá período de tempo de até 30 (trinta) minutos, aleatoriamente determinado também pelo sistema, findo o qual, será automaticamente encerrada a etapa de lances.

**7.6.** – Depois de encerrados os itens/lotes, encerrar-se-á a etapa da disputa e o Sistema emitirá aviso no Chat iniciando as fases de negociação, aceitabilidade e habilitação.

**7.7** – O Sistema, automaticamente, verificará os requisitos para a aplicação da Lei Complementar nº 123/2006. Na sequência o pregoeiro poderá negociar a redução dos preços com o proponente.

**7.7.1** – O pregoeiro decidirá sobre a aceitação dos preços, observado o critério de julgamento, não se admitindo negociar condições diferentes daquelas previstas no edital.

**7.7.2** – A negociação será realizada por meio do Sistema de troca de mensagens (Chat), podendo ser acompanhada pelos demais licitantes.

**7.8** – Ocorrendo o empate será assegurada, como critério de desempate, preferência de contratação para as MicroEmpresas (ME) e Empresas de Pequeno Porte (EPP).

**7.8.1** – Entende-se por empate aquelas situações em que as propostas/lances apresentados pelas ME/EPP sejam iguais ou até 5% (cinco por cento) superiores à proposta/lance mais bem classificada;

**7.8.2** – Ocorrendo o empate, proceder-se-á, automaticamente, da seguinte forma:

- a)** o sistema aplicará o benefício, quando houver empresas dentro das condições previstas na lei.
- b)** o sistema convocará a ME/EPP mais bem classificada para apresentar nova proposta inferior àquela considerada vencedora do certame (no prazo máximo de 5 (cinco) minutos sob pena de preclusão), situação em que será adjudicado em seu favor o objeto licitado;
- c)** não ocorrendo a contratação da ME/EPP, serão convocadas as remanescentes que porventura se enquadrem como ME/EPP na ordem classificatória, para o exercício do mesmo direito;
- d)** no caso de equivalência dos valores apresentados pelas ME/EPP que se encontrem nos intervalos da Lei Complementar, será realizado sorteio automático entre elas para que se identifique aquela que primeiro poderá enviar melhor oferta.

**7.9** – O disposto no subitem 7.8 somente se aplicará quando a melhor oferta inicial não tiver sido apresentada por ME/EPP.

**7.10** – Na hipótese da não-contratação nos termos previstos no subitem 7.8, o objeto licitado será adjudicado em favor da proposta originalmente vencedora do certame.

**7.11** – Encerrada a recepção de lances dos beneficiários da Lei Complementar nº 123, quando houver, o Pregoeiro poderá, antes de anunciar o vencedor, encaminhar, pelo sistema eletrônico, contraproposta diretamente à proponente que tenha apresentado o lance de menor preço, para que seja obtido preço melhor, bem como decidir sobre sua aceitação.

**7.12** – O sistema anunciará a licitante vencedora após o encerramento da etapa de lances da sessão pública ou, quando for o caso, após negociação e decisão previstas nos itens anteriores.

**7.13** – Encerrada a etapa de lances da sessão pública, a licitante detentora da melhor oferta deverá atender as exigências de habilitação previstas neste Edital.

**7.14** – Se a proposta ou o lance de menor valor não for aceitável, ou se a licitante desatender às exigências habilitatórias, o Pregoeiro examinará a proposta ou o lance subsequente, verificando a sua



compatibilidade e a habilitação do participante, na ordem de classificação, e assim sucessivamente, até a apuração de uma proposta ou lance que atenda o Edital.

## **8 – DOS DOCUMENTOS DE HABILITAÇÃO**

**8.1** – Será verificada a situação de regularidade da licitante detentora da melhor oferta, da seguinte forma:

**8.1.1** – Consulta do Certificado de Cadastro de Fornecedores(CCF), pertinente ao grupo-classe objeto desta licitação.

**8.1.1.1** – O CCF que apresentar Situação Cadastral com alguma restrição nos documentos por ele abrangidos, o pregoeiro ou equipe de apoio comunicará por meio eletrônico, a obrigatoriedade do encaminhamento de documento hábil correspondente no prazo de até 30 minutos.

**8.1.1.2** – Para suprir a documentação vencida, no que diz respeito à comprovação de regularidade fiscal e trabalhista, relacionada no CCF, o Pregoeiro poderá verificar nos sites dos emissores de certidões, o documento hábil correspondente, constituindo meio legal de prova.

**8.2** – A regularidade fiscal das ME/EPP's, que apresentem restrição (documento vencido) no CCF, poderá ser comprovada no prazo de 5 (cinco) dias úteis do encerramento da sessão, prorrogáveis por igual período, a critério da Administração Pública, para a regularização da documentação e emissão de eventuais certidões negativas ou positivas com efeito de certidão negativa.

**8.2.1** – A não-regularização da documentação, no prazo estabelecido, implicará na decadência do direito da ME/EPP à contratação, sem prejuízo das sanções administrativas cabíveis, sendo facultada à Administração convocar os licitantes remanescentes, na ordem de classificação, para a assinatura do Contrato/ARP ou revogar a licitação.

**8.3** - Empresas em recuperação judicial ou extrajudicial ou cuja falência tenha sido declarada, que se encontram sob concurso de credores ou em dissolução ou em liquidação, com plano de recuperação deferido e homologado judicialmente, que apresentarem certidão positiva deverão apresentar ainda certidão de aptidão financeira emitida pela instância judicial competente, que ateste que a interessada está apta econômica e financeiramente a participar de licitação nos termos das Leis 8.666/1993 e 11.101/2005.

**8.3.1** – Comprovação do acolhimento judicial do plano de recuperação, nos termos do art. 58 da Lei nº 11.101/05, em caso de recuperação judicial; ou da homologação judicial do plano de recuperação, no caso de recuperação extrajudicial.

**8.3.2** – Os licitantes que se encontrarem em recuperação judicial ou extrajudicial devem demonstrar todos os demais requisitos para habilitação econômico-financeira, como qualquer licitante.

**8.4** – O pregoeiro fará, durante a fase de habilitação, a verificação por meio de consulta online:

**8.4.1** – Da existência de registros impeditivos da contratação no Cadastro Nacional de Empresas Inidôneas e Suspensas (CEIS) ([www.transparencia.gov.br](http://www.transparencia.gov.br));

**8.4.2** – Da existência de registros impeditivos da contratação no Cadastro Nacional de Condenações Cíveis por Ato de Improbidade Administrativa mantido pelo Conselho Nacional de Justiça ([www.cnj.jus.br / improbidade\\_adm/consultar\\_requerido.php](http://www.cnj.jus.br/improbidade_adm/consultar_requerido.php)).

## **9 – JULGAMENTO**

**9.1** – Será considerada primeira classificada, a proposta que, obedecendo às condições, especificações e procedimentos deste edital, apresentar o **menor preço por lote**, conforme **Anexo II**.

**9.2** – Quando na especificação do objeto forem estabelecidas medidas aproximadas, no julgamento serão adotadas as variações admitidas pela ABNT ou, na ausência de parâmetros oficiais, o Pregoeiro adotará critérios próprios, justificadamente, limitados em qualquer hipótese à margem superior ou inferior de 10% (dez por cento).

**9.3** – Serão desclassificadas as propostas:

- a) que não atenderem às exigências do ato convocatório da licitação;
- b) que conflitem com a legislação em vigor;
- c) a pedido da licitante, devidamente justificada, analisada e aceita pelo Pregoeiro;
- d) que não cotarem marca/modelo conforme solicitado pelo sistema e-Lic.

**9.4** – Não serão consideradas, para efeitos de julgamento, quaisquer vantagens não previstas no edital.

**9.5** – No julgamento da habilitação e das propostas, o pregoeiro poderá sanar erros ou falhas que não alterem a substância das propostas, dos documentos e sua validade jurídica, mediante despacho fundamentado, registrado em ata via *chat* e acessível a todos, atribuindo-lhes validade e eficácia para fins de habilitação e classificação.

## **10 – DAS IMPUGNAÇÕES E DOS RECURSOS ADMINISTRATIVOS**

**10.1** – Qualquer pessoa até dois dias úteis antes da abertura da sessão poderá impugnar o Edital por meio do Sistema eletrônico, no espaço destinado ao “Registro de Impugnação ao Edital”.

**10.1.1** – Fornecedores cadastrados podem optar por registrar a impugnação efetuando o login, acessando o processo eletrônico, botão “Impugnação”.

**10.1.2** – Excepcionalmente, a impugnação poderá ser realizada pelo **e-mail**: [licita@udesc.br](mailto:licita@udesc.br).

**10.1.3** – O Sistema permite, após salvar as informações iniciais e emitir o número de registro da impugnação, inserir Anexos na aba correspondente.

**10.2** – Declarado o vencedor, qualquer licitante poderá manifestar sua intenção de recorrer, de forma motivada no prazo de 30 minutos, **em campo próprio do Sistema**, sendo-lhe concedido o prazo de 03 (três) dias para a apresentação das razões do recurso, ficando os demais licitantes, desde logo, intimados a apresentar contrarrazões em igual número de dias, que começarão a correr do término do prazo da recorrente, sendo-lhes assegurada vista dos autos.

**10.2.1** – O Sistema permite, após salvar as informações iniciais e emitir o número de registro do recurso, inserir Anexos antes de fechar a janela.

**10.2.2** – Os recursos devem ser registrados no Sistema.

**10.2.3** – Não serão conhecidos os recursos apresentados fora do prazo legal, contados no sistema.

**10.2.4** – Decididos os recursos e constatada a regularidade dos atos praticados, a autoridade competente adjudicará o objeto e homologará o procedimento licitatório.

## **11 – DO REGISTRO DE PREÇOS**

**11.1** - Os atos de homologação e assinatura da Ata de Registro de Preços (ARP) desta licitação serão de competência do Magnífico Sr. Reitor;

**11.2** – Homologado o procedimento licitatório, a licitante vencedora será convocada, por e-mail, para assinatura da Ata de Registro de Preços (ARP).

**11.2.1** – A assinatura da ARP se dará de forma eletrônica, mediante uso de certificação digital ICP Brasil, no prazo de até 1 (um) dia útil da convocação, por meio do sistema SGPe.

**11.2.2** – Orientações sobre como assinar documentos no Sistema do Estado podem ser acessadas por meio do site: [https://sgpe.sea.sc.gov.br/capdoc/pergunta\\_frequente/novo-portal-de-processos-digitais/](https://sgpe.sea.sc.gov.br/capdoc/pergunta_frequente/novo-portal-de-processos-digitais/)

**11.3** - O prazo de validade da ARP será de 12 (doze) meses contadas da data de publicação do extrato no Diário Oficial do Estado de Santa Catarina (DOE/SC);

**11.3.1** - Dentro do prazo de vigência da ARP, as licitantes registradas ficarão obrigadas ao fornecimento, desde que obedecidas às condições deste Edital e a manter todas as condições de habilitação exigidas neste Edital;

**11.4** - No caso do fornecedor primeiro classificado, depois de convocado, não atender as condições de habilitação, não comparecer ou recusar-se a assinar a Ata de Registro de Preços, responderá na forma da legislação vigente e a UDESC registrará os demais licitantes, respeitada a ordem de classificação;



**11.5** – Os fornecedores classificados, subsequentemente, poderão registrar os seus preços na ARP, desde que aceitem fornecer ao preço do detentor do preço registrado;

**11.6** - As aquisições obedecerão à conveniência e às necessidades da Udesc e será procedida pela emissão de Autorização de Fornecimento (AF) ou Contrato;

**11.6.1** – A UDESC encaminhará ao licitante registrado a AF, conforme Anexo V, via e-mail com aviso de recebimento, devendo atender ao fornecimento no prazo e no local de entrega estabelecido;

**11.6.2** – Quando necessário a emissão de contrato, conforme minuta Anexo IV, será solicitada a assinatura via sistema SGPe no prazo de 03 dias úteis.

**11.7** - A existência de preços registrados não obriga os órgãos: gerenciador e participantes deste Registro de Preços a efetivar as contratações que dele poderão advir, ficando-lhes facultada a adoção de outros meios para a contratação, respeitado a legislação relativa às licitações, sendo assegurado ao detentor do Preço Registrado a preferência em igualdade de condições;

**11.7.1** - O exercício de preferência dar-se-á caso os órgãos participantes optem por contratar o fornecimento através de licitação específica e o preço encontrado for igual ou superior ao registrado;

**11.8** – A ARP, durante sua vigência, poderá ser utilizada por qualquer Órgão Estadual ou Municipal que não tenha participado do certame licitatório (carona), mediante anuência da Unidade Gerenciadora e do licitante registrado, conforme Decreto Estadual 558, de 14 de Abril de 2020.

**11.8.1.** De acordo com o DECRETO Nº 558, DE 14 DE ABRIL DE 2020, as aquisições adicionais não poderão exceder, por órgão, a 50% (cinquenta por cento) dos quantitativos dos itens registrados na ARP, nem tampouco poderá exceder, na totalidade, ao dobro do quantitativo de cada item registrado na ARP, independentemente do número de órgãos não participantes aderentes.

## **12 – DO PAGAMENTO**

**12.1** – A Udesc efetuará o pagamento em até 30 (trinta) dias após o recebimento e aceite do material com a respectiva Nota Fiscal/Fatura ou documento legalmente equivalente, observado o cumprimento integral das disposições contidas neste edital;

**12.1.1** - Caso o vencimento do prazo de pagamento da Nota Fiscal/Fatura ocorra fora do calendário semanal, o pagamento será efetuado na próxima data do calendário, imediatamente posterior ao vencimento, não incidindo qualquer compensação financeira neste período;

**12.2** - A fornecedora deverá apresentar, obrigatoriamente, juntamente com a Nota Fiscal/Fatura, as Certidões Negativas de Débitos Federal, Estadual, Municipal, FGTS e Trabalhista;

**12.3** - A empresa deverá mencionar na respectiva Nota Fiscal/Fatura informações sobre o produto, tais como: fabricante/marca/modelo/procedência/apresentação/nome comercial/referência/número ou Certificado de Registro do Produto junto ao ente fiscalizador (quando cabível)/descrição exaustiva que permita à Administração identificá-lo e avaliar se o produto atende ou não às especificações mínimas requeridas. Indispensável ainda informar os números do Contrato, Licitação e empenho;

**12.4** – A empresa deverá mencionar na Nota Fiscal/Fatura os dados bancários para pagamento, como: número do banco, número da agência com dígito, número da conta corrente com dígito.

## **13 – DAS PENALIDADES E SANÇÕES:**

**13.1** - As empresas que não cumprirem as obrigações assumidas na fase licitatória e/ou de execução do Contrato/ARP estão sujeitas às seguintes sanções:

a) advertência;

b) multa;

c) impedimento de licitar e contratar com o Estado de Santa Catarina; e

d) declaração de inidoneidade para licitar com a Administração Pública;

**13.2** - A advertência será emitida quando o contratado descumprir qualquer obrigação;

**13.3** - A multa será imposta à contratada pelo atraso injustificado na entrega ou execução do Contrato/ARP, de acordo com as alíquotas a seguir:

- a) 0,33 % (zero, trinta e três por cento) por dia de atraso na entrega do objeto ou execução de serviços, sobre o valor correspondente à parte inadimplente, até o limite de 9,9% (nove, nove por cento);
- b) 10 % (dez por cento) em caso de não entrega do objeto ou não conclusão do serviço ou rescisão do contrato por culpa da contratada, calculado sobre a parte inadimplente;
- c) até 20% (vinte por cento) sobre o valor do Contrato/ARP, pelo descumprimento de qualquer cláusula do Contrato/ARP, exceto prazo de entrega;

**13.3.1** - O valor da multa e/ou custas de depósito será deduzido dos créditos ou garantias da empresa, ou cobrado administrativa ou judicialmente;

**13.3.2** - Sempre que a multa ultrapassar os créditos da contratada e/ou garantias, o valor excedente será encaminhado à cobrança extrajudicial ou judicial;

**13.3.3** - O atraso, para efeito de cálculo de multa, será contado em dias corridos, a partir do dia seguinte ao do vencimento do prazo de entrega ou execução do serviço;

**13.3.4** - A multa será aplicada quando o atraso for superior a cinco dias;

**13.3.5** - A aplicação da multa não impede que sejam aplicadas outras penalidades;

**13.4** - A penalidade de impedimento impossibilitará a participação da empresa em licitações, ficando suspenso o seu registro no Cadastro Geral de Fornecedoros/SC, de acordo com os prazos a seguir:

- a) por até 30 (trinta) dias, quando aplicada a pena de advertência emitida pela Administração e a empresa permanecer inadimplente;
- b) por até 90 (noventa) dias, quando a empresa interessada solicitar cancelamento da proposta após a abertura e antes do resultado do julgamento;
- c) por até 12 (doze) meses, quando a empresa adjudicada se recusar a receber a autorização de fornecimento ou assinar o Contrato/ARP;
- d) por até 12 (doze) meses, quando a empresa adjudicada motivar a rescisão total ou parcial da autorização de fornecimento e/ou do contrato;
- e) por até 12 (doze) meses, quando a empresa praticar atos que claramente visem à frustração dos objetivos da licitação;
- f) por até 24 (vinte e quatro) meses, quando a empresa apresentar documentos fraudulentos;
- g) por até 5 (cinco) anos quando, na modalidade de pregão, a fornecedora, que: não celebrar o contrato, deixar de entregar ou apresentar documentação falsa, ensejar o retardamento da execução de seu objeto, não mantiver a proposta, falhar ou fraudar na execução do contrato, se comportar de modo inidôneo ou cometer fraude fiscal, ficará impedida de licitar e contratar com o Estado de SC; e
- h) até a realização do pagamento, quando a empresa receber multas previstas no item anterior;

**13.4.1** - A penalidade de impedimento, publicada no Diário Oficial do Estado, implicará na suspensão da fornecedora junto ao Cadastro Geral de Fornecedoros do Estado de Santa Catarina/SEA;

**13.4.2** - O impedimento do direito de licitar poderá ser ampliada até o dobro, em caso de reincidência;

**13.5** - A declaração de inidoneidade será aplicada pelo Secretário de Estado da Administração/SEA;

**13.5.1** - A declaração de inidoneidade permanecerá em vigor enquanto perdurarem os motivos que determinaram a punibilidade ou até que seja promovida a reabilitação perante a autoridade que a aplicou;

**13.5.2** - A declaração de inidoneidade terá seus efeitos extensivos a toda Administração Pública;

**13.6** - As empresas que apresentarem documentos fraudulentos, adulterados ou falsificados, ou que por quaisquer outros meios praticarem atos irregulares ou ilegalidades para obtenção do registro no Cadastro Geral de Fornecedoros do Estado de Santa Catarina/SEA, estarão sujeitas às seguintes penalidades:

- a) a penalidade de impedimento acarretará na suspensão temporária do Certificado de Cadastro de Fornecedoros - CCF ou da obtenção do registro, por até 5 (cinco) anos dependendo da natureza e gravidade dos fatos; e
- b) declaração de inidoneidade, nos termos do artigo anterior.

**13.7** - As sanções previstas neste edital poderão também ser aplicadas às empresas ou profissionais que:

a) tenham sofrido condenação definitiva por praticarem, por meios dolosos, fraude fiscal no recolhimento de quaisquer tributos; e

b) tenham praticado atos ilícitos, visando frustrar os objetivos da licitação;

**13.8** - Compete ao Setor de Gestão de Contratos da CLC/Reitoria, após análise a indicação das penalidades deste edital, cuja aplicação dependerá da homologação da autoridade competente;

**13.9** - A interessada poderá interpor recurso contra a aplicação das penalidades deste edital, em 5 (cinco) dias úteis, a contar do recebimento da notificação, que será dirigido à autoridade competente;

**13.10** - Homologadas e publicadas as penalidades serão registradas Cadastro Geral de Fornecedores;

#### **14 – DAS DISPOSIÇÕES FINAIS**

**14.1** - Informações, impugnações e esclarecimentos sobre o edital serão protocoladas pelo interessado, acessando o pregão eletrônico, no portal de compras e-Lic, sendo que:

**14.1.1** - Para pedidos de informações e esclarecimentos, deve ser utilizada a opção “fórum” do edital;

**14.1.2** - Para pedidos de impugnação deve ser utilizada a opção “Impugnação” do edital.

**14.2** – Cópias e vistas obedecerão aos seguintes procedimentos:

**14.2.1** – Cópia deste edital e seus anexos poderá ser obtida pelos interessados, no endereço eletrônico <http://portaldecompras.sc.gov.br/> ou <https://e-lic.sc.gov.br/>

**14.2.2** – Vistas ao processo licitatório poderão ser realizadas no endereço <https://portal.sgpe.sea.sc.gov.br>, informando o nº do processo UDESC 00037084/2022.

**14.2.3** – A Udesc não se responsabiliza pelo conteúdo e autenticidade de cópias deste edital, senão aquelas que estiverem nos sites informados anteriormente.

**14.3** – É facultado ao Pregoeiro ou à autoridade superior, em qualquer fase desta licitação, promover diligência destinada a esclarecer ou complementar a instrução do processo.

**14.3.1** – As normas disciplinadoras da licitação serão sempre interpretadas em favor da ampliação da disputa entre os participantes, desde que não comprometam o interesse da Administração, a finalidade e a segurança da contratação.

**14.4** – Não será permitida a subcontratação do objeto deste edital.

**14.5** – A Udesc poderá revogar este pregão por razões de interesse público decorrente de fato superveniente, comprovado, pertinente e suficiente para justificar o ato, ou anulá-lo por ilegalidade, de ofício ou por provocação de terceiros, mediante parecer escrito e devidamente fundamentado.

**14.6** – O presente edital e seus Anexos poderão ser alterados, pela Udesc, antes de aberta a licitação, no interesse público, por sua iniciativa ou decorrente de provocação de terceiros, atendido o que estabelece o art. 21, §4º, da Lei Federal nº 8.666, de 21 de junho de 1993, bem como adiar ou prorrogar o prazo para recebimento e/ou a abertura das Propostas Eletrônicas.

**14.6.1** – Caso ocorram alterações neste edital, elas serão disponibilizadas no Portal de compras;

**14.7** – A participação na licitação implica automaticamente na aceitação integral e irretratável dos termos deste edital, a observância dos preceitos legais e regulamentos em vigor; e a responsabilidade pela fidelidade e legitimidade das informações apresentados em qualquer fase da licitação.

**14.8** – Fica eleito o Foro da Comarca da Capital do Estado de Santa Catarina, com prevalência sobre qualquer outro, para apreciação judicial de quaisquer questões resultantes deste edital.

**Florianópolis/SC, 29 de setembro de 2022.**

**DILMAR BARETTA**  
**REITOR DA FUNDAÇÃO UNIVERSIDADE DO ESTADO DE SANTA CATARINA**

**ANEXO I**  
**PREGÃO ELETRÔNICO Nº 1204/2022**

**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:

- 1.1** Licença perpétua para 01 processador, independentemente da quantidade de servidores virtuais, containers ou aplicações instalados ou gerenciados;
- 1.2** 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;
- 1.3** Serviço de subscrição e garantia de 60 meses com suporte Basic;
- 1.4** 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:

- 1.1** Licença perpétua para 01 processador, independentemente da quantidade de servidores virtuais, containers ou aplicações instalados ou gerenciados;
- 1.2** 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;
- 1.3** Serviço de subscrição e garantia de 60 meses com suporte Production;
- 1.4** 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**

- 1.1** 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;
- 1.2** Deverá ser entregue um cronograma à SETIC em até 5 (cinco) dias corridos após a realização da reunião;
- 1.3** 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;
- 1.4** 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;
- 1.5** 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:
  - 1.5.1** Levantamento do ambiente e preparação para instalação nova da solução VMware NSX;
  - 1.5.2** Design da solução;
  - 1.5.3** Instalação da solução;
  - 1.5.4** Instalação e configuração das Manager controllers;
  - 1.5.5** Instalação e configuração dos Edge Appliances;
  - 1.5.6** Configuração de Compute Managers;
  - 1.5.7** Configuração das transport zones;
  - 1.5.8** Configuração dos profiles (hosts, edge e network);
  - 1.5.9** Configuração dos Segments;
  - 1.5.10** Configuração de IP Pools;
  - 1.5.11** Configuração dos Transport Nodes;
  - 1.5.12** Configuração de roteamento T0 e/ou T1;
  - 1.5.13** Configuração integração do Distributed Firewall;

- 1.5.14** Configuração e integração entre os dois datacenters da UDESC através dos respectivos vCenters Servers, considerando as arquiteturas similares entre eles;
- 1.5.15** 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
- 1.5.16** Testes;
- 1.5.17** Liberar para uso;
- 1.6** 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:
  - 1.6.1** 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;
- 1.7** 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);
- 1.8** Documentação
  - 1.8.1** Ao término da implementação da solução, a Contratada deverá fornecer toda a documentação técnica dos softwares instalados, incluindo, mas não se limitando, a:
    - 1.8.1.1** Documentação descritiva dos produtos, com todos os componentes e softwares que perfazem a solução;
    - 1.8.1.2** 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;
- 1.9** 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:

- 1.1** Licença perpétua para 02 cores ou 4 vCPUs, independentemente da quantidade de servidores virtuais, containers ou aplicações instalados ou gerenciados;



**1.2** 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;

**1.3** Serviço de subscrição e garantia de 60 meses;

**1.4** 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:

**1.1** Licença perpétua para 02 cores ou 4 vCPUs, independentemente da quantidade de servidores virtuais, containers ou aplicações instalados ou gerenciados;

**1.2** 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;

**1.3** Serviço de subscrição e garantia de 60 meses;

**1.4** 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:

**1.1** Licença perpétua para 02 cores ou 4 vCPUs, independentemente da quantidade de servidores virtuais, containers ou aplicações instalados ou gerenciados;

**1.2** 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;

**1.3** Serviço de subscrição e garantia de 60 meses;

**1.4** 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**

- 1.1** Os serviços listados deverão ser realizados diretamente pelo fabricante da solução;
- 1.2** 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;
- 1.3** Deverá ser entregue um cronograma à SETIC em até 5 (cinco) dias corridos após a realização da reunião;
- 1.4** 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;
- 1.5** Todas 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;
- 1.6** 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:
  - 1.6.1** Instalação e configuração dos servidores;
  - 1.6.2** Instalação e configuração da ferramenta de gerência e monitoramento do ambiente e integração desta ao Active Directory da UDESC (idUDESC);
  - 1.6.3** Instalação, configuração e validação da ferramenta de provisionamento de containers;
  - 1.6.4** Instalação, configuração e validação da ferramenta de orquestração de containers;
  - 1.6.5** Criação, configuração e implantação de uma rotina de deploy de uma aplicação JAVA integrada a um repositório GIT que será fornecido pela UDESC;
  - 1.6.6** Criação, configuração e implantação de uma rotina de deploy de uma aplicação PHP integrada a um repositório GIT que será fornecido pela UDESC;
- 1.7** 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:
  - 1.7.1** 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;

**1.8** 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);

**1.9 Documentação**

**1.9.1** Ao término da implementação da solução, a Contratada deverá fornecer toda a documentação técnica dos softwares instalados, incluindo, mas não se limitando, a:

**1.9.1.1** Documentação descritiva dos produtos, com todos os componentes e softwares que perfazem a solução;

**1.9.1.2** Documentação técnica do ambiente;

**1.9.1.3** 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:

**1.1** Deverá ser ministrado por instrutor, online, estando disponível durante todo período do treinamento.

**1.2** Não serão aceitos treinamentos gravados.

**1.3** Deverá contemplar todos os itens descritos na ementa disponível em: <https://www.redhat.com/pt-br/services/training/do700-container-adoption-boot-camp>;

**1.4** Deverá ser ministrado por empresa provedora de treinamento oficial autorizada pelo respectivo fabricante;

**1.5** 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;

**1.6** 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:

- 1.1** Deverá ser ministrado por instrutor, online, estando disponível durante todo período do treinamento.
- 1.2** Não serão aceitos treinamentos gravados.
- 1.3** 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](https://mylearn.vmware.com/mgrReg/courses.cfm?ui=www_edu&a=one&id_subject=93065);
- 1.4** Deverá ser ministrado por empresa provedora de treinamento oficial autorizada pelo respectivo fabricante;
- 1.5** 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;
- 1.6** 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:

- 1.1** Deverá ser ministrado por instrutor, online, estando disponível durante todo período do treinamento.
- 1.2** Não serão aceitos treinamentos gravados.
- 1.3** 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](https://mylearn.vmware.com/mgrReg/courses.cfm?ui=www_edu&a=one&id_subject=93070);
- 1.4** Deverá ser ministrado por empresa provedora de treinamento oficial autorizada pelo respectivo fabricante;
- 1.5** 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;
- 1.6** 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:

- 1.1** Deverá ser ministrado por instrutor, online, estando disponível durante todo período do treinamento.
- 1.2** Não serão aceitos treinamentos gravados.
- 1.3** 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](https://mylearn.vmware.com/mgrReg/courses.cfm?ui=www_edu&a=one&id_subject=98675);
- 1.4** Deverá ser ministrado por empresa provedora de treinamento oficial autorizada pelo respectivo fabricante;
- 1.5** 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;
- 1.6** 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:

- 1.1** Deverá ser ministrado por instrutor, online, estando disponível durante todo período do treinamento.
- 1.2** Não serão aceitos treinamentos gravados.
- 1.3** 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](https://mylearn.vmware.com/mgrReg/courses.cfm?ui=www_edu&a=one&id_subject=97477);
- 1.4** Deverá ser ministrado por empresa provedora de treinamento oficial autorizada pelo respectivo fabricante;
- 1.5** 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;
- 1.6** 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:

- 1.1** Deverá ser ministrado por instrutor, presencial ou online, estando disponível durante todo período do treinamento.
- 1.2** Não serão aceitos treinamentos gravados.
- 1.3** Deverá contemplar todos os itens descritos na ementa disponível em: <https://docs.microsoft.com/en-us/training/courses/az-800t00>;
- 1.4** Deverá ser ministrado por empresa provedora de treinamento oficial autorizada pelo respectivo fabricante;
- 1.5** 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;
- 1.6** 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:

- 1.1** Deverá ser ministrado por instrutor, presencial ou online, estando disponível durante todo período do treinamento.
- 1.2** Não serão aceitos treinamentos gravados.
- 1.3** Deverá contemplar todos os itens descritos na ementa disponível em: <https://docs.microsoft.com/en-us/training/courses/az-800t01>;
- 1.4** Deverá ser ministrado por empresa provedora de treinamento oficial autorizada pelo respectivo fabricante;
- 1.5** 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;
- 1.6** 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**

**1.1** 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

**1.2** Deverá possuir serviço de suporte e garantia de 60 meses;

**1.3** 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

**1.4** 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

**1.5** 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

**1.6** 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

**1.7** 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

**1.8** 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

**1.9** 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

- 1.10** 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
- 1.11** Deverá possuir funcionalidade de monitoramento pró-ativo que permita a detecção, o isolamento e o registro de falhas sem que faça necessária intervenção manual
- 1.12** Caberá à contratada o fornecimento dos dispositivos necessários à implementação dos mecanismos de monitoramento e abertura automática de chamados
- 1.13** 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
- 1.14** 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
- 1.15** Caso o suporte remoto seja feito por um computador externo ao equipamento, esse computador deverá se fixar em um rack de 19 polegadas padrão
- 1.16** 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
- 1.17** Deverá disponibilizar interface gráfica web (GUI - Graphical User Interface) para viabilizar seu gerenciamento centralizado
- 1.18** 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
- 1.19** A solução ofertada deverá se integrar nativamente ao software de backup Commvault , devendo esta compatibilidade ser comprovada através de matriz de compatibilidade do fabricante
- 1.20** 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
- 1.21** Não serão aceitos equipamentos usados, remanufaturados ou de demonstração
- 1.22** 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**

- 2.1** Deverá suportar expansões em sua arquitetura pelo acréscimo de novos componentes de hardware e de software
- 2.2** 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
- 2.3** 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"
- 2.4** Deverá ser implementado em "hardware" específico, via emprego de equipamento do tipo "appliance", dedicado exclusivamente a esta função visando prover suas funcionalidades
- 2.5** Deverá prover conectividade de forma concorrente e distribuída a todos os clientes do serviço de cópia e de restauração dos dados
- 2.6** 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
- 2.7** A rede de "back-end" SAS deverá prover velocidade mínima de 6 (seis) Gbps em regime de alta disponibilidade
- 2.8** 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
- 2.9** 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
- 2.10** 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
- 2.11** 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
- 2.12** 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
- 2.13** Deverá implementar nativamente o protocolo IP ("Internet Protocol") v4
- 2.14** Deverá possibilitar a criação de rotas estáticas unicast IP v4
- 3. Capacidade**
  - 3.1** 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, deduplicação 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).
  - 3.2** Complementarmente, não poderão ser considerados quaisquer ganhos de capacidade oriundos

de deduplicação, compressão de dados ou outros algoritmos similares

**3.3** A licença não deverá possuir limitações quanto à quantidade de dados armazenados

**3.4** Deverá suportar o aumento da área de armazenamento local em pelo menos 250 (duzentos e cinquenta) TB líquidos

**3.5** Deverá atingir sua capacidade máxima de expansão pela simples adição de discos e/ou gavetas de discos

**3.6** Deverá implementar pelo menos 14 TB/hora de throughput sustentado nas interfaces de "front-end" do equipamento, desconsiderando qualquer taxa de deduplicação

**3.7** Deverá implementar pelo menos 250 (duzentos e cinquenta) fluxos (sessões) de backups simultâneos

#### **4. Controladoras**

**4.1** Deverão ser compatíveis com o sistema a ser fornecido

**4.2** A controladora deverá empregar processadores com múltiplos núcleos (ou cores) visando o aumento de desempenho do sistema

**4.3** No caso do fornecimento de múltiplas controladoras, no funcionamento em modalidade ativo/passivo:

**4.3.1** 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

**4.3.2** 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

**4.3.3** 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

**4.3.4** O sistema de armazenamento deverá possibilitar a substituição das controladoras de forma alternada em caso de falha

**4.3.5** 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

**4.3.6** 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

**4.4** A(s) controladora(s) deverá possuir no mínimo 2 (duas) conexões redundantes ao barramento de "back-end" SAS do sistema

## **5. Memória Cache**

**5.1** 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

**5.2** 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

**5.3** 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")

**5.4** 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")

**5.5** 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**

**6.1** 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

**6.2** Deverá ser fornecido com no mínimo 4 (quatro) interfaces 10Gbps, de acordo com o padrão IEEE 802.3ae, com conectores SFP+. deverão ser fornecidos transceivers e cordões de fibra ótica com conectores LC-LC para todas as interfaces disponíveis. Os transceivers deverão ser do tipo SR. O cordão de fibra ótica deverá possuir o comprimento mínimo de 10 metros.

**6.3** 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**

**7.1** 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

**7.2** Deverá implementar caminhos de acesso redundantes aos discos contidos no barramento de "back-end"

**7.3** 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

**7.4** O quantitativo total de discos a ser fornecido pela proponente deverá estar distribuído homogeneamente entre os diversos canais de comunicação do equipamento

**7.5** 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**

**8.1** 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

**8.2** Deverá implementar algoritmos de deduplicação, permitindo eliminar segmentos redundantes e compactar os dados, de forma a reduzir a área de disco destinada ao armazenamento dos dados de backup

**8.3** O mecanismo de deduplicação deverá ser nativo da solução, sem utilização de software externo instalado nos servidores ou clientes de backups

**8.4** O mecanismo de deduplicação 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 deduplicação 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

**8.5** Deverá efetuar deduplicação global, ou seja, um único pool de deduplicação por sistema, deduplicando assim de forma global todos os dados oriundos de qualquer protocolo (CIFS, NFS, OST e VTL), cliente e/ou aplicação

**8.6** Caso não suporte deduplicação 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

**8.7** A solução deve fazer uso de recursos dedicados para realizar a compressão dos dados via hardware antes ou após a deduplicação dos dados, de forma que este processo de compressão



não deve impactar o desempenho do equipamento

**8.8** Suportar criptografia do tipo DARE (Data At Rest Encryption) de no mínimo 256 bits com certificação FIPS 140-2

**8.9** 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

**8.10** 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

**8.11** 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

**8.12** O mecanismo de replicação deverá ser nativo da solução, sem necessidade de utilização de recursos externos

**8.13** 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

**8.14** O mecanismo de replicação deverá permitir o emprego de algoritmos de compressão, deduplicação e criptografia no tráfego trocado entre o "cluster" de controladoras de origem e o "cluster" de controladoras de destino

**8.15** 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

**8.16** 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

## **9. Proteção contra Ransomware**

**9.1** O equipamento deve suportar enviar de forma deduplicada 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

**9.2** 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

**9.3** 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

**9.4** 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

**9.5** Possuir recurso de dupla autenticação (2FA – Two Factor Authentication) para executar atividades administrativas de exclusão no equipamento

## **10. Protocolos de Acesso aos Dados**

**10.1** Deverá suportar simultaneamente as seguintes formas de acesso para backup: CIFS, NFS e OST

**10.2** Deverá permitir a criação e a deleção de CIFS "Shares"

**10.3** 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)

**10.4** 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**

**11.1** 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

**11.2** Deverá possuir interface de linha de comando, a qual deverá ser acessada remotamente por meio do emprego do protocolo SSH

**11.3** 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

**11.4** 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)

**11.5** 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)

**11.6** Deverá prover MIBs 18 que possam ser compiladas para o sistema de gerenciamento SNMP empregado pelo contratante 19

**11.7** Deverá permitir o envio de SNMP traps para gerentes SNMP

**11.8** Deverá possibilitar o envio de mensagens de notificação de eventos para servidores SYSLOG

**11.9** Deverá possibilitar o envio de mensagens de notificação de eventos para servidores SMTP

**11.10** Deverá possibilitar a criação de usuários, com atribuição a grupos e permissões específicas de acesso as funcionalidades

**11.11** 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

**11.12** Deverá permitir executar as seguintes funções de administração do sistema de armazenamento:

**11.12.1** Prover dados de medição sobre o consumo corrente de recursos do sistema: Número de requisições: totais, com sucesso e com falha

**11.12.2** Capacidade em disco: total, usada e disponível

**11.12.3** Desempenho: taxa de transferência na escrita e taxa de transferência na leitura

**11.12.4** Replicação: tráfego de leitura e tráfego de escrita

**11.12.5** Estado do sistema: controladoras, memória, portas de I/O, interfaces de rede, discos, fontes e ventiladores

**11.12.6** Viabilizar a configuração dos mecanismos de criptografia e replicação

**11.12.7** Monitorar o status do sistema, com recursos para definição de thresholds e geração de alertas

**11.12.8** Registrar o histórico de eventos do sistema com possibilidade de análise remota e envio remoto de logs

## **12. Segurança**

**12.1** 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

**12.2** Deverá permitir o uso de listas de controle de acesso para permitir o acesso aos dados armazenados no sistema

## **13. Características Físicas e Elétricas**

**13.1** 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

**13.2** 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

**13.3** 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

**13.4** Cada rack do sistema deverá ser fornecido com cabo de conexão ao sistema de aterramento de cada data center do contratante

**13.5** As fontes de alimentação deverão operar com uma tensão monofásica nominal de 220 VCA e com uma frequência nominal de 60 Hz

**13.6** 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

**13.7** Deverá implementar mecanismo de refrigeração a ar por meio do emprego de unidades de ventilação redundantes e "hot-swap"

**13.8** 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**

**14.1** O equipamento deverá ser instalado e configurado pela CONTRATADA

**14.2** Todas 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;

**14.3** 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:

**14.4** Instalação e configuração do hardware;

**14.5** Instalação e configuração da ferramenta de gerência e monitoramento e integração desta ao Active Directory da UDESC (idUDESC);

**14.6** Criação de pools de armazenamento conforme orientações da UDESC;

**14.7** Configuração da rede e VLANs;

**14.8** Integração com a solução de backup hoje existente na UDESC - Commvault;

**14.9** Realização de testes de backup e restore dos seguintes componentes:

**14.9.1 Máquinas Virtuais**

**14.9.2 Bases de dados SQLServer**

**14.9.3 Filesystems EXT4 e NTFS**

**14.10** 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:

**14.11** 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;

**14.12** O certificado deverá contemplar a instalação, configuração e gerenciamento da solução proposta;

**15. Documentação**

**15.1** Ao término da implementação da solução, a Contratada deverá fornecer toda a documentação técnica dos softwares instalados, incluindo, mas não se limitando, a:

**15.2** Documentação descritiva dos produtos, com todos os componentes e softwares que perfazem a solução;

**15.3** Documentação técnica do ambiente;

**15.4** 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:

**1.1** Deverá ser ministrado por instrutor, online, estando disponível durante todo período do treinamento.

**1.2** Não serão aceitos treinamentos gravados.

**1.3** Deverá contemplar, no mínimo, as seguintes pautas:

**1.3.1** Solução em Backup;

**1.3.2** Monitoramento do sistema;

**1.3.3** Configurar e gerenciar interfaces de rede;

**1.3.4** Acessar e copiar dados para o sistema de Backup;

**1.3.5** Personalizar e gerenciar sistema de arquivos de deduplicação;

- 1.3.6** Descrever e realizar replicação e recuperação de dados;
- 1.3.7** Descrever e configurar a solução de backup;
- 1.3.8** Descrever o planejamento de capacidade e rendimento;
- 1.3.9** Descrever e configurar multilocação segura;
- 1.4** Deverá ser ministrado por empresa provedora de treinamento oficial autorizada pelo respectivo fabricante;
- 1.5** 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;
- 1.6** 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:**
  - 1.1** 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);
  - 1.2** Todas as funcionalidades deverão ser fornecidas pelo mesmo fabricante, de maneira integrada e em uma mesma arquitetura, com atualizações, dentro do período do contrato;
  - 1.3** Um único appliance deve ser capaz de executar e suportar a totalidade das capacidades exigidas, não sendo aceitos somatórias para atingir os limites mínimos;
    - 1.3.1** Não serão aceitos módulos adicionais de hardware para atingir a capacidade exigida;
    - 1.3.2** 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;
    - 1.3.3** Não serão aceitos módulos adicionais de hardware para prover as funcionalidades exigidas;
    - 1.3.4** Todas as interfaces fornecidas nos appliances devem estar licenciadas e habilitadas para uso imediato;
  - 1.4** A solução deverá permitir a instalação em ambientes de alta disponibilidade das seguintes formas:



- 1.4.1** Ativo/Standby, com equipamento da mesma marca e modelo;
- 1.4.2** 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;
- 1.5** 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;
- 1.6** Todos os recursos necessários (hardware, software, licenças, assinaturas, cabos, etc) para implementar alta-disponibilidade devem ser fornecidos sem custo adicional;
- 1.7** A solução deve permitir escalabilidade, podendo crescer na forma de cluster adicionando novos appliances inclusive de modelos diferentes;
- 1.8** 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;
- 1.9** Deverá fornecer recurso de agregação de portas baseado no protocolo LACP:
  - 1.9.1** Deverá possuir suporte a LACP em modo passivo e ativo;
  - 1.9.2** Deverá fornecer recurso para suportar até 8 portas em um mesmo conjunto agregado;
- 1.10** Deverá possuir suporte a Spanning-Tree(802.1D), Fast Spanning-Tree (802.1w, 802.1t) e Multi Spanning-Tree (802.1s);
- 1.11** 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;
- 1.12** Deverá oferecer suporte a IPv6;
- 1.13** A solução deve suportar múltiplas tabelas de rotas independentes;
- 1.14** 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;
  - 1.14.1** Deverá possuir capacidade para gerenciar os recursos disponíveis de acordo com as funções habilitadas;
- 1.15** A solução deve permitir múltiplos domínios de roteamento em IPv4 e IPv6;
- 1.16** Deverá suportar à funcionalidade de VXLAN, para integração com o ambiente de virtualização de redes (Software Defined Network);
- 1.17** Cada appliance deve possuir, no mínimo, as seguintes especificações de desempenho;
  - 1.17.1** Possuir capacidade para tratar 350.000 (trezentas e cinquenta mil) requisições por

segundo em camada 7;

**1.17.2** Possuir capacidade para tratar 125.000 (cento e vinte e cinco mil) conexões por segundo em camada 4;

**1.17.3** Possuir capacidade para sustentar pelo menos 14.000.000 (catorze milhões) de conexões simultâneas em camada 4;

**1.17.4** Possuir capacidade mínima de throughput em camada 4 de 10 (dez) Gbps;

**1.17.5** 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;

**1.17.6** 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;

**1.17.7** Possuir capacidade de criptografar com throughput mínimo de 5 (cinco) Gbps;

**1.18** Cada appliance deverá possuir, no mínimo, 4 (quatro) interfaces de 1 Gigabit Ethernet SFP e 2 (duas) interfaces de 10G SFP+;

**1.18.1** Todas as interfaces já devem ser fornecidas com os respectivos transceivers SR e com cordões de fibra ótica LC-LC;

**1.19** Cada appliance deverá possuir fontes de alimentação redundantes 100-240V com seleção automática de tensão;

## **2. Gerenciamento:**

**2.1** Deverá ser possível realizar a configuração de endereçamento IP estático ou dinâmico (DHCP/BOOTP) para o gerenciamento;

**2.2** 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;

**2.3** Deve permitir administração remota através de SSH;

**2.4** Deverá permitir manter internamente múltiplos arquivos de configurações do sistema;

**2.5** Deverá suportar transferência de arquivos de configuração e Sistema Operacional utilizando SCP ou HTTPS;

**2.6** 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:

**2.6.1** Possuir função de auto completar de comandos na CLI;

**2.6.2** Possuir ajuda contextual dos comandos na CLI;

**2.6.3** Possuir comando para visualizar o tráfego de utilização das interfaces em bits/segundo

(bps) e pacotes/segundo (pps);

**2.6.4** Reinicialização do equipamento por comando na CLI;

**2.6.5** Possuir ferramentas para identificação de problemas (debugging) através da CLI;

**2.7** Permitir a criação de no mínimo, três níveis de usuários na GUI – administrador, usuário com permissões reduzidas e usuário somente leitura;

**2.8** Deverá permitir a autenticação dos usuários de gerência em bases remotas e suportar no mínimo RADIUS, LDAP e TACACS+;

**2.9** Deverá permitir a autenticação dos usuários em bases Microsoft Active Directory;

**2.10** Possuir interface de gerência gráfica web com acesso seguro utilizando HTTP sobre TLS;

**2.11** 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;

**2.12** Deverá suportar a restauração de forma simples (rollback) de configuração e sistema operacional;

**2.13** Possuir e fornecer geração de mensagens de syslog para eventos relevantes ao sistema;

**2.14** Possuir a possibilidade de configuração de múltiplos syslog servers para os quais o equipamento irá enviar as mensagens de syslog;

**2.15** Possuir armazenamento de mensagens de syslog em dispositivo interno ao equipamento;

**2.16** A interface gráfica deverá permitir a reinicialização do equipamento;

**2.17** Possuir recurso de gerência via SNMP e implementar SNMPv1, SNMPv2c e SNMPv3;

**2.18** Implementar envio de notificações (traps) via SNMP;

**2.19** Possui suporte a monitoração utilizando RMON através de pelo menos 4 grupos: statistics, history, alarms e events

**2.20** Implementar Link Layer Discovery Protocol (LLDP);

**2.21** A Solução deve implementar exportação de informações de fluxo através de Netflow ou sFlow;

**3.** Características do balanceamento e carga e cache de dados:

**3.1** A solução deverá suportar todas as aplicações comuns de um Switch Layer 7, como:

**3.1.1** Server Load-Balancing;

**3.1.2** Firewall Load-Balancing;

**3.1.3** Proxy Load-Balancing;

**3.2** Deverá permitir balanceamento apenas em direção ao servidor, onde a resposta do servidor real é enviada diretamente ao cliente;

- 3.3** 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;
- 3.4** 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;
- 3.5** Possuir recursos para balancear servidores com qualquer hardware, sistema operacional e tipo de aplicação;
- 3.6** 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;
- 3.7** 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.
- 3.8** 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.
- 3.9** 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;
- 3.10** Suportar os seguintes métodos de balanceamento:
- 3.10.1** Round Robin;
  - 3.10.2** Least Connections;
  - 3.10.3** Weighted Percentage (por peso);
  - 3.10.4** Servidor ou equipamento com resposta mais rápida baseado no tráfego real;
  - 3.10.5** Weighted Percentage dinâmico (baseado no número de conexões);
  - 3.10.6** Dinâmico, baseado em parâmetros de um determinado servidor ou equipamento, coletados via SNMP ou WMI;
- 3.11** A solução deve permitir aplicar criptografia de cookies para a proteção dos cookies utilizados pela aplicação web;
- 3.12** Possuir recursos para balancear as sessões novas, mas preservar sessões existentes no mesmo servidor, implementando persistência de sessão dos seguintes tipos:

- 3.12.1** Por cookie: inserção de um novo cookie na sessão;
- 3.12.2** Por cookie: utilização do valor do cookie da aplicação, sem adição de cookie;
- 3.12.3** Por endereço IP destino;
- 3.12.4** Por endereço IP origem;
- 3.12.5** Por sessão SSL;
- 3.12.6** Através da análise da URL acessada.;
- 3.12.7** Através da análise de qualquer parâmetro no header HTTP;
- 3.12.8** Através da análise do MS Terminal Services Session (MSRDP);
- 3.12.9** Através da análise do SIP Call ID ou Source IP;
- 3.12.10** Através da análise de qualquer informação da porção de dados (camada 7);
- 3.13** A solução deve utilizar Cache Array Routing Protocol (CARP) no algoritmo de HASH;
- 3.14** O equipamento oferecido deverá suportar os seguintes métodos de monitoramento dos servidores reais:
  - 3.14.1** Layer 3 – ICMP;
  - 3.14.2** Conexões TCP e UDP pela respectiva porta no servidor;
- 3.15** 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;
- 3.16** Possuir recursos para balanceamento de carga de servidores SIP para VoIP (equipamento SIP PROXY);
- 3.17** Possuir recursos para limitar o número de sessões estabelecidas com cada servidor real;
- 3.18** Possuir recursos para limitar o número de sessões estabelecidas com cada servidor virtual;
- 3.19** Possuir recursos para limitar o número de sessões estabelecidas com cada grupo de servidores;
- 3.20** Possuir recursos para limitar o número de sessões estabelecidas com cada servidor físico:
  - 3.20.1** Realizar Network Address Translation (NAT);
  - 3.20.2** Realizar Proteção contra Denial of Service (DoS);
  - 3.20.3** Realizar Proteção contra SYN flood;
  - 3.20.4** Realizar Limpeza de cabeçalho HTTP;

- 3.21** A solução deve permitir o controle da resposta ICMP por servidor virtual;
- 3.22** Possuir recursos para que a configuração seja baseada em perfis, permitindo uma fácil administração;
- 3.23** Possuir capacidade de geração e gestão de perfis hierarquizados, permitindo maior facilidade na administração de políticas similares;
- 3.24** Permitir a criação de servidores virtuais com endereço IPv4 e os servidores reais com endereços IPv6;
- 3.25** Possuir recursos para executar compressão de conteúdo HTTP, para reduzir a quantidade de informações enviadas ao cliente;
  - 3.25.1** Permitir definir qual tipo de compressão será habilitada (gzip1 a gzip9, deflate);
  - 3.25.2** Possuir capacidade para definir compressão especificamente para certos tipos de objetos;
- 3.26** 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;
- 3.27** 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;
- 3.28** 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;
- 3.29** A solução deve possuir a funcionalidade de espelhamento de conexões SSL.
- 3.30** 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;
- 3.31** 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:
  - 3.31.1** 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;
  - 3.31.2** 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;

**3.31.3** Ambas as autenticações acima mencionadas ocorrendo de forma simultânea;

**3.32** Ao realizar inspeção, proteção, offLoad e aceleração de tráfego criptografado através de SSL/TLS, a solução deverá ser capaz de:

**3.32.1** 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;

**3.32.2** 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;

**3.33** A solução deve permitir aplicar criptografia de cookies para a proteção dos cookies utilizados pela aplicação web;

**3.34** 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;

**3.35** 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:

**3.35.1** SSL session cache Timeout;

**3.35.2** Session Ticket;

**3.35.3** OCSP (Online Certificate Status Protocol) Stapling;

**3.35.4** Dynamic Record Sizing;

**3.35.5** ALPN (Application Layer Protocol Negotiation);

**3.35.6** Perfect Forward Secrecy;

**3.36** Suportar a utilização de memória RAM como cache de objetos HTTP, para responder às requisições dos usuários sem utilizar recursos dos servidores;

**3.37** Possuir capacidade, no uso do recurso de cache, em definir quais tipos de objeto serão armazenados em cache e quais nunca devem ser cacheados;

**3.38** Garantir que o recurso de cache possa ajustar quanta memória será utilizada para armazenar objetos;

**3.39** Suporte a otimização do protocolo TCP para ajustes a parâmetros das conexões clientes e servidor;

**3.40** A solução deve suportar Internet Content Adaptation Protocol (ICAP);

**3.41** Deve ser capaz de realizar DHCP relay;



- 3.42** Deve possuir relatórios das aplicações, com pelos menos os seguintes gráficos:
- 3.42.1** Tempo de resposta da aplicação;
  - 3.42.2** Latência;
  - 3.42.3** Conexões para conjunto de servidores, servidores individuais;
  - 3.42.4** Por URL;
- 3.43** A ferramenta de relatórios deve possuir pelo menos os seguintes filtros para a geração dos gráficos:
- 3.43.1** Servidores virtuais;
  - 3.43.2** Servidores balanceados;
  - 3.43.3** URLs;
  - 3.43.4** Países de origem, baseados em geolocalização (GEOIP);
  - 3.43.5** Dispositivos de origem do cliente (user agent);
- 3.44** Deve possuir framework unificado para configuração da aplicação;
- 3.45** Deve possuir criptografia IPSEC para comunicação entre os balanceadores;
- 3.46** Quando licenciada, a solução deve ter a capacidade de realizar cache transparente das respostas DNS;
- 3.47** A solução deve permitir que cada domínio de roteamento utilize BGP, OSPF e RIP em IPv4 e IPv6;
- 3.48** A solução deve suportar Equal Cost Multipath (ECMP);
- 3.49** A solução deve realizar Bidirectional Forward Detection (BFD);
- 3.50** A solução deve ter suporte a Stream Control Transmission Protocol (SCTP);
- 3.51** Deve ter suporte a Transport Layer Security (TLS) Server Name Indication (SNI);
- 3.52** 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;
- 3.53** A solução deve realizar SSL Forward Proxy;
- 3.54** A solução deve ter suporte a TLS 1.2, SHA 2 Cipher e SHA256 hash;
- 3.55** A solução deve ter suporte a criptografia Perfect Forward Secrecy não apenas para troca de chaves RSA.
- 3.56** 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:

- 3.56.1** Deve ser possível configurar o tamanho máximo da fila;
- 3.56.2** Deve ser possível configurar o tempo máximo de permanência na fila;
- 3.57** A solução deve realizar Controle de Banda Estático para grupos de aplicações e rede;
- 3.58** A solução deve realizar Controle de Banda Dinâmico por aplicação e usuário;
- 3.59** A solução deve realizar Controle de Banda baseado em domínio de roteamento;
- 3.60** 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;
- 3.60.1** 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.
- 3.61** A solução deve permitir a priorização de tráfego de entrada para determinadas aplicações.
- 3.62** A solução deve permitir a criação de túneis IP por domínio de roteamento utilizando GRE, IPIP, PPP;
- 3.63** A solução deve permitir a criação de túneis IP transparente utilizando GRE e IPIP;
- 3.64** Fornecer recursos para o uso de servidores (reals) no mesmo Virtual Server;
- 3.65** Possuir suporte ao protocolo SPDY e HTTP 2.0;
- 3.66** O equipamento deve possuir suporte ao espelhamento de conexões FTP, HTTP, UDP, SSL.
- 3.67** O equipamento deverá permitir a sincronização das configurações de forma automática e manualmente, forçando a sincronização apenas no momento desejado;
- 3.68** 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;
- 3.69** Permitir a criação de regras customizadas através de linguagem aberta para modificar a distribuição dinâmica de tráfego e aumentar a proteção contra ataques;
- 3.70** Permita a manipulação do tráfego de entrada e saída, viabilizando assim a alteração de parâmetros no cabeçalho e no corpo das mensagens;
- 3.71** 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
- 3.72** Deve ser possível tomar as seguintes ações através dessas políticas:
  - 3.72.1** Bloqueio de tráfego;

**3.72.2** Reescrita e manipulação de URL;

**3.72.3** Registro de tráfego (log);

**3.72.4** Adição de informação no cabeçalho HTTP;

**3.72.5** Redirecionamento do tráfego para um membro específico;

**3.72.6** Selecionar uma política específica para Aplicação Web;

**3.73** A solução deverá ser capaz de fazer log de todas as sessões, onde os registros deverão conter:

**3.73.1** Endereço IP de origem;

**3.73.2** Porta TCP ou UDP de origem;

**3.73.3** Endereço IP de destino;

**3.73.4** Porta TCP ou UDP de destino;

**3.73.5** Protocolo de camada 4 (TCP ou UDP);

**3.73.6** Data e hora da mensagem;

**3.73.7** URL acessada;

**3.74** 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;

**3.75** A solução deve suportar controle de versão da política de configuração de forma a permitir a restauração (rollback) de qualquer versão de políticas;

**3.76** A solução deve ser capaz de analisar a performance de aplicações web;

**3.77** A solução deve possuir relatórios das aplicações;

**3.78** Deve prover métricas de aplicações como:

**3.78.1** Transações por Segundo;

**3.78.2** Tempo de latência do cliente e servidor;

**3.78.3** Throughput de requisição e resposta;

**3.79** 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;

**3.80** 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;

**3.81** 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;

**3.82** A geração de informações históricas deverá permitir:

**3.82.1** O detalhamento do tempo de resposta total de carregamento de uma URL e ou Página;

**3.82.2** Permitir a correlação de métricas de uso de rede com o comportamento das aplicações;

**4.** Características de Segurança WEB:

**4.1** O equipamento oferecido deverá proteger a infraestrutura web de ataques contra a camada de aplicação (Camada 7);

**4.2** Deve possuir tecnologia para mitigação de DDoS em camada 7 baseado em análise comportamental, usando o aprendizado;

**4.3** Deve possuir proteção contra ataques DDoS, através da análise de comportamento de tráfego usando técnicas de análise de dados e Machine Learning;

**4.4** 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;

**4.5** Ao detectar uma condição de DDoS, assinaturas dinâmicas devem ser automaticamente criadas e implementadas em tempo real para proteção da aplicação;

**4.6** 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;

**4.7** Através da análise continua de carga e monitoração de saúde de servidores, deve ser possível identificar anomalias e mitiga-las;

**4.8** 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;

**4.9** 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;

**4.10** 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;

**4.11** O equipamento oferecido deverá possuir a certificação ICSA para Firewall de Aplicação (Web Application Firewall);

**4.12** 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;

**4.13** Possuir política de segurança de aplicações web predefinidas na solução;

**4.14** Permitir a criação de políticas diferenciadas por aplicação e por URL, onde cada

aplicação e URL poderão ter políticas totalmente diferentes;

**4.15** Permitir a criação de políticas diferenciadas por aplicação;

**4.16** 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;

**4.17** 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;

**4.18** A solução deve permitir a inspeção de upload de arquivos para os servidores de aplicação;

**4.18.1** Essa inspeção pode ser feito via integração ICAP. Deve ser possível integrar com diferentes softwares de Antivírus;

**4.19** Permitir que regras customizadas em linguagem aberta possam ser utilizadas para customizar e aumentar a proteção contra ataques recentes;

**4.20** A solução deve se integrar com outras soluções de segurança e análise de logs de outros fabricantes;

**4.21** 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;

**4.22** 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;

**4.23** A solução deve prover suporte e fazer a proteção do tráfego em cima de protocolo WebSocket;

**4.24** A solução deve possibilitar o uso de múltiplas formas de logging remoto ao mesmo tempo para a mesma aplicação. Portanto deve 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;

**4.25** A solução deverá possuir funcionalidade de proteção positiva e segura contra ataques, incluindo pelo menos:

**4.25.1** Acesso por Força Bruta;

**4.25.2** Ameaças Web AJAX/JSON;

- 4.25.3** DoS e DDoS camada 7;
- 4.25.4** Buffer Overflow;
- 4.25.5** Cross Site Request Forgery (CSRF);
- 4.25.6** Cross-Site Scripting (XSS);
- 4.25.7** SQL Injection;
- 4.25.8** Parameter tampering;
- 4.25.9** Cookie poisoning;
- 4.25.10** HTTP Request Smuggling;
- 4.25.11** Manipulação de campos escondidos;
- 4.25.12** Manipulação de cookies;
- 4.25.13** Roubo de sessão através de manipulação de cookies;
- 4.25.14** Sequestro de sessão;
- 4.25.15** Força bruta no browser;
- 4.25.16** XML bombs/DoS;
- 4.25.17** Checagem de consistência de formulários;
- 4.25.18** Checagem do cabeçalho do “user-agent” para identificar clientes inválidos.
- 4.26** A solução deve suportar o uso de páginas de login AJAX/JSON tanto com configuração manual como descoberta automática;
- 4.27** Deverá ser capaz de identificar e bloquear ataques através de:
  - 4.27.1** Assinaturas, com atualização periódica da base pelo fabricante;
    - 4.27.1.1** 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;
  - 4.27.2** Regras de verificação personalizadas – política de segurança configurada.
- 4.28** 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;
- 4.29** Permitir a customização da resposta de bloqueio;
- 4.30** Permitir a liberação temporária ou definitiva (whitelist) de endereços IP bloqueados por terem originados ataques detectados pela solução;
- 4.31** Deve permitir limitar o número de conexões e requisições por IP de origem para cada endereço IP Virtual;

- 4.32** 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;
- 4.33** Deve permitir criar lista de exceção (whitelist) por endereço IP específico ou faixa de sub-rede;
- 4.34** A solução deve suportar o modelo de segurança positiva definido pelo OWASP, pelo menos o que consta no TOP 10;
- 4.35** Permitir o uso do parâmetro HTTP X-Forwarded-For como parte da política de controle;
- 4.36** Deverá implantar, no mínimo, as seguintes funcionalidades:
  - 4.36.1** Proteção contra Buffer Overflow;
  - 4.36.2** Checagem de URL;
  - 4.36.3** Checagem de métodos HTTP utilizados (GET, POST, HEAD, OPTIONS, PUT, TRACE, DELETE, CONNECT);
  - 4.36.4** Proteção contra envios de comandos SQL escondidos nas requisições enviadas a bases de dados (SQL Injection);
  - 4.36.5** Proteção contra Cross-site Scripting;
  - 4.36.6** Funcionalidade de Cookie Encryption;
  - 4.36.7** Checagem de consistência de formulários;
  - 4.36.8** Checagem do cabeçalho “user-agent” para identificar clientes inválidos;
- 4.37** Implementar funcionalidades para proteção contra exposição de informações do ambiente e servidores internos, incluindo pelo menos:
  - 4.37.1** Informações que identifique o sistema operacional e o servidor web através de “impressão digital” dos sistemas;
  - 4.37.2** Esconder qualquer mensagem de erro HTTP dos usuários;
  - 4.37.3** Remover as mensagens de erro às páginas que serão enviadas aos usuários;
- 4.38** Permitir a utilização de uma página HTML informativa e personalizável como HTTP Response aos bloqueios;
- 4.39** Deve ser possível verificar o endereço de origem do pacote IP no cabeçalho IP e no parâmetro X-forwarded-for (XFF);
- 4.40** Deve suportar a criação de políticas por geolocalização, permitindo que o tráfego de determinado(s) país/países seja(m) bloqueado(s);
- 4.41** 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;

- 4.42** 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;
- 4.43** O perfil aprendido de forma automatizada pode ser ajustado, editado ou bloqueado;
- 4.44** 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;
- 4.45** 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;
- 4.46** 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;
- 4.47** O equipamento oferecido deverá possuir as seguintes formas de detecção de ataques DoS na camada de aplicação:
- 4.47.1** Número de requisições por segundo enviados a uma URL específica;
- 4.47.2** Número de requisições por segundo enviados de um IP específico;
- 4.47.3** Detecção através de código executado no cliente com o objetivo de detectar interação humana ou comportamento de robôs (bots);
- 4.47.4** Número máximo de transações por segundo (TPS) de um determinado IP;
- 4.47.5** Aumento de um determinado percentual do número de transações por segundo (TPS);
- 4.47.6** Aumento do stress do servidor de aplicação;
- 4.48** 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;
- 4.49** 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;
- 4.50** 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;

**4.51** O equipamento oferecido deverá permitir o cadastro de robôs que podem acessar a aplicação;

**4.52** A solução deverá proteger a aplicação Web contra robôs sofisticados através da combinação de desafios enviados ao browser do usuário e técnicas avançadas de análise comportamental;

**4.53** A solução deverá possuir proteção proativa contra ataques automatizados por robôs e outras ferramentas de ataque;

**4.54** A solução deverá encriptar dados e credenciais na camada de aplicação, sem ter a necessidade de atualizar a aplicação;

**4.54.1** Essas informações devem ser encriptadas para proteger o login e as credenciais dos usuários e com isso os dados da aplicação;

**4.55** Deve proteger informações sensíveis e confidenciais da interceptação por terceiros, através da criptografia de dados quando ainda no browser do usuário;

**4.55.1** Deve proteger esses dados criptografados de malwares e keyloggers;

**4.56** O equipamento oferecido deverá implementar proteção ao JSON (JavaScript Object Notation);

**4.57** Possuir firewall XML integrado com suporte a filtro e validação de funções XML específicas da aplicação;

**4.58** Implementar a segurança de web services, através dos seguintes métodos:

**4.58.1** Criptografar/Decriptografar partes das mensagens SOAP;

**4.58.2** Assinar digitalmente partes das mensagens SOAP;

**4.58.3** Verificação de partes das mensagens SOAP;

**4.59** Prevenir o vazamento de informações, permitindo o bloqueio ou a remoção dos dados confidenciais;

**4.60** Prevenir que erros de aplicação ou infra-estrutura sejam mostrados ao usuário;

**4.61** Deverá ter integração, via ICAP, com servidor de anti-vírus para verificação dos arquivos a serem carregados nos servidores;

**4.62** Permitir o uso do parâmetro HTTP X-Forwarded-For como parte da política de controle;

**4.63** Deverá proteger o protocolo FTP com pelo menos os seguintes métodos:

**4.63.1** Determinar os comandos FTP permitidos;

**4.63.2** Requests FTP anônimos;

**4.63.3** Checar conformidade com o protocolo FTP;

- 4.63.4** Proteger contra ataques de força bruta nos logins;
- 4.64** Deverá proteger o protocolo SMTP com pelo menos os seguintes métodos:
  - 4.64.1** A comunicação deve ser aderente a RFC 2821;
  - 4.64.2** Limitar o número de mensagens;
  - 4.64.3** Validar registro SPF do DNS;
  - 4.64.4** Determinar quais métodos SMTP podem ser utilizados;
- 4.65** Deverá armazenar os registros (logs) localmente ou exportar para Syslog server;
- 4.66** Deverá proteger contra ataques CSRF (Cross-Site Request Forgery), podendo ser possível especificar quais URLs serão examinadas;
- 4.67** 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;
- 4.68** A solução deve fornecer relatórios consolidados de ataques com pelo menos os seguintes dados:
  - 4.68.1** Resumo geral com as políticas ativas;
  - 4.68.2** Anomalias e estatísticas de tráfego;
  - 4.68.3** Ataques de DoS, força bruta e robôs;
  - 4.68.4** Informações sobre violações, URL, endereços IP, países, severidade e PCI Compliance;
- 4.69** Deverá permitir o agendamento de relatórios a serem entregues por e-mail;
- 4.70** Fornecer os seguintes Gráficos de alertas por:
  - 4.70.1** Política de segurança;
  - 4.70.2** Tipos de ataques;
  - 4.70.3** Violações;
  - 4.70.4** URL;
  - 4.70.5** Endereços IP;
  - 4.70.6** Países;
  - 4.70.7** Severidade;
  - 4.70.8** Código de resposta;
  - 4.70.9** Métodos;
  - 4.70.10** Protocolos;
  - 4.70.11** Vírus;

**4.70.12** Usuário;

**4.70.13** Sessão;

**4.71** Deverá exportar as requisições que contém os ataques, pelo menos no formato PDF;

**4.72** Deve possuir relatório em tempo real sobre ataques de DoS L7, atualizado automaticamente;

**4.73** A solução deve mostrar o impacto de ataques de DoS L7 na performance e memória do servidor;

**4.74** Os logs devem indicar o momento de início e final de um ataque de DoS L7;

**4.75** Possuir método de mitigação de DoS L7 baseado em:

**4.75.1** CAPTCHA;

**4.75.2** Descarte de todas as requisições de um determinado IP e/ou país suspeito;

**4.75.3** Geolocalização, incluindo a prevenção com CAPTCHA para países suspeitos que ultrapassem limiares;

**4.75.4** Defesa proativa contra bot, através da injeção de um desafio JavaScript para detectar se é um usuário legítimo ou robô;

**4.76** A solução deve permitir que ao detectar um falso positivo, o administrador aceite a requisição e atualize a política automaticamente;

**4.77** A solução ao se integrar com um Scanner de vulnerabilidade deve mostrar quais as 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 avisos de possíveis consequências na aplicação Web;

**4.78** 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;

**4.79** A solução deve possuir proteção de DDoS L7 baseado em análise comportamental, sem precisar de nenhuma configuração manual;

**5.** Características de alta disponibilidade global

**5.1** A solução deve operar, no mínimo, das seguintes formas:

**5.1.1** DNS autoritativo;

**5.1.2** DNS secundário;

**5.1.3** DNS resolver;

**5.1.4** DNS cache;

- 5.1.5** Balanceamento de DNS servers;
- 5.1.6** DNSSec;
- 5.2** A solução deve ser capaz de realizar transferência de zonas para múltiplos servidores DNS Primários responsáveis por diferentes zonas;
- 5.3** 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;
- 5.4** A solução deve realizar o offload dos servidores de DNS, funcionando como o DNS secundário;
- 5.5** A solução deve possuir certificação ICSA;
- 5.6** A solução deve possuir proteções contra ataques DNS, de no mínimo dos seguintes tipos:
  - 5.6.1** Inspeção de protocolo;
  - 5.6.2** Validação de protocolo;
  - 5.6.3** UDP flood;
  - 5.6.4** Pacotes mal formados;
  - 5.6.5** Ataque Teardrop;
  - 5.6.6** Ataque ICMP;
- 5.7** Permitir que regras customizadas em linguagem aberta possam ser utilizadas para customizar a distribuição dinâmica de tráfego e aumentar a proteção contra ataques;
- 5.8** A solução deve ser capaz de realizar balanceamento dos servidores DNS;
- 5.9** A solução deve ser capaz de realizar filtragem de pacotes;
- 5.10** A solução deve prover segurança do protocolo DNS, protegendo contra ataques de negação de serviço, NXDOMAIN e reflexão e amplificação de DNS;
- 5.11** A solução deve prover segurança do protocolo DNS, protegendo contra ataques de Cache Poisoning;
- 5.12** A solução deve realizar stateful inspection;
- 5.13** A solução deve possuir base de Geolocalização IP;
- 5.14** A solução deve implementar DNS64;
- 5.15** A solução deve suportar pelo menos os seguintes tipos de requisição DNS: SOA, A, AAAA, CNAME, DNAME, HINFO, MX, NS, PTR, SRV, TXT;
- 5.16** Deve ser capaz de gerar estatísticas sobre consultas de DNS por: Aplicação, nome da query, tipo da query, endereço IP do cliente;
- 5.17** Deve ser possível configurar a solução de modo inline a estrutura de DNS existente e

transparente sem requerer grandes mudanças na infraestrutura;

**5.18** Deve prover as respostas as queries DNS da própria RAM CACHE;

**5.19** A solução deve ser capaz de realizar IP Anycast;

**5.20** A solução deve ser capaz de realizar DNSSec, independente da estrutura dos servidores DNS em uso;

**5.21** A solução de alta disponibilidade não deve depender de BGP ou outro protocolo de roteamento;

**5.22** 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;

**5.23** 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;

**5.24** Deve ser possível ajustar quantos endereços são enviados em uma única resposta;

**5.25** Suporte a monitoração de estado de saúde de servidores, serviços e links de conexão a provedor de serviço, garantindo a disponibilidade do serviço oferecido;

**5.26** Suportar pelo menos os seguintes algoritmos de balanceamento:

**5.26.1** Round Robin;

**5.26.2** Global Availability;

**5.26.3** Ratio;

**5.26.4** LDNS Persist;

**5.26.5** Geografia;

**5.26.6** Disponibilidade da Aplicação;

**5.26.7** Capacidade do Virtual Server;

**5.26.8** Least Connections;

**5.26.9** Pacotes por segundo;

**5.26.10** Round trip time;

**5.26.11** Hops;

**5.26.12** Packet Completion Rate;

**5.26.13** QoS definido pelo usuário;

**5.26.14** Kilobytes per Second;

**5.27** A solução deverá ser capaz de implementar persistência da conexão do usuário entre

aplicações ou data centers;

**5.28** 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;

**5.29** A solução deverá permitir que as políticas sejam configuradas individualmente por aplicação sendo balanceada;

**5.30** A solução deverá permitir que a contingência seja automática, mas que o retorno seja manual;

**5.31** A solução deve ser capaz de atender clientes IPv6 quando o site atende apenas com IPv4 (requests AAAA ou A6);

**5.32** Possuir suporte a IPv6 no balanceamento global entre datacenters.

**5.33** 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;

**5.34** Deverá possuir a funcionalidade de resposta rápida a queries DNS permitindo respostas mais rápidas para zonas que seja autoritativo;

**5.35** 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**

**6.1** Deverá possuir serviço de suporte e garantia DO FABRICANTE de 60 meses;

**6.2** 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

**6.3** 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;

**6.4** 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**

**7.1** O equipamento deverá ser instalado e configurado pela CONTRATADA



**7.2** 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;

**7.2.1** Instalação de todos os componentes da solução fornecidos como softwares;

**7.2.2** 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;

**7.2.3** Ativação de todas os componentes da solução fornecidos como assinaturas (subscription);

**7.2.4** Disposição e conectorização de hardwares no rack que os acomodarão;

**7.2.5** Instalação dos transceivers em seus módulos/slots;

**7.2.6** Interconexão a outros switches, roteadores e servidores de rede, entre outros;

**7.2.7** 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;

**7.2.8** Ajuste dos demais parâmetros de configuração, conforme Projeto Executivo;

**7.2.9** Configuração relativa ao balanceamento de carga:

**7.2.9.1** Configuração de alta disponibilidade;

**7.2.9.2** Configuração de interfaces virtuais para balanceamento de servidores;

**7.2.9.3** Configuração de perfis de otimização de tráfego;

**7.2.9.4** Configuração de políticas de acesso;

**7.2.9.5** Configuração de regras de manipulação de tráfego;

**7.2.10** Configuração relativa à solução de segurança de aplicações web:

**7.2.10.1** Configurações de bloqueios de máscara contra violações, técnicas de invasão, compliance de protocolos HTTP e segurança de web services;

**7.2.10.2** Configuração de assinaturas de ataques;

**7.2.10.3** Configuração de ataques baseados em assinatura com base nas requisições do cliente;

**7.2.10.4** Configuração de parâmetros para uma aplicação específica;

**7.2.10.5** Configuração de segurança de aplicação baseada em DoS Protection;

**7.2.11 Configuração relativas a alta disponibilidade de sites e DNS:**

**7.2.11.1** Configuração de até 2 (dois) data centers;

**7.2.11.2** Configuração de até 4 (quatro) links de dados;

**7.2.11.3** Configuração de até 8 (oito) Wide-IPs (hosts dns alto disponível);

**7.2.11.4** Configuração de até 4 zonas DNS com DNSSEC;

**7.2.11.5** Configuração de forwarding e recursividade;

**7.3** 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:

**7.3.1** 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;

**7.3.2** 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);

**7.4** 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;

**7.5** As configurações deverão seguir fielmente a padronização previamente estabelecida pela CONTRATANTE;

**7.6** 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;

**7.6.1** 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;

**7.6.2** A carga horária deverá ser de, no mínimo, 8 (oito) horas e contar com até 5 (dez) participantes indicados pela CONTRATANTE;

**7.6.3** 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;

**7.6.4** 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**

**8.1** 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:

**8.1.1** Documentação descritiva dos produtos, com todos os componentes e softwares que perfazem a solução;

**8.1.2** 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:

**1.1** Deverá ser ministrado por instrutor, online, estando disponível durante todo período do treinamento.

**1.2** Não serão aceitos treinamentos gravados.

**1.3** Deverá ser ministrado por empresa provedora de treinamento oficial autorizada pelo respectivo fabricante;

**1.4** O treinamento deverá englobar, no mínimo, os seguintes tópicos:

**1.4.1** Configuração relativa ao balanceamento de carga;

**1.4.2** Configuração de alta disponibilidade;

**1.4.3** Configuração de interfaces virtuais para balanceamento de servidores;

**1.4.4** Configuração de perfis de otimização de tráfego;

- 1.4.5 Configuração de políticas de acesso;
- 1.4.6 Configuração de regras de manipulação de tráfego;
- 1.4.7 Configuração relativa a solução de segurança de aplicações web;
- 1.4.8 Configurações de bloqueios de máscara contra violações, técnicas de invasão, compliance de protocolos HTTP e segurança de web services;
- 1.4.9 Configuração de assinaturas de ataques;
- 1.4.10 Configuração de ataques baseados em assinatura com base nas requisições do cliente;
- 1.4.11 Configuração de parâmetros para uma aplicação específica;
- 1.4.12 Configuração de segurança de aplicação baseada em DoS Protection;
- 1.4.13 Configuração relativas a alta disponibilidade de sites e DNS;
- 1.4.14 Configuração de data centers;
- 1.4.15 Configuração de links de dados;
- 1.4.16 Configuração de Wide-IPs (hosts dns alto disponível);
- 1.4.17 Configuração de zonas DNS com DNSSEC;
- 1.4.18 Configuração de forwarding e recursividade;
- 1.5 Caso seja necessário mais de um treinamento, cabe a CONTRATADA o fornecimento de proposta que englobe todos;
- 1.6 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;
- 1.7 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:

- 1.1 Licença perpétua para backup de 1(uma) conta do Microsoft365, independentemente da volumetria utilizada, incluindo a possibilidade de fazer backup as seguintes ferramentas:
  - 1.1.1 Exchange;
  - 1.1.2 One Drive;

**1.1.3** SharePoint;

**1.1.4** Microsoft Teams;

**1.2** 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;

**1.3** Garantia e suporte técnico, com direito à atualização de software, na modalidade Production (24x7) atendido diretamente pela Commvault

**1.4** 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:**

**1.1** Painel Traseiro para Servidor Hp DL380 Gen10 para acomodação da expansão de discos;

**1.2** Suportar oito unidades SAS / SAFA SFF 2,5” na caixa;

**1.3** Acompanhar cabos de energia;

**1.4** Deve ser totalmente compatível com o servidor Hp DL380 Gen10(Part Number 19720-B21);

**1.5** 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:**

**1.1** Controlador modular para expansão da capacidade de armazenamento;

**1.2** Suporte para 12 Gb/s SAS e PCIe 3.0;

**1.3** Deve possuir 16 portas internas SAS, compatível com níveis avançados de RAID com cache de gravação garantido por flash de 4GB (FBWC);

**1.4** Deve ser totalmente compatível com o servidor Hp DL380 Gen10(Part Number 19720-B21);

**1.5** 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:**

- 1.1** Capacitores híbridos de armazenamento inteligente HPE com kit de cabo de 145 mm
- 1.2** Deve ser totalmente compatível com o servidor Hp DI380 Gen10(Part Number 19720-B21);
- 1.3** 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:**

- 1.1** Disco SAS do tipo hard drive HDD;
- 1.2** Capacidade de no mínimo 2.4 TB;
- 1.3** Interface SAS 12GB/S, tipo HOT-SWAP;
- 1.4** Formato de tamanho 2,5” SFF;
- 1.5** Taxa de transferência de dados de 1.2 GBPS;
- 1.6** Velocidade de rotação de 10000 RPM;
- 1.7** Formato avançado 512E;
- 1.8** Deve ser totalmente compatível com o servidor Hp DI380 Gen10(Part Number 19720-B21);
- 1.9** 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:**

- 1.1** Disco SAS do tipo Drive de Estado Sólido SSD;
- 1.2** Capacidade de no mínimo 1.9 TB;
- 1.3** Interface SAS 12GB/S;
- 1.4** Formato de tamanho 2,5” SFF;

- 1.5** Leitura randômica de 4K com 155000IOPS;
- 1.6** Deve ser totalmente compatível com o servidor Hp DL380 Gen10(Part Number 19720-B21);
- 1.7** Deve possuir garantia de 12 meses;

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

##### **ESPECIFICAÇÃO TÉCNICA – Serviço de Implementação/Instalação**

Características mínimas:

- 1.1** Instalação/Implantação do itens presentes no LOTE 08;
- 1.2** O escopo da instalação consiste em 01 (um) servidor HP DL380 Gen10(Part Number: 19720-B21) de propriedade da contratante;
- 1.3** O serviço deverá ser realizado pelo fabricante do equipamento ou seu representante autorizado;
- 1.4** A instalação consiste no pleno funcionamento dos itens contratados;

### **3. CONDIÇÕES GERAIS**

#### **3.1 Licenciamento para o Lote 01, Lote 02 e Lote 07:**

**3.1.1** 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.

#### **3.2 Garantia e Suporte:**

**3.2.1** 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;

**3.2.2** Em caso de software a garantia deve englobar a atualização de versões de software, incluindo upgrades, updates ou patches de correção;

**3.2.3** 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;

**3.2.4** 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.

**3.2.5** 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;

**3.2.6** 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.

**3.2.7** A garantia deverá abranger todo e qualquer defeito de projeto, fabricação, transporte, softwares e acessórios envolvidos;

**3.2.8** 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;

### **3.3** Abertura de Chamados:

**3.3.1** A abertura de chamados técnicos poderá ser realizada no fabricante da solução ofertada. Os chamados poderão ser abertos através dos seguintes canais:

**3.3.1.1** Telefone 0800;

**3.3.1.2** Página web mantida pela Contratada e pelo fabricante do equipamento.

**3.4** 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;

**3.5** 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;

**3.6** 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;

**3.7** 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: <a href="http://www.fabricante.com/zzzzz">www.fabricante.com/zzzzz</a>

## **4. LOCAL, PRAZOS E CONDIÇÕES DE FORNECIMENTO:**

**4.1 Locais** – Os produtos serão entregues e/ou executados pelo(s) Contratado(s), conforme a necessidade e mediante Autorização de Fornecimento – AF/Contrato.

### **4.1.1 CAMPUS I – GRANDE FLORIANÓPOLIS:**

**4.1.1.1 Reitoria:** Av. Madre Benvenuta, 2007, Itacorubi, Florianópolis/SC, CEP 88035-001. **Horário de funcionamento: 13h às 19h.**

**4.1.2 CAMPUS II – Norte Catarinense:**

**4.1.2.1 CCT - Centro de Ciências Tecnológicas.** Rua Paulo Malschitzki, Zona Industrial Norte - Joinville, SC, CEP: 89.219-710.

**4.2** 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.

**4.3** As solicitações só poderão ser atendidas se houver saldo do item na Autorização de Fornecimento (AF)/Contrato vigente.

**4.4** 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.

**4.5** 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.

**4.6** A Contratante não aceitará, sob nenhum pretexto, a transferência de responsabilidade da Contratada para terceiros.

**4.7** A Contratante reserva-se o direito de a qualquer tempo, previamente ao aceite, ou durante o prazo de validade do produto, proceder a análise técnica e de qualidade do mesmo, através de Parecer Técnico, realizado diretamente ou por intermédio de terceiros.

**4.7.1** Caso o Parecer Técnico rejeite o produto analisado este deverá ser substituído imediatamente pela Contratada, sem qualquer ônus para a Contratante.

**4.8** 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.

**4.8.1** 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).

**4.9** Para efeitos de garantia, será suficiente à UDESC a apresentação de cópia da Nota Fiscal de compra.

**4.10** 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**  
**PREGÃO ELETRÔNICO Nº 1204/2022**

Quadro de Quantitativo e Especificação Mínima dos Itens

# **ANEXO AO EDITAL**

**ANEXO III**  
**PREGÃO ELETRÔNICO nº 1204/2022**  
**MINUTA DA ATA DE REGISTRO DE PREÇOS**

Conforme datas das assinaturas digitais, a FUNDAÇÃO UNIVERSIDADE DO ESTADO DE SANTA CATARINA, inscrita no CNPJ sob o nº 83.891.283/0001-36, doravante denominado Órgão Gerenciador, representado neste ato pelo Magnífico Reitor, Dilmar Baretta, CI nº 2876321/SSPSC, CPF 824.161.769-00, nos termos do art. 15 da Lei nº 8.666, de 21 de junho de 1993, em face da classificação das propostas apresentadas neste pregão eletrônico, resolve REGISTRAR OS PREÇOS das empresas com preços mais vantajosos, por lote, sujeitando-se as partes ao edital deste pregão eletrônico, as determinações da Lei Federal nº 10.520 de 17 de julho de 2002, com aplicação subsidiária da Lei Federal nº 8.666, de 21 de junho de 1993, Decreto Estadual nº 2.617, de 16 de setembro de 2009, alterações posteriores, demais normas legais federais e estaduais vigentes e pelas cláusulas e condições que se seguem.

ITEM	OBJETO	MARCA/MODELO	QUANTIDADE	UNIDADE	VALOR UNITÁRIO
Empresa ....., inscrita no CNPJ/MF sob o nº ....., com sede na ..... – Bairro .....-...../SC, doravante, denominada fornecedora.					

**CLÁUSULA PRIMEIRA – Do Objeto e sua Execução**

Constitui objeto da presente Ata de Registro de Preços (ARP) o registro dos preços dos produtos especificados no Anexo II do Edital.

§ 1º – São Participantes desta ARP, aqueles descritos no Anexo I, deste Edital de pregão eletrônico.

§ 2º – É vedada a formalização de contratos de qualquer natureza, incluindo os relativos à concessão de serviços públicos e programas de apoio e linhas de crédito, pela Administração Pública estadual direta ou indireta, com as empresas inseridas no Cadastro de Empregadores que tenham mantido trabalhadores em condições análogas à de escravo, do Ministério do Trabalho e Emprego (MTE), conforme o art. 2º da Lei nº 16.493/2014.

**CLÁUSULA SEGUNDA – Da Vigência**

O prazo de vigência da Ata de Registro de Preços será de 12 (doze) meses contadas da data de publicação do extrato no Diário Oficial do Estado de Santa Catarina (DOE/SC), vedada a sua prorrogação.

**CLÁUSULA TERCEIRA – Dos Contratos**

Para consecução do fornecimento dos produtos registrados nesta Ata, serão emitidas autorizações de fornecimento/contratos entre as empresas julgadas vencedoras – Fornecedoras e a FUNDAÇÃO UNIVERSIDADE DO ESTADO DE SANTA CATARINA, Órgão Participante, deste pregão eletrônico.

**CLÁUSULA QUARTA** – São partes integrantes da presente Ata, independentemente de sua transcrição, o Edital deste pregão eletrônico, seus Anexos e a proposta eletrônica da Fornecedora.

**CLÁUSULA QUINTA – Do Foro**

Fica eleito o Foro da Comarca da Capital do Estado de Santa Catarina, com a renúncia expressa de qualquer outro, por mais privilegiado que seja, para serem dirimidas questões originárias da execução desta Ata.

**Florianópolis/SC,**

(Assinatura Digital)  
**Órgão Gerenciador**  
Fundação Universidade do  
Estado de Santa Catarina

(Assinatura Digital)  
**Contratada 1**

(Assinatura Digital)  
**Contratada 2**

**ANEXO IV**  
**PREGÃO ELETRÔNICO nº 1204/2022**  
**MINUTA DE CONTRATO**

**AQUISIÇÃO DE DISPOSITIVO APPLIANCE PARA ARMAZENAMENTO DE BACKUP, SEGURANÇA WEB, LICENÇAS VMWARE, REDHAT, COMMVAULT, SERVIÇOS ESPECIALIZADOS DE IMPLANTAÇÃO DE REDHAT, VMWARE E TREINAMENTOS MICROSOFT, VMWARE E REDHAT QUE ENTRE SI CELEBRAM A FUNDAÇÃO UNIVERSIDADE DO ESTADO DE SANTA CATARINA – UDESC E A EMPRESA .....**

A FUNDAÇÃO UNIVERSIDADE DO ESTADO DE SANTA CATARINA - UDESC, com sede na Av. Madre Benvenuta, 2007, Itacorubi, Florianópolis, SC – CEP 88035-901, inscrito no CNPJ sob o nº 83.891.283/0001-36, inscrição estadual isenta, doravante denominada CONTRATANTE, neste ato representado pelo seu titular, Reitor Dilmar Baretta, CI nº xxxxx/SSPSC, CPF xxxxxx, e de outro lado a empresa ....., estabelecida na ....., inscrita no CNPJ sob o nº ....., doravante denominada CONTRATADA, firmam o presente instrumento de Contrato, regido pela Lei Federal nº 8.666, de 21 de junho de 1993, Lei Federal nº 10.520, de 17 de julho de 2002, Decreto Estadual nº 2.617, de 16 de setembro de 2009, alterações posteriores, demais normas legais federais e estaduais vigentes e pelas seguintes cláusulas e condições:

**CLÁUSULA PRIMEIRA – Do Objeto e sua Execução**

Constitui objeto do presente a **AQUISIÇÃO DE DISPOSITIVO APPLIANCE PARA ARMAZENAMENTO DE BACKUP, SEGURANÇA WEB, LICENÇAS VMWARE, REDHAT, COMMVAULT, SERVIÇOS ESPECIALIZADOS DE IMPLANTAÇÃO DE REDHAT, VMWARE E TREINAMENTOS MICROSOFT, VMWARE E REDHAT**, de acordo com as especificações e condições para execução do objeto, descritos no **Anexo I e II** do Edital do Pregão Eletrônico.

**PARÁGRAFO ÚNICO** – São partes integrantes do Contrato, como se transcritos estivessem, o edital de licitação e seus anexos, os documentos, proposta e informações apresentadas pela Contratada que deram suporte ao julgamento do referido pregão.

**CLÁUSULA SEGUNDA – Dos itens, Do Preço e do Reajuste.**

**§ 1º Do Preço**

**I** - O valor total deste Contrato é de R\$ ..... (.....), conforme discriminado no quadro abaixo:

Lote/Item	Características Mínimas	Marca/modelo	Quantidade	Valor Unitário (R\$)	Valor Total (R\$)

**II** - Do reajuste de preço – O preço estabelecido é fixo, único e irrevogável, durante a vigência do Contrato, e inclui todos e quaisquer ônus, quer sejam tributários, fiscais ou trabalhistas, seguros, impostos e taxas, transporte, frete e quaisquer outros encargos necessários à execução do objeto do Contrato, exceto nos casos previstos no art. 65 da Lei Federal nº 8.666, de 21 de junho de 1993.

**III** – A revisão dos preços poderá ser concedida, pelo CONTRATANTE, a partir da análise e discussão de planilha que demonstre a alteração dos custos, a ser encaminhada pela CONTRATADA à (ao) CONTRATANTE, nos termos do art. 65, inc. II, letra “d” da Lei Federal nº 8.666, de 21 de junho de 1993.

**CLÁUSULA TERCEIRA – Da Dotação Orçamentária**

O pagamento do presente Contrato correrá a conta dos recursos consignados no orçamento abaixo:

SUBAÇÃO	FONTE	ELEMENTO DE DESPESA

#### **CLÁUSULA QUARTA – Do Prazo de Vigência do Contrato**

I - O prazo de vigência deste instrumento tem início na sua assinatura até o encerramento dos créditos orçamentários do ano de sua emissão.

#### **CLÁUSULA QUINTA – Das Obrigações das Partes**

I – A UDESC e a licitante vencedora declaram que tem ciência da existência da Lei nº 13.709/2018 (Lei Geral de Proteção de Dados - LGPD) e se comprometem a adequar todos os procedimentos internos ao disposto na legislação, com o intuito de proteger os dados pessoais que lhe forem repassados, cumprindo, a todo momento, as normas de proteção de dados pessoais, jamais colocando, por seus atos ou por sua omissão, em situação de violação de tais regras.

II – A UDESC e a licitante vencedora se comprometem no sentido de que somente poderão tratar dados pessoais dos usuários dos serviços contratados, nos limites e finalidades exclusivas do cumprimento de suas obrigações com base na presente avença/instrumento e jamais para qualquer outra finalidade.

III - A UDESC e a licitante vencedora assumem o compromisso de confidencialidade e de não compartilhar e/ou garantir acesso aos dados pessoais, que detenha por força do presente contrato, sendo, em regra, vedada a transferência das informações a outras pessoas físicas ou jurídicas, salvo aquelas decorrentes de obrigações legais ou para viabilizar o cumprimento do próprio contrato; se a solicitação for realizada por autoridade de proteção de dados, deverá haver deliberação conjunta sobre tal pedido e suas decorrências.

IV - A UDESC e a licitante vencedora ficam obrigadas a denunciar eventual incidente de acessos não autorizados aos dados pessoais, situações acidentais ou ilícitas de destruição, perda, alteração, comunicação ou qualquer forma de tratamento inadequado ou ilícito, bem como adotar as providências dispostas no art. 48 da Lei Geral de Proteção de Dados Pessoais.

De acordo com a Instrução Normativa CGE/SEA Nº 1 DE 26/03/2020, as Partes:

I - Declaram que têm conhecimento das normas previstas na legislação sobre anticorrupção, entre as quais nas Leis nºs 8.429/1992 e 12.846/2013, seus regulamentos e eventuais outras aplicáveis;

II - Comprometem-se em não adotar práticas ou procedimentos que se enquadrem nas hipóteses previstas nas leis e regulamentos mencionados no inciso acima e se comprometem em exigir o mesmo pelos terceiros por elas contratados;

III - Comprometem-se em notificar à Controladoria-Geral do Estado qualquer irregularidade que tiverem conhecimento acerca da execução deste contrato;

IV - Declaram que têm ciência que a violação de qualquer das obrigações previstas na Instrução Normativa, além de outras, é causa para a rescisão unilateral do contrato, sem prejuízo da cobrança das perdas e danos, inclusive danos potenciais, causados à parte inocente e das multas pactuadas.

#### **I - DA CONTRATADA**

a) - A CONTRATADA deve cumprir todas as obrigações constantes no Edital, seus anexos e na sua proposta, sobretudo do Termo de Referência, assumindo com exclusividade, os riscos e as despesas decorrentes da boa e perfeita execução do objeto;

#### **II - DA CONTRATANTE**

a) Receber o objeto no prazo e condições estabelecidas no Edital e seus anexos;

b) Efetuar o pagamento à CONTRATADA no valor correspondente ao fornecimento do objeto, no prazo e forma estabelecidos no Edital deste Pregão Eletrônico e seus anexos;

c) A CONTRATANTE não responderá por quaisquer compromissos assumidos pela CONTRATADA com terceiros, ainda que vinculados à execução do objeto da licitação, bem como, por qualquer dano causado a outrem, em decorrência de ato da CONTRATADA, de seus empregados, prepostos ou subordinados;

d) Efetuar os recolhimentos tributários incidentes sobre o objeto da licitação, na proporção prevista na legislação aplicável a matéria;

#### **CLÁUSULA SEXTA – Da Inexecução e da Rescisão do Contrato**

A inexecução total ou parcial do Contrato ensejará a sua rescisão com as consequências contratuais e as previstas em Lei, com assento no Capítulo III, Seção V, da Lei Federal nº 8.666, de 21 de junho de 1993, nos seguintes casos:

I – por ato unilateral e escrito da Contratante, nos casos enumerados nos incisos de I a XII, XVII e XVIII do artigo 78 da Lei Federal nº 8.666, de 21 de junho de 1993;

II – amigavelmente, por acordo entre as partes, desde que haja conveniência para a Administração, mediante formalização através de aviso com antecedência mínima de 30 dias, não cabendo indenização de qualquer das partes, exceto para pagamento dos fornecimentos comprovadamente prestados;

III – judicialmente, na forma da legislação vigente;

IV – a rescisão contratual determinada por ato unilateral, em que constatado o descumprimento do avençado, acarreta as seguintes consequências para a CONTRATADA, sem prejuízo das sanções previstas:

a) execução dos valores das multas e indenizações devidas à CONTRATANTE;

b) retenção dos créditos decorrentes do Contrato até o limite dos prejuízos causados à CONTRATANTE.

#### **CLÁUSULA SÉTIMA - DA FISCALIZAÇÃO DO CONTRATO**

A gestão do Contrato será realizada pela Udesc devendo ser observado o disposto no art. 67 da Lei 8.666/93, e suas alterações posteriores, bem como na Instrução Normativa UDESC Nº 017, de 25 de novembro de 2019.

A execução do Contrato será acompanhada e fiscalizada por servidor(es) designado(s) pela Udesc, para esse fim, na forma dos artigos 67 e 73 da Lei nº 8.666/93, bem como na Instrução Normativa UDESC Nº 017, de 25 de novembro de 2019.

A fiscalização exercida pelo(s) fiscal(ais) do Contrato, não reduz nem exclui a responsabilidade da CONTRATADA, inclusive de terceiros, por qualquer irregularidade.

#### **CLÁUSULA OITAVA– Das Sanções Administrativas**

As empresas que não cumprirem as normas de licitação e as obrigações contratuais ora assumidas estarão sujeitas às sanções e penalidades estabelecidas na Lei Federal nº 8.666, 21 de junho de 1993, e conforme antevisto no Edital do certame.

#### **CLÁUSULA NONA– DO FORO**

Fica eleito o Foro da Comarca da Capital, do Estado de Santa Catarina, com a renúncia expressa de qualquer outro, para serem dirimidas questões originárias da execução do presente Contrato.

E, por assim estarem justas e contratadas, as partes assinam o presente Termo Digitalmente.

**Florianópolis/SC**, conforme datas das assinaturas digitais.

(Assinatura Digital)

FUNDAÇÃO UNIVERSIDADE DO ESTADO DE  
SANTA CATARINA - UDESC

**CONTRATANTE**

(Assinatura Digital)

**CONTRATADA**



**ANEXO V**

**PREGÃO ELETRÔNICO nº 1204/2022**  
**MODELO DE AUTORIZAÇÃO DE FORNECIMENTO/ORDEN DE SERVIÇO**

Autorização de fornecimento vinculada a Ata de Registro de Preços e ao Edital de Pregão Eletrônico nº \_\_\_\_/2022

Autorização de fornecimento / Ordem de Serviço nº \_\_\_\_/2022

Fornecedor:			Endereço:		
CNPJ/MF:			Bairro:		CEP:
Banco:	Agência:	Conta:	Município:	UF:	Telefone:
			e-mail:		

  

ITEM	Descrição dos Materiais	Unidade	Quantidade	Preço (R\$)	Preço Total (R\$)
01					
02					
TOTAL DA AF (R\$):					

  

ATENÇÃO – EMITIR NOTA FISCAL EM NOME DE	UNID. ORÇAMENT.	SUB-AÇÃO	NATUREZA	FONTE	Quantidade	Valor (R\$)
(Centro participante – Anexo I e II)						

**Local da Entrega:**

**Fiscal da AF:**

**Vigência da AF:**

**ATENÇÃO:**

**1) Frete – CIF**

**2)** para efeitos de pagamento, apresentar: Nota Fiscal; CND do Estado de Santa Catarina e do Estado sede do fornecedor; CND municipal; CND da União; INSS e FGTS;

**3)** advertimos que o não cumprimento das obrigações assumidas na fase licitatória e/ou na execução desta A.F. estarão sujeitas às sanções previstas;

**4)** são partes integrantes desta Autorização de fornecimento, como se transcritos estivessem, o edital de licitação, seus anexos, a Ata de Registro de Preços e quaisquer complementos, os documentos, propostas e informações apresentadas pela licitante vencedora e que deram suporte ao julgamento da licitação.

Florianópolis, .....

Assinatura do Ordenador Primário

**ANEXO VI**  
**PREGÃO ELETRÔNICO Nº 1204/2022**

**INFORMAÇÕES DA EMPRESA VENCEDORA PARA CONTRATAÇÃO**

**Razão Social/Nome:**

Endereço:

Município:

Estado:

CEP:

CNPJ:

Telefones: ( )

E-Mail:

Banco:

Agência:

Conta:

**Representante legal/Nome responsável pela assinatura da ARP/Contratos:**

CPF:

Documento de Identidade:

Cargo/Função na empresa:

Telefones: ( )      Celular: ( )

Local e data, .....

NOME, CARGO E ASSINATURA  
DO REPRESENTANTE DA EMPRESA