

MINISTÉRIO DA EDUCAÇÃO
UNIVERSIDADE FEDERAL DE SANTA MARIA

EDITAL DE PREGÃO ELETRÔNICO Nº 051/2020
(SRP)

A Universidade Federal de Santa Maria, por meio de seu pregoeiro, designado pela Portaria nº 96.463 de 17 de outubro de 2019, torna público para conhecimento dos interessados, que realizará Licitação na Modalidade PREGÃO ELETRÔNICO, **do TIPO MENOR PREÇO GLOBAL POR GRUPO**, para o **REGISTRO DE PREÇOS PARA AQUISIÇÃO E INSTALAÇÃO DE EQUIPAMENTO DE SOLUÇÃO DE FIREWALL DE PRÓXIMA GERAÇÃO PARA SEGURANÇA DE INFORMAÇÃO PARA O CENTRO DE PROCESSAMENTO DE DADOS DA UNIVERSIDADE FEDERAL DE SANTA MARIA – UFSM**, especificados no item 2, pelo período de **12 (doze) meses**, a partir da data de homologação da presente licitação, de acordo com o que prescreve a Lei 10.520 de 17 de julho de 2002, Lei 8.666, de 21 de junho de 1993, e suas alterações posteriores, e em conformidade com o Decreto 10.024/2019 de 20 de setembro de 2019, Decreto 7.892, de 23 de janeiro de 2013, alterado pelo Decreto 9.488 de 30 de agosto de 2018, Lei Complementar 123, de 14 de dezembro de 2006, alterada pela Lei Complementar 147 de 07 de agosto de 2014 e Instrução Normativa nº 03 de 26 de abril de 2018.

DATA: 10/07/2020.

HORÁRIO: 09:00 horas (horário de Brasília).

LOCAL: www.comprasgovernamentais.gov.br

UASG: 153164

1.1. A presente licitação visa o registro, em ata, dos preços dos itens licitados, nas quantidades expressas na listagem anexa ao presente deste Edital, tendo em vista o que consta do Processo nº. **23081.021471/2020-56**.

2. DO OBJETO DA LICITAÇÃO

2.1. Esta licitação tem por objeto o **REGISTRO DE PREÇOS PARA AQUISIÇÃO E INSTALAÇÃO DE EQUIPAMENTO DE SOLUÇÃO DE FIREWALL DE PRÓXIMA GERAÇÃO PARA SEGURANÇA DE INFORMAÇÃO PARA O CENTRO DE PROCESSAMENTO DE DADOS DA UNIVERSIDADE FEDERAL DE SANTA MARIA-UFSM**, constantes no Termo de Referência, em anexo ao presente Edital, que faz parte deste Edital, como se aqui estivesse transcrito.

2.1.1. As quantidades constantes da relação anexa serão fornecidas pela Licitante Vencedora, relativas a cada item, mediante a emissão da Nota de Empenho, de acordo com o disposto neste Edital e condições expressas na proposta, através de fornecimento parcial, de acordo com as necessidades da Unidade Solicitante da UFSM.

2.1.2 **Os descritivos e unidades a serem considerado na elaboração de proposta são os que constam no termo de referência emitido pela UFSM e devem ser os entregue a cada empenho pela licitante vencedora.**

2.1.3. O contrato vigorará por **36 (trinta e seis) meses**, contados a partir da data da sua assinatura, podendo ser prorrogado por períodos iguais e sucessivos, limitado a **60(sessenta)meses** desde que haja preços e condições mais vantajosas para a Administração, nos termos do Inciso II, Art. 57,

da Lei nº 8.666, de 1993.

2.1.4 A prorrogação do contrato dependerá da verificação da manutenção da necessidade, economicidade e oportunidade da contratação, acompanhada de a realização de pesquisa de mercado que demonstre a vantajosidade dos preços contratados para a Administração.

2.1.5 O prazo de entrega do equipamento deverá ocorrer em até no máximo 90 (noventa) dias corridos a partir da data de assinatura do contrato.

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

2.1.7 A implantação completa da solução deve ser concluída em até 30 (trinta) dias corridos após a entrega do objeto.

2.1.8 Toda solução deste termo de referência deverá considerar período de garantia por um prazo de até 3 anos, para hardware e licenças de software.

2.1.9. Os serviços de garantia deverão ser prestados pelo próprio fabricante da solução ofertada ou por empresa autorizada oficialmente pelo fabricante a prestar este tipo de serviço no Brasil.

2.1.10 Como comprovação de autorizada, deverá ser apresentado documento com informações da empresa prestadora da assistência técnica com sua identificação, endereço, CNPJ, responsável técnico e região de atuação.

2.1.11. A licitante vencedora não poderá transferir a terceiros o objeto lícitado.

3. DAS CONDIÇÕES PARA PARTICIPAÇÃO

3.1. Poderão participar deste Pregão os interessados do ramo de atividade pertinente ao objeto da contratação que atenderem a todas as exigências constantes deste Edital e seus Anexos.

3.2. A licitante deverá estar cadastrada no Sistema de Cadastro Unificado de Fornecedores – SICAF, na forma da Lei.

3.3. Como condição de participação da presente licitação, a licitante, NÃO deverá:

A) Possuir em seu quadro societário nenhum Servidor Público Federal, salvo na forma executada no Inciso X do artigo nº 117 da Lei 8.112/90.

B) Possuir em seu quadro, atuando de forma direta ou indireta, nenhum servidor ou dirigente da UFSM, conforme dispõe o Inciso III do artigo 9º da Lei 8.666/93.

3.4 A licitante deverá assinalar “sim” ou “não” em campo próprio do sistema eletrônico, relativo às seguintes declarações:

a) que cumpre plenamente os requisitos de habilitação e que sua proposta está em conformidade com as exigências do instrumento convocatório e seus anexos.

b) que cumpre os requisitos estabelecidos no artigo 3º da Lei Complementar nº 123, de 2006, estando apta a usufruir do tratamento favorecido estabelecido em seus arts. 42 a 49;

c) que inexistem fatos impeditivos para sua habilitação no certame, ciente da obrigatoriedade de declarar ocorrências posteriores;

- d) que não emprega menor de 18 anos em trabalho noturno, perigoso ou insalubre e não emprega menor de 16 anos, salvo menor, a partir de 14 anos, na condição de aprendiz, nos termos do artigo 7º, XXXIII, da Constituição;
- e) que a proposta foi elaborada de forma independente, nos termos da Instrução Normativa SLTI/MP nº 2, de 16 de setembro de 2009;
- f) que não possui, em sua cadeia produtiva, empregados executando trabalho degradante ou forçado, observando o disposto nos incisos III e IV do art. 1º e no inciso III do art. 5º da Constituição Federal;
- g) que os serviços são prestados por empresas que comprovem cumprimento de reserva de cargos prevista em lei para pessoa com deficiência ou para reabilitado da Previdência Social e que atendam às regras de acessibilidade previstas na legislação, conforme disposto no art. 93 da Lei nº 8.213, de 24 de julho de 1991.

3.5. Não será permitida a participação de empresas estrangeiras que não funcionem no País, de interessados que se encontrem sob falência, concordata, concurso de credores, dissolução e liquidação, de consórcio de empresas, qualquer que seja sua forma de constituição, estando também abrangidos pela proibição aqueles que tenham sido punidos com suspensão do direito de licitar e contratar com a Administração Pública, ou declarados inidôneos para licitar ou contratar com a Administração Pública.

4. DO CREDENCIAMENTO

4.1. O credenciamento dar-se-á pela atribuição da chave de identificação e da senha, pessoal e intransferível, para acesso ao sistema eletrônico, no sítio: www.comprasgovernamentais.gov.br.

4.2. O credenciamento da Licitante dependerá de registro atualizado, bem como a sua manutenção, no Sistema de Cadastramento Unificado de Fornecedores-SICAF.

4.3. O uso da senha de acesso pela licitante é de sua responsabilidade exclusiva, incluindo qualquer transação efetuada diretamente ou por seu representante, não cabendo ao provedor do sistema ou à UFSM responsabilidade por eventuais danos decorrentes de uso indevido da senha, ainda que por terceiros.

4.4. O credenciamento junto ao provedor do sistema implica na responsabilidade legal da licitante e a presunção de sua capacidade técnica para realização das transações inerentes a este pregão eletrônico.

5. DA APRESENTAÇÃO DA PROPOSTA E DOS DOCUMENTOS DE HABILITAÇÃO

5.1 Os licitantes encaminharão, exclusivamente por meio do sistema, **concomitantemente com os documentos de HABILITAÇÃO exigidos no edital, proposta com a descrição do objeto ofertado e o preço, até a data e o horário estabelecidos para abertura da sessão pública**, quando, então, encerrar-se-á automaticamente a etapa de envio dessa documentação.

5.2 O envio da proposta, acompanhada dos documentos de habilitação exigidos neste Edital, ocorrerá por meio de chave de acesso e senha.

5.3 Os licitantes poderão deixar de apresentar os documentos de habilitação que constem do SICAF, assegurado aos demais licitantes o direito de acesso aos dados constantes dos sistemas.

5.4 As Microempresas e Empresas de Pequeno Porte deverão encaminhar a documentação de habilitação, ainda que haja alguma restrição de regularidade fiscal e trabalhista, nos termos do art. 43, § 1º da LC nº 123, de 2006.

5.5 Incumbirá ao licitante acompanhar as operações no sistema eletrônico durante a sessão pública do Pregão, ficando responsável pelo ônus decorrente da perda de negócios, diante da inobservância de quaisquer mensagens emitidas pelo sistema ou de sua desconexão.

5.6 Até a abertura da sessão pública, os licitantes poderão retirar ou substituir a proposta e os documentos de habilitação anteriormente inseridos no sistema;

5.7 Não será estabelecida, nessa etapa do certame, ordem de classificação entre as propostas apresentadas, o que somente ocorrerá após a realização dos procedimentos de negociação e julgamento da proposta.

5.8 Os documentos que compõem a proposta e a habilitação do licitante melhor classificado somente serão disponibilizados para avaliação do pregoeiro e para acesso público após o encerramento do envio de lances.

5.9. A licitante será responsável pelas transações efetuadas em seu nome, assumindo como firmes e verdadeiras suas propostas e lances, inclusive os atos praticados diretamente ou por seu representante, não cabendo ao provedor do sistema ou à UFSM responsabilidade por eventuais danos decorrentes de uso indevido da senha, ainda que por terceiros.

5.10. A PROPOSTA DEVERÁ CONTER:

5.10.1. O Preço **unitário e total** (CIF), por item, para cada item cotado.

5.10.1.1. As propostas analisadas serão as incluídas **exclusivamente** no sítio das compras governamentais. **Propostas impressas não serão consideradas.**

5.10.2. Citar a **marca** para cada item cotado, no sistema compras governamentais, não sendo aceito outra forma de envio.

5.10.2.1. As propostas apresentadas que não identificarem a marca do produto ofertado, poderão ser desclassificadas.

5.10.3. Especificação clara do objeto de acordo com o Termo de Referência em anexo ao presente Edital.

5.10.4. Nos preços de cada produto deverão estar incluídos, obrigatoriamente, impostos, fretes, taxas e demais incidências.

5.10.5. Na cotação de preços unitários serão aceitos **até 04 (quatro)** dígitos após a vírgula.

5.10.6. O pregoeiro verificará as propostas apresentadas, desclassificando aquelas que não estejam de acordo com os requisitos estabelecidos neste Edital.

5.10.7. A desclassificação da proposta será fundamentada, registrada e acompanhada em tempo, no sistema eletrônico.

5.10.8. O descumprimento das regras supramencionadas pela UFSM por parte das licitantes pode ensejar a fiscalização do Tribunal de Contas da União e, após o devido processo legal, gerar as seguintes consequências: assinatura de prazo para a adoção das medidas necessárias ao exato cumprimento da lei, nos termos do art. 71, inciso IX, da Constituição; ou condenação dos agentes públicos responsáveis e da licitante vencedora ao pagamento dos prejuízos ao erário, caso

verificada a ocorrência de superfaturamento por sobrepreço na execução do contrato.

6. DA ABERTURA DA SESSÃO E DA FORMULAÇÃO DOS LANCES

6.1. A abertura da presente licitação dar-se-á em sessão pública, por meio de sistema eletrônico, na data, horário e local indicados neste Edital.

6.2. O sistema ordenará, automaticamente, as propostas classificadas pelo pregoeiro, sendo que somente estas participarão da fase de lance.

6.3. Iniciada a etapa competitiva, as licitantes poderão encaminhar lances exclusivamente por meio de sistema eletrônico, sendo a licitante imediatamente informada, pelo sistema, o recebimento dos lances e o valor consignado no registro.

6.3.1. Os lances deverão ser ofertados para o valor unitário do item.

6.4. As licitantes poderão oferecer lances sucessivos, observados o horário fixado para abertura da sessão e as regras estabelecidas neste Edital.

6.5. A licitante somente poderá oferecer lance inferior ao último por ele ofertado e registrado pelo sistema.

6.6. Não serão aceitos dois ou mais lances iguais, prevalecendo aquele que for recebido e registrado primeiro no sistema.

6.7. Durante o transcurso da sessão pública, as licitantes serão informadas em tempo real, do valor do menor lance registrado, vedada a identificação da licitante.

6.8 MODO DE DISPUTA

6.8.1 *Será adotado para o envio de lances no pregão eletrônico o modo de disputa “aberto e fechado”, em que os licitantes apresentarão lances públicos e sucessivos, com lance final e fechado.*

6.8.2 *A etapa de lances da sessão pública terá duração inicial de 15 (quinze) minutos. Após esse prazo, o sistema encaminhará aviso de fechamento iminente dos lances, após o que transcorrerá o período de tempo de até 10 (dez) minutos, aleatoriamente determinado, findo o qual será automaticamente encerrada a recepção de lances.*

6.8.3 *Encerrado o prazo previsto no item anterior, o sistema abrirá oportunidade para que a licitante da oferta de valor mais baixo e as das ofertas com preços até 10% (dez por cento) superior àquela possam ofertar um lance final e fechado em até 05 (cinco) minutos, o qual será sigiloso até o encerramento deste prazo.*

6.8.3.1. *Não havendo pelo menos 03 (três) ofertas nas condições definidas neste item, poderão as licitantes dos melhores lances, na ordem de classificação, até o máximo de 03 (três), oferecer um lance final e fechado em até 05 (cinco) minutos, o qual será sigiloso até o encerramento deste prazo.*

6.8.4 *Após o término dos prazos estabelecidos nos itens anteriores, o sistema ordenará os lances segundo a ordem crescente de valores.*

6.8.4.1. *Não havendo lance final e fechado classificado na forma estabelecida nos itens anteriores, haverá o reinício da etapa fechada, para que as demais licitantes, até o máximo de 03 (três), na ordem de classificação, possam ofertar um lance final e fechado em até 05 (cinco) minutos, o qual será sigiloso até o encerramento deste prazo.*

6.8.5 *Na hipótese de não haver licitante classificada na etapa de lance fechado que atenda às exigências para habilitação, o pregoeiro poderá, auxiliado pela equipe de apoio, mediante justificativa, admitir o reinício da etapa fechada.*

6.9. No caso de desconexão do pregoeiro, no decorrer da etapa competitiva do pregão, se o sistema eletrônico permanecer acessível às licitantes, os lances continuarão sendo recebidos, sem prejuízos aos atos realizados.

6.10. Quando a desconexão do pregoeiro persistir por tempo superior a dez (10) minutos, a sessão do pregão eletrônico será suspensa e terá reinício somente após comunicação expressa do pregoeiro aos participantes.

6.11 Após o encerramento dos lances, se a proposta de menor valor não for ofertada por microempresa ou empresa de pequeno porte e houver proposta apresentada por microempresa ou empresa de pequeno porte igual ou até 5% (cinco por cento) superior à proposta mais bem classificada, proceder-se-á da seguinte forma:

6.11.1. A microempresa ou empresa de pequeno porte mais bem classificada poderá, no prazo de 5 (cinco) minutos após a convocação, apresentar proposta de preço inferior àquela considerada vencedora do certame, situação em que será adjudicado em seu favor o objeto licitado.

6.11.2. No caso de equivalência dos valores apresentados pelas microempresas ou empresa de pequeno porte que se encontrem nos intervalos estabelecidos no subitem 6.11 deste edital, será realizado sorteio entre elas para que se identifique àquela que primeiro poderá apresentar melhor oferta.

6.12 Persistindo o empate, a proposta vencedora será sorteada pelo sistema eletrônico dentre as propostas empatadas.

6.13. Após o encerramento da etapa de lances da sessão pública, o pregoeiro deverá encaminhar, pelo sistema eletrônico, contraproposta à licitante que tenha apresentado lance mais vantajoso, para que seja obtida melhor proposta, observado o critério de julgamento, não se admitindo negociar condições diferentes daquelas previstas neste edital.

7. DO JULGAMENTO E ACEITAÇÃO DAS PROPOSTAS

7.1. Após a negociação, caso o menor preço ofertado seja superior ao máximo admitido pela UFSM, o mesmo não será aceito.

7.2. Caso não se realize lance, será verificado a conformidade entre a proposta de menor preço e o valor estimado para a contratação, respeitado o estabelecido no subitem 7.1 deste edital.

7.3. Para julgamento e classificação das propostas será adotado o critério do **Menor Preço Global, (Grupo 01 – itens 01, 02, 03 e 04)**, observados as especificações constantes no Termo de Referência em anexo do presente Pregão.

7.4. Não ocorrendo a contratação da microempresa ou empresa de pequeno porte, na forma do subitem 6.11.1. deste edital, serão convocadas as remanescentes que porventura se enquadrem na hipótese do subitem 6.11. deste edital, na ordem classificatória, para o exercício do mesmo direito.

7.5. Na hipótese da não-contratação nos termos previstos nos subitens anteriores, o objeto licitado será adjudicado em favor da proposta originalmente vencedora do certame.

7.6. Se a oferta não for aceitável ou se a licitante não atender às exigências editalícias, o Pregoeiro examinará as ofertas subseqüentes e, assim sucessivamente, na ordem de classificação, até a apuração de uma proposta que atenda às especificações deste edital.

7.7. Declarada encerrada a etapa competitiva, o pregoeiro examinará a proposta classificada em primeiro lugar quanto à compatibilidade do preço em relação ao estimado para a contratação e verificará a habilitação da licitante, conforme disposto no item 8 deste Edital.

7.8. A indicação do lance da vencedora, a classificação dos lances apresentados e demais informações relativas à sessão pública do Pregão constarão na ata divulgada no sistema eletrônico, sem prejuízo das demais formas de publicidade previstas na legislação pertinente.

8. DA HABILITAÇÃO

8.1. Como condição de habilitação do licitante detentor da proposta classificada em primeiro lugar, o **Pregoeiro verificará** o eventual descumprimento das condições de participação, mediante a consulta *on line* aos seguintes cadastros:

I) SICAF, **nos níveis I, II e III**;

II) Consulta Consolidada de Pessoa Jurídica do Tribunal de Contas da União (<https://certidoes-apf.apps.tcu.gov.br/>).

8.1.1. O(s) documento(s) elencado(s) abaixo deverá(ao) ser incluído(s) pela licitante em campo próprio do sistema eletrônico, **no momento do envio da proposta**:

I. A licitante deverá comprovar a sua qualificação, mediante a apresentação, em uma única via, de cópia(s) autenticada(s), ou cópia(s) acompanhada(s) do(s) original(is), de atestado(s), expedido(s) por pessoas jurídicas de direito público ou privado, que comprove(m) a aptidão para desempenho de atividades pertinentes ao objeto da licitação. No(s) atestado(s) deverá constar o nome da pessoa de contato e telefone. Caso conste informações desatualizadas no(s) atestado(s) a licitante deverá informar os dados atualizados.

II. O atestado acima referido deverá conter identificação do emitente, características e localização da prestação do serviço, local, data da expedição e declaração do emitente do atestado de que o serviço foi realizado a contento. Os atestados devem ser em nome da LICITANTE, e elaborados em papel timbrado da empresa emitente, contendo os seguintes dados mínimos e obrigatórios: a) Razão Social, CNPJ e endereço completo da empresa emitente; b) Razão Social da LICITANTE; c) Vigência: de ___/___/___ a ___/___/___; d) Objeto do contrato; e) Descrição do objeto do contrato: (descrição detalhada dos serviços prestados); f) Local e Data de emissão do Atestado; g) Nome, assinatura do signatário, telefone e e-mail de contato da empresa emitente

III. A licitante deverá possuir, pelo menos, técnicos certificados pelo fabricante compatível com o objeto deste termo de referência;

IV. A comprovação de vínculo profissional entre a licitante e o(s) técnicos indicados na linha (III) fará com a apresentação de cópia da carteira de trabalho (CTPS) em que conste o licitante como contratante; do contrato social do licitante em que conste o profissional como sócio; do contrato de prestação de serviços, sem vínculo trabalhista, regido pela legislação civil ou, ainda, de declaração de contratação futura do profissional, desde que acompanhada de declaração de

anuência do profissional.

8.1.1.1 Os documentos mencionados no item 8.1.1 deverão ser apresentados como forma de anexo no local específico deste edital no site www.comprasgovernamentais.gov.br.

8.2. No caso de participação de Microempresa e Empresa de Pequeno Porte na presente licitação, estas serão HABILITADAS mesmo que apresentarem alguma restrição na comprovação de regularidade fiscal, sendo que a regularidade da sua situação deverá ser efetuada nos moldes do subitem 8.2.1 deste edital, como condição de adjudicação.

8.2.1 Havendo alguma restrição na comprovação da regularidade fiscal, as Microempresa (ME) ou Empresa de Pequeno Porte (EPP), será assegurado o prazo de 5 (cinco) dias úteis, cujo termo inicial corresponderá ao momento em que o proponente for declarado o vencedor do certame, prorrogáveis por igual período, a critério da Administração Pública, para a regularização da documentação, pagamento ou parcelamento do débito, e emissão de eventuais certidões negativas ou positivas com efeito de certidão negativa.

8.2.2. A prorrogação que se refere o subitem 8.2.1 deste edital deverá ser solicitada pela licitante interessada, cujo prazo para o encaminhamento da solicitação, devidamente formalizada, deverá ser até a data final do primeiro período.

8.2.3. A não-regularização da documentação, no prazo previsto no subitem 8.2.1 deste edital, implicará decadência do direito à contratação, sem prejuízo das sanções previstas no art. 81 da Lei no 8.666, de 21 de junho de 1993, sendo facultado à Administração convocar os licitantes remanescentes, na ordem de classificação, para a contratação, ou revogação da licitação.

9. DA HOMOLOGAÇÃO DA LICITAÇÃO

9.1. O prazo da homologação da presente licitação será no máximo 15 (quinze) dias, contados a partir da data da adjudicação da presente licitação.

9.2. No momento da homologação, o ordenador de despesa convocará para o registro dos licitantes que aceitarem o objeto da presente licitação com preços iguais aos da licitante vencedora na sequência da classificação do certame.

9.2.1. Será concedido um prazo não inferior a 24 (vinte e quatro) horas para as licitantes com propostas não recusadas manifestarem interesse na intenção de participar no cadastro reserva.

9.3. O registro referente ao subitem 9.2 deste edital tem por objetivo a formação de cadastro de reserva no caso de impossibilidade de atendimento pelo primeiro colocado da ata, nas hipóteses previstas nos arts. 20 e 21 do Decreto n. 7.892/2013, alterado pelo Decreto n. 8.250/2014.

9.4. A licitante vencedora terá prazo de 05 (cinco) dias para a assinatura do contrato, após a convocação feita pela UFSM, sob pena de decair o direito à contratação.

9.4.1. Como garantia contratual, a licitante vencedora caucionará uma quantia equivalente a 5% (cinco por cento) do valor contratado, através de:

- a) Caução em dinheiro ou títulos da dívida pública;
- b) Fiança bancária e ou
- c) Seguro-garantia.

9.4.2. Caberá à licitante vencedora optar por uma das modalidades de garantia acima enumeradas, no momento da assinatura do contrato, efetuando o depósito ou a entrega da documentação referente à mesma, no prazo máximo de 10 (dez) dias após a assinatura do Contrato, sob pena de decair do direito de adjudicação.

10. DO PEDIDO DE ESCLARECIMENTOS E DA IMPUGNAÇÃO DO EDITAL

10.1. Até 03 (três) dias úteis antes da data fixada para abertura da sessão pública, qualquer pessoa poderá solicitar, ao pregoeiro, esclarecimentos e/ou impugnar o edital, exclusivamente por meio eletrônico, no seguinte endereço: pregao@ufsm.br.

10.2. Caberá ao Pregoeiro decidir sobre a petição no prazo de 02 (dois) dias úteis contados da data de recebimento do pedido de esclarecimentos e/ou impugnação.

10.4. Acolhida a petição contra o Edital, será definida e publicada nova data para a realização do certame.

10.5. As respostas aos pedidos de esclarecimentos serão divulgadas através do sistema e vincularão os participantes e a UFSM, nos casos em que a Administração julgar necessário.

11. DOS RECURSOS ADMINISTRATIVOS

11.1. Declarado o vencedor, qualquer licitante poderá, durante a sessão pública, de forma imediata e motivada, em campo próprio do sistema, manifestar sua intenção de recorrer, quando lhe será concedido o prazo de 03 (três) dias para apresentação das razões do recurso, ficando os demais licitantes desde logo intimados para, querendo, apresentarem contrarrazões em igual prazo, que começará a contar do término do prazo do recorrente, sendo-lhes assegurada vista imediata dos elementos indispensáveis à defesa dos seus interesses.

11.2. O acolhimento do recurso importará na invalidação apenas dos atos insuscetíveis de aproveitamento.

12. DA FORMALIZAÇÃO DA ATA DE REGISTRO DE PREÇOS

12.1. A Ata da realização do Pregão Eletrônico, publicada no sítio: www.comprasgovernamentais.gov.br, terá efeito de compromisso de fornecimento nas condições e prazo estipulados no Edital.

12.1.1. O Registro de Preços será formalizado mediante a assinatura do Termo de Registro de Preços, conforme modelo no Anexo 01 deste Edital. O Termo de Registro de Preços deverá ser enviado pelas licitantes vencedoras após a homologação do pregão.

12.1.2. A Licitante vencedora após a homologação do pregão, deverá, imediatamente, enviar o referido Termo de Registro de Preços devidamente preenchido, assinado e datado, através do e-mail: pregao@ufsm.br.

12.2. A existência de preços registrados não assegura ao licitante o direito ao fornecimento do objeto, podendo a Administração, se assim entender, promover nova licitação específica para aquisição dos mesmos, sendo assegurada, entretanto, ao fornecedor com preço registrado o fornecimento em igualdade de condições.

13. DOS RECURSOS ORÇAMENTÁRIOS.

13.1. Os recursos orçamentários, para fazer frente às despesas da presente licitação serão alocados quando da emissão de Notas de Empenho, em caso de necessidade de aquisição, obedecido o prazo de entrega previsto na proposta.

14. DO PAGAMENTO

14.1. O pagamento será efetuado mediante a apresentação da Nota Fiscal, devidamente certificada, acusando o recebimento, por parte do responsável pelo órgão solicitante/UFSM. O prazo para pagamento será de no máximo 30 (trinta) dias a partir da data de sua entrega na UFSM, desde que não haja impedimento legal.

14.1. O pagamento será atualizado monetariamente pela variação INPC/IBGE, ocorrida no período, a partir da data do prazo final do adimplemento da obrigação até o efetivo pagamento.

15. DAS PENALIDADES

15.1. As sanções contratuais são as previstas no artigo 7º da Lei 10.520/2002 e artigo 49 do Decreto n. 10.024/2019.

15.2. A multa em caso de atraso na entrega dos produtos/serviços solicitados será de 0,5% (cinco décimos por cento) ao dia sobre o valor do produto não entregue.

15.2.1. A licitante vencedora incorrerá em atraso na entrega do objeto licitado se não fornecer o produto a partir do 1º (primeiro) dia após o prazo estipulado no item 16.5 do Edital.

15.3. A Multa em caso de inadimplemento da licitante vencedora será de 20% (vinte por cento) sobre o valor empenhado que, requisitado, deixar de ser entregue.

15.3.1. A licitante vencedora será considerada inadimplente se a partir do 15º (décimo quinto) dia da não entrega do produto/serviço, após o prazo estipulado no item 16.5 deste Edital.

15.3.2. A licitante vencedora também será considerada inadimplente se não cumprir com as condições estipuladas no Termo de Referência em anexo ao presente edital.

16. DAS DISPOSIÇÕES GERAIS

16.1. À Universidade, por interesse público justificado, é reservado o direito de revogar este Registro de Preços, nos termos da legislação, sem que caiba aos participantes, direito à reclamação ou indenização.

16.2. A simples participação nessa licitação implica na aceitação plena e incondicional do inteiro teor expresso neste Edital, desde que transcorrido "in albis", o prazo estabelecido no art. 41, § 2º da Lei 8.666/93.

16.3. Serão concedidas adesões ao presente registro de preços até o dobro do quantitativo de cada item registrado na ata de registro de preços, respeitadas as condições estabelecidas no Decreto n. 7.892, de 23 de janeiro de 2013, alterado pelo Decreto 9.488 de 30 de agosto de 2018.

16.4. A instalação deverá ser prestada conforme especificações no Termo de Referência.

16.4.1. O produto/serviço fornecido fora das especificações ficará sujeito à imediata substituição pelo fornecedor, sem qualquer ônus para a UFSM.

16.5. O prazo de *fornecimento total dos produtos, objeto de cada Nota de Empenho* não poderá **exceder 90 (noventa) dias** a contar do recebimento do mesmo. O prazo indicado pela unidade solicitante para a entrega parcelada do objeto empenhado deverá ser rigorosamente observado, sujeitando a licitante vencedora às cominações previstas no presente Edital.

16.6. O prazo de validade da proposta será de 60 (sessenta) dias, após a fase de lances. Se o pregão não for homologado até este prazo, a proposta perderá sua vigência.

16.7. Após a homologação do presente pregão, a licitante vencedora obriga-se a manter sua proposta pelo prazo de vigência do Registro de Preços, indicada no “caput” deste Edital.

16.8. Não haverá reajuste de preços durante a vigência do Registro de Preços, de que trata o presente Edital.

16.9. O produto fornecido fora das especificações ficará sujeito à imediata substituição pelo fornecedor, sem qualquer ônus para a Universidade.

16.10. As condições e preços acolhidos na proposta aceita serão irreversíveis, na forma determinada pelo Edital.

16.11. A licitante vencedora obriga-se a manter durante o período de vigência do Registro de Preços, as condições de qualificação e habilitação exigidas no ato convocatório.

16.12. No caso e não haver expediente no dia marcado para a realização esta licitação, a mesma será realizada no primeiro dia útil subsequente, mantidas todas as demais condições.

16.13. O resultado desta Licitação estará disponível, após a homologação, no sítio <http://comprasnet.gov.br/aceso.asp?url=/livre/Resultado/conreelit00.asp> e na página da UFSM, no endereço <http://coral.ufsm.br/demapa/index.php/licitacoes/resultado>.

16.14. Cópias deste Edital estão disponíveis para download nos portais www.comprasgovernamentais.gov.br e site.ufsm.br.

16.15. Em atendimento à Lei nº. 12.846/2013, para a participação neste certame, nenhuma das partes poderá oferecer dar ou se comprometer a dar a quem quer que seja, ou aceitar ou se comprometer a aceitar de quem quer que seja, tanto por conta própria quanto através de outrem, qualquer pagamento, doação, compensação, vantagens financeiras ou não financeiras ou benefícios de qualquer espécie que constituam prática ilegal ou de corrupção sob as leis de qualquer país, seja de forma direta ou indireta quanto ao objeto deste certame, ou de outra forma que não relacionada a este certame, devendo garantir, ainda, que seus prepostos e colaboradores ajam da mesma forma.

16.16. As dúvidas e inadimplência serão resolvidas no foro da Justiça Federal no Estado do Rio Grande do Sul, na cidade de Santa Maria.

16.17. Informações e outros elementos necessários ao perfeito conhecimento do objeto desta licitação, serão solicitados ao pregoeiro, exclusivamente através do endereço eletrônico: pregao@ufsm.br

16.18. As cópias originais ou autenticadas dos documentos solicitados neste edital deverão ser remetidas, quando convocados pelo pregoeiro, em até 03 (três) dias úteis após a homologação do pregão para o seguinte endereço:

UNIVERSIDADE FEDERAL DE SANTA MARIA
CNPJ: 95.591.764/0001-05
Edifício da Administração Central,
Departamento de Material de Patrimônio
6º andar, sala 666 – Comissão de Licitações
CEP: 97105-900, Campus Universitário
Bairro Camobi, Santa Maria, RS

Santa Maria – RS, 24 de junho de 2020.

Jane Lucia Sartori Lampert
Coordenadora de Editais e contratos

ANEXO 01

TERMO DE REGISTRO DE PREÇOS

Pelo presente a Empresa _____, CNPJ
_____/_____-_____, estabelecida à Rua
_____, CEP _____-_____, em
_____ - _____ concorda plenamente com o Edital e os termos da Ata
de Realização do Pregão Eletrônico constante no sítio do comprasgovernamentais.gov.br, referente
ao Pregão Eletrônico nº ____/____, Processo nº _____/_____-_____/ UFSM, como se aqui
estivesse transcrito.



Em ____/____/_____.

Assinatura

Termo de Compromisso Anexo II

A _____, CNPJ _____, por intermédio de seu representante _____ legal _____ abaixo assinado, _____, CPF _____, doravante designados simplesmente CONTRATADA e RESPONSÁVEL, se comprometem, por intermédio do presente TERMO DE COMPROMISSO, a não divulgar sem autorização, quaisquer Informações Confidenciais (conforme definido abaixo) em relação ao Projeto de Implantação de Next-Generation Firewall e de propriedade da Universidade Federal de Santa Maria, CNPJ 95.591.764/0001-05, doravante designada UFSM, em conformidade com as seguintes cláusulas e condições:

1. Por este instrumento, a Contratada declara estar apta a aceitar e receber INFORMAÇÕES com respeito ao parque tecnológico da UFSM, se comprometendo a manter absoluta confidencialidade destas INFORMAÇÕES, independente de solicitação expressa neste sentido pela UFSM ou quaisquer de seus representantes;
2. As INFORMAÇÕES abrangidas por este termo são de natureza técnica, operacional, comercial, jurídica e financeira expressas de forma escrita, verbal, ou em linguagem computacional em qualquer nível, ou de qualquer outro modo apresentada, ficando expressamente vedada sua divulgação a terceiros, a qualquer título;
3. As partes deverão restringir a divulgação das INFORMAÇÕES para o pessoal que estiverem diretamente envolvidos na sua utilização em razão do fornecimento das INFORMAÇÕES e da elaboração do serviço a ser fornecido, ficando vedado o intercâmbio destas INFORMAÇÕES com terceiros que não estejam diretamente envolvidos com a prestação dos serviços;
4. A CONTRATADA obriga-se a informar imediatamente a UFSM qualquer violação das regras de sigilo que tenha ocorrido por sua ação ou omissão, independentemente da existência de dolo, bem como de seus empregados, prepostos e prestadores de serviço;
5. A não observância de qualquer das disposições estabelecidas neste instrumento sujeitará a CONTRATADA aos procedimentos judiciais cabíveis relativos a perdas e danos que possam advir ao UFSM e aos seus usuários;
6. O descumprimento de quaisquer das cláusulas do presente Termo acarretará a responsabilidade civil e criminal de acordo com as leis aplicáveis dos que, comprovadamente, estiverem envolvidos no descumprimento ou violação.

Santa Maria, RS, _____ de _____ de _____.

Representante da UFSM: _____

Representante da Contratada: _____

ANEXO AO TERMO DE REFERÊNCIA AO PREGÃO 051-2020

1. OBJETO DA LICITAÇÃO

Esta licitação tem por objeto o Registro de Preços para contratação de solução de firewall de próxima geração para segurança da informação de perímetro que possibilite a visibilidade e controle de tráfego e aplicações em camada 7, filtragem de conteúdo web, prevenção contra ataques e ameaças avançadas e modernas, filtro de dados, VPN e controle granular de banda de rede, compreendendo fornecimento de equipamentos e softwares integrados em forma de appliance conforme quantidades e exigências estabelecidas neste instrumento.

2. Bens e serviços que compõem a solução

GRUPO	Id.	Descrição do Bem ou Serviço	Código CATMAT/CATSER	QTD	Métrica ou Unidade
1	1	FIREWALL TIPO 1 COM SUPORTE, GARANTIA E LICENÇAS DE PROTEÇÃO COM VIGÊNCIA DE 36 MESES.	150100	2	Peça
	2	FIREWALL TIPO 2 COM SUPORTE, GARANTIA E LICENÇAS DE PROTEÇÃO COM VIGÊNCIA DE 36 MESES.	150100	2	Peça
	3	SERVIÇOS DE INSTALAÇÃO DE FIREWALL	5398	4	Serviço
	4	TREINAMENTO OFICIAL DE FIREWALL DE PRÓXIMA GERAÇÃO	3840	4	Serviço

3. Estimativa da demanda

GRUPO	Item	Descrição	Valor unitário máximo
1	1	FIREWALL TIPO 1 COM SUPORTE, GARANTIA E LICENÇAS DE PROTEÇÃO COM VIGÊNCIA DE 36 MESES	R\$
	2	FIREWALL TIPO 2 COM SUPORTE, GARANTIA E LICENÇAS DE PROTEÇÃO COM VIGÊNCIA DE 36 MESES	R\$
	3	SERVIÇOS DE INSTALAÇÃO DE FIREWALL	R\$
	4	TREINAMENTO OFICIAL DE FIREWALL DE PRÓXIMA GERAÇÃO	R\$

4. OS PREÇOS

Id.	Descrição do Bem ou Serviço	Qtd	Unidade de medida	Valor unitário	Valor total
1	FIREWALL TIPO 1 COM SUPORTE, GARANTIA E LICENÇAS DE PROTEÇÃO COM VIGÊNCIA DE 36 meses	2	Peça	R\$	R\$
2	FIREWALL TIPO 2 COM SUPORTE, GARANTIA E LICENÇAS DE PROTEÇÃO COM VIGÊNCIA DE 36 meses	2	Peça	R\$	R\$
3	SERVIÇOS DE INSTALAÇÃO DE FIREWALL	4	Serviço	R\$	R\$
4	TREINAMENTO OFICIAL DE FIREWALL DE PRÓXIMA GERAÇÃO	4	Serviço	R\$	R\$

5. Parcelamento da Solução de TIC

Os equipamentos, licenças e serviços que constituem a solução aqui proposta se interagem entre si de forma a convergir para um sistema unificado, de modo que o fornecimento parcelado inviabilizaria a implantação de tecnologia capaz de atender as necessidades deste órgão.

A eventual divisão do objeto em grupos diversos poderia ocasionar uma situação onde um proponente "A", por não conhecer a solução, não teria condições de fornecer eventual licenciamento correto para tal ou mesmo propor equipamentos compatíveis. Ante ao exposto, é evidente que o agrupamento do objeto, de maneira a compor uma solução unificada, é necessário a fim de evitar eventuais problemas de compatibilidade.

Ademais, lidar com um único fornecedor diminui o custo administrativo de gerenciamento de todo o processo de contratação. O aumento da eficiência administrativa do setor público passa pela otimização do gerenciamento de seus contratos de fornecimento. Essa eficiência administrativa também é de estatura constitucional e deve ser buscada pela administração pública.

Por fim, o agrupamento em lote de todos os itens deste processo visa garantir a otimização dos prazos de execução, viabilizando a sincronia nos fornecimentos e serviços de instalações e treinamento, evitando assim que um fornecedor venha a prejudicar a execução de outro.

5.1. Resultados e Benefícios a Serem Alcançados

1. Adequação às legislações vigentes, tais como LGPD – Lei Geral de Proteção de Dados (Lei nº 13.709/2018) e Marco Civil da Internet Lei nº 12.965/2014);
2. Maior visibilidade do tráfego de rede e aplicações em camada 7, possibilitando a detecção e proteção em tempo real contra ameaças;
3. Proteção do ambiente de rede contra ameaças tipo worms, vírus, malwares entre outras pragas virtuais, atendendo às exigências do Marco Civil da Internet.
4. Geração de relatórios diversos para rápida análise de informações sobre tráfego, aplicações, ameaças, etc.
5. Implantação de controle de acesso à rede, possibilitando a rastreabilidade de usuários e

endereços IP, atendendo ao Marco Civil da Internet Lei nº 12.965/2014;

6. Melhoria da qualidade da internet disponibilizada, diminuindo perda e tempo de transmissão de pacotes;

7. Criação de políticas e medidas de segurança para proteção da rede contra-ataques e/ou invasões.

6 – ESPECIFICAÇÃO DOS REQUISITOS DA CONTRATAÇÃO

Aquisição de solução de proteção de rede com características de Next Generation Firewall (NGFW) para segurança de informação perimetral que inclui filtro de pacote, controle de aplicação, administração de largura de banda (QoS), VPN IPSec e SSL, IPS, prevenção contra ameaças de vírus, spywares e malwares “Zero Day”, Filtro de URL, bem como controle de transmissão de dados e acesso à internet compondo uma plataforma de segurança integrada e robusta.

6.1 CARACTERÍSTICAS GERAIS COMUNS AOS ITENS 1 E 2

1.1. A solução deve consistir em appliance de proteção de rede com funcionalidades de Next Generation Firewall (NGFW), e console de gerência e monitoração;

1.2. Por funcionalidades de NGFW entende-se: reconhecimento de aplicações, prevenção de ameaças, identificação de usuários e controle granular de permissões;

1.3. As funcionalidades de proteção de rede que compõe a plataforma de segurança, podem funcionar em múltiplos appliances desde que obedeçam a todos os requisitos desta especificação;

1.4. A plataforma deve ser otimizada para análise de conteúdo de aplicações em camada 7;

1.5. O hardware e software que executem as funcionalidades de proteção de rede, bem como a console de gerência e monitoração, devem ser do tipo appliance. Não serão aceitos equipamentos servidores e sistema operacional de uso genérico;

1.6. Todos os equipamentos fornecidos devem ser próprios para montagem em rack 19”, incluindo kit tipo trilho para adaptação se necessário e cabos de alimentação;

1.7. O software deverá ser fornecido em sua versão mais atualizada;

1.8. Os dispositivos de proteção de rede devem possuir pelo menos as seguintes funcionalidades:

1.8.1. Suporte a 4094 VLAN Tags 802.1q;

1.8.2. Agregação de links 802.3ad e LACP;

1.8.3. Policy based routing ou policy based forwarding;

1.8.4. Roteamento multicast (PIM-SM);

1.8.5. DHCP Relay;

1.8.6. DHCP Server;

1.8.7. Jumbo Frames;

1.8.8. Suporte a criação de objetos de rede que possam ser utilizados como endereço IP de interfaces L3

1.9. Suportar sub-interfaces ethernet lógicas;

1.9.1. Suporte a, no mínimo, 10 (dez) roteadores virtuais na mesma instância de firewall;

1.10. O firewall deve ter a capacidade de testar o funcionamento de rotas estáticas e rota default com a definição de um endereço IP de destino que deve estar comunicável através de uma rota. Caso haja falha na comunicação o firewall deve ter a capacidade de usar rota alternativa para estabelecer a comunicação;

1.11. Deve suportar os seguintes tipos de NAT:

1.11.1. Nat dinâmico (Many-to-1);

1.11.2. Nat dinâmico (Many-to-Many);

1.11.3. Nat estático (1-to-1);

1.11.4. NAT estático (Many-to-Many);

1.11.5. Nat estático bidirecional 1-to-1;

1.11.6. Tradução de porta (PAT);

1.11.7. NAT de Origem;

- 1.11.8. NAT de Destino;
- 1.11.9. Suportar NAT de Origem e NAT de Destino simultaneamente;
- 1.11.10. Deve implementar Network Prefix Translation (NPTv6), prevenindo problemas de roteamento assimétrico;
- 1.11.11. Deve implementar balanceamento de link através de políticas por usuário e grupos de usuários do LDAP/AD;
- 1.11.12. Deve implementar balanceamento de link através de políticas por aplicação e porta de destino;
- 1.11.13. Deve implementar o protocolo Link Layer Discovery (LLDP), permitindo que o appliance e outros ativos da rede se comuniquem para identificação da topologia da rede em que estão conectados e a função dos mesmos facilitando o processo de troubleshooting. As informações aprendidas e armazenadas pelo appliance devem ser acessíveis via SNMP;
- 1.11.14. Enviar log para sistemas de monitoração externos, simultaneamente;
- 1.11.15. Deve haver a opção de enviar logs para os sistemas de monitoração externos via protocolo TCP e SSL;
- 1.11.16. Deve permitir configurar certificado caso necessário para autenticação no sistema de monitoração externo de logs;
- 1.11.17. Proteção contra anti-spoofing;
- 1.11.18. Deve permitir bloquear sessões TCP que usem variações do 3-way hand-shake, como 4 way e 5 way split hand-shake, prevenindo desta forma possíveis tráfegos maliciosos;
- 1.11.19. Deve permitir bloquear conexões que contenham dados no payload de pacotes TCP-SYN e SYN-ACK durante o three-way handshake;
- 1.11.20. Deve exibir nos logs de tráfego o motivo para o término da sessão no firewall, incluindo sessões finalizadas onde houver de-criptografia de SSL e SSH;
- 1.11.21. Suportar no mínimo as seguintes funcionalidades em IPv6: SLAAC (address auto configuration), NAT64, Identificação de usuários a partir do LDAP/AD, Captive Portal, IPv6 over IPv4 IPSec, Regras de proteção contra DoS (Denial of Service), De-criptografia SSL e SSH, PBF (Policy Based Forwarding), QoS, DHCPv6 Relay, IPSec, VPN SSL, Ativo/Ativo, Ativo/Passivo, SNMP, NTP, SYSLOG, DNS, Neighbor Discovery (ND), Recursive DNS Server (RDNS), DNS Search List (DNSSL) e controle de aplicação;
- 1.11.22. Os dispositivos de proteção devem ter a capacidade de operar de forma simultânea em uma única instância de firewall, mediante o uso de suas interfaces físicas nos seguintes modos: Modo sniffer (monitoramento e análise do tráfego de rede), camada 2 (L2) e camada 3 (L3);
 - 1.11.22.1. Modo Sniffer, para inspeção via porta espelhada do tráfego de dados da rede;
 - 1.11.22.2. Modo Camada – 2 (L2), para inspeção de dados em linha e ter visibilidade e controle do tráfego em nível de aplicação;
 - 1.11.22.3. Modo Camada – 3 (L3), para inspeção de dados em linha e ter visibilidade e controle do tráfego em nível de aplicação operando como default gateway das redes protegidas;
- 1.11.23. Modo misto de trabalho Sniffer, L2 e L3 em diferentes interfaces físicas;
- 1.12. Suporte a configuração de alta disponibilidade Ativo/Passivo e Ativo/Ativo:
 - 1.12.1. Em modo transparente;
 - 1.12.2. Em layer 3;
- 1.13. A configuração em alta disponibilidade deve sincronizar:
 - 1.13.1. Sessões;
 - 1.13.2. Configurações, incluindo, mas não limitado a políticas de Firewall, NAT, QOS e objetos de rede;
 - 1.13.3. Certificados de-criptografados;
 - 1.13.4. Associações de Segurança das VPNs;
 - 1.13.5. Tabelas FIB;
 - 1.13.6. O HA (modo de Alta-Disponibilidade) deve possibilitar monitoração de falha de link.
- 1.14. As funcionalidades de controle de aplicações, VPN IPSec e SSL, QOS, SSL e SSH Decryption e protocolos de roteamento dinâmico devem operar em caráter permanente, podendo ser utilizadas por tempo indeterminado, mesmo que não subsista o direito de receber atualizações ou que não haja contrato de garantia de software com o fabricante.

CONTROLE POR POLÍTICA DE FIREWALL

- 1.1. Deverá suportar controles por zona de segurança.
- 1.2. Deverá suportar controles de políticas por porta e protocolo.
- 1.3. Deverá suportar controle de políticas por aplicações, grupos estáticos de aplicações, grupos dinâmicos de aplicações (baseados em características e comportamento das aplicações) e categorias de aplicações.
- 1.4. Deverá suportar controle de políticas por usuários, grupos de usuários, IPs, redes e zonas de segurança.
- 1.5. Deve suportar a consulta a fontes externas de endereços IP, domínios e URLs podendo ser adicionados nas políticas de firewall para bloqueio ou permissão do tráfego;
 - 1.5.1. Deve permitir autenticação segura através de certificado nas fontes externas de endereços IP, domínios e URLs;
 - 1.5.2. Deve permitir consultar e criar exceção para objetos das listas externas a partir da interface de gerência do próprio firewall;
- 1.6. Controle, inspeção e de-criptografia de SSL por política para tráfego de entrada (Inbound) e Saída (Outbound).
- 1.7. Deve suportar offload de certificado em inspeção de conexões SSL de entrada (Inbound);
- 1.8. Deve de-criptografar tráfego Inbound e Outbound em conexões negociadas com TLS 1.2;
- 1.9. Deve de-criptografar sites e aplicações que utilizam certificados ECC, incluindo Elliptical Curve Digital Signature Algorithm (ECDSA);
- 1.10. Controle de inspeção e de-criptografia de SSH por política;
- 1.11. A de-criptografia de SSH deve possibilitar a identificação e bloqueio de tráfego caso o protocolo esteja sendo usado para tunelar aplicações como técnica evasiva para burlar os controles de segurança;
- 1.12. A plataforma de segurança deve implementar espelhamento de tráfego de-criptografado (SSL e TLS) para soluções externas de análise (Forense de rede, DLP, Análise de Ameaças, entre outras);
 - 1.12.1. É permitido uso de appliance externo, específico para a de-criptografia de (SSL e TLS), com espelhamento de cópia do tráfego de-criptografado tanto para o firewall, quanto para as soluções de análise.
- 1.13. Bloqueios dos seguintes tipos de arquivos: bat, cab, dll, exe, pif, e reg
- 1.14. Traffic shaping QoS baseado em Políticas (Prioridade, Garantia e Máximo)
- 1.15. QoS baseado em políticas para marcação de pacotes (diffserv marking), inclusive por aplicações.
- 1.16. Suporte a objetos e regras IPV6.
- 1.17. Suporte a objetos e regras multicast.
- 1.18. Deve suportar no mínimo três tipos de negação de tráfego nas políticas de firewall: Drop sem notificação do bloqueio ao usuário, Drop com opção de envio de ICMP Unreachable para máquina de origem do tráfego, TCP-Reset para o client, TCP-Reset para o server ou para os dois lados da conexão;
- 1.19. Suportar a atribuição de agendamento as políticas com o objetivo de habilitar e desabilitar políticas em horários pré-definidos automaticamente.

CONTROLE DE APLICAÇÕES

- 1.1. Os dispositivos de proteção de rede deverão possuir a capacidade de reconhecer aplicações, independente de porta e protocolo, com as seguintes funcionalidades:
 - 1.1.1. Deve ser possível a liberação e bloqueio somente de aplicações sem a necessidade de liberação de portas e protocolos.
 - 1.1.2. Deve inspecionar o payload do pacote de dados com o objetivo de detectar através de expressões regulares assinaturas de aplicações conhecidas pelo fabricante independente de porta e protocolo. A

checagem de assinaturas também deve determinar se uma aplicação está utilizando a porta default ou não, incluindo, mas não limitado a RDP na porta 80 ao invés de 389;

1.1.3. Deve aplicar heurística a fim de detectar aplicações através de análise comportamental do tráfego observado, incluindo, mas não limitado a Encrypted Bittorrent e aplicações VOIP que utilizam criptografia proprietária;

1.1.4. Identificar o uso de táticas evasivas, ou seja, deve ter a capacidade de visualizar e controlar as aplicações e os ataques que utilizam táticas evasivas via comunicações criptografadas, tais como Skype e ataques mediante a porta 443.

1.1.5. Para tráfego criptografado SSL, deve de-criptografar pacotes a fim de possibilitar a leitura de payload para checagem de assinaturas de aplicações conhecidas pelo fabricante;

1.1.6. Deve realizar decodificação de protocolos com o objetivo de detectar aplicações encapsuladas dentro do protocolo e validar se o tráfego corresponde com a especificação do protocolo, incluindo, mas não limitado a Yahoo Instant Messenger usando HTTP. A decodificação de protocolo também deve identificar funcionalidades específicas dentro de uma aplicação, incluindo, mas não limitado a compartilhamento de arquivo dentro do Webex. Além de detectar arquivos e outros conteúdos que devem ser inspecionados de acordo as regras de segurança implementadas;

1.1.7. Identificar o uso de táticas evasivas via comunicações criptografadas;

1.1.8. Atualizar a base de assinaturas de aplicações automaticamente;

1.1.9. Reconhecer aplicações em IPv6;

1.1.10. Permitir limitar a banda (download/upload) usada por aplicações (traffic shaping), baseado no IP de origem;

1.1.11. Os dispositivos de proteção de rede devem possuir a capacidade de identificar o usuário de rede com integração ao Microsoft Active Directory, sem a necessidade de instalação de agente no Domain Controller, nem nas estações dos usuários;

1.1.12. Deve ser possível adicionar controle de aplicações em todas as regras de segurança do dispositivo, ou seja, não se limitando somente a possibilidade de habilitar controle de aplicações em algumas regras;

1.1.13. Deve suportar múltiplos métodos de identificação e classificação das aplicações, por pelo menos checagem de assinaturas, decodificação de protocolos e análise heurística;

1.1.14. Para manter a segurança da rede eficiente, deve suportar o controle sobre aplicações desconhecidas e não somente sobre aplicações conhecidas;

1.1.15. Permitir nativamente a criação de assinaturas personalizadas para reconhecimento de aplicações proprietárias na própria interface gráfica da solução, sem a necessidade de ação do fabricante, mantendo a confidencialidade das aplicações do órgão;

1.1.16. A criação de assinaturas personalizadas deve permitir o uso de expressões regulares, contexto (sessões ou transações), usando posição no payload dos pacotes TCP e UDP e usando decoders de pelo menos os seguintes protocolos:

1.1.16.1. HTTP, FTP, SMB, SMTP, Telnet, SSH, MS-SQL, IMAP, IMAP, MS-RPC, RTSP e File body.

1.1.17. O fabricante deve permitir a solicitação de inclusão de aplicações na base de assinaturas de aplicações;

1.1.18. Deve alertar o usuário quando uma aplicação for bloqueada;

1.1.19. Deve possibilitar que o controle de portas seja aplicado para todas as aplicações;

1.1.20. Deve permitir criar filtro na tabela de regras de segurança para exibir somente:

1.1.20.1. Regras que permitem passagem de tráfego baseado na porta e não por aplicação, exibindo quais aplicações estão trafegando nas mesmas, o volume em bytes trafegado por cada aplicação por, pelo menos, os últimos 30 dias e o primeiro e último registro de log de cada aplicação trafegada por esta determinada regra;

1.1.20.2. Aplicações permitidas em regras de forma desnecessária, pois não há tráfego da mesma na determinada regra;

1.1.20.3. Regras de segurança onde não houve passagem de tráfego nos últimos 90 dias;

1.1.21. Deve possibilitar a diferenciação de tráfegos Peer2Peer (Bittorrent, emule, neonet, etc.) possuindo granularidade de controle/políticas para os mesmos;

1.1.22. Deve possibilitar a diferenciação de aplicações Proxies (ghostsurf, freegate, etc.) possuindo granularidade de controle/políticas para os mesmos;

1.1.23. Deve ser possível a criação de grupos estáticos de aplicações e grupos dinâmicos de aplicações baseados em características das aplicações como:

1.1.23.1. Tecnologia utilizada na aplicação (Client-Server, Browser Based, Network Protocol, etc).

1.1.23.2. Nível de risco da aplicação.

1.1.23.3. Categoria e subcategoria de aplicações.

- 1.1.23.4. Aplicações que usem técnicas evasivas, utilizadas por malwares, como transferência de arquivos e/ou uso excessivo de banda, etc.
- 1.2. comum reativo não ser capaz de detectar os mesmos com a mesma velocidade que suas variações são criadas, a solução ofertada deverá possuir funcionalidades para análise de Malwares não conhecidos incluídas na própria ferramenta ou entregue com composição com outro fabricante;
- 1.3. O dispositivo de proteção deve ser capaz de enviar arquivos trafegados de forma automática para análise "In Cloud" ou local, onde o arquivo será executado e simulado em ambiente controlado;
- 1.4. Selecionar através de políticas granulares quais tipos de arquivos sofrerão esta análise incluindo, mas não limitado a: endereço IP de origem/destino, usuário/grupo do AD/LDAP, aplicação, porta, URL/categoria de URL de destino, tipo de arquivo e todas estas opções simultaneamente;
- 1.5. Deve possuir a capacidade de diferenciar arquivos analisados em pelo menos três categorias: malicioso, não malicioso e arquivos não maliciosos, mas com características indesejáveis como softwares que deixam o sistema operacional lento, que alteram parâmetros do sistema, etc.;
- 1.6. Suportar a análise de arquivos maliciosos em ambiente controlado com, no mínimo, sistema operacional Windows XP e Windows 7;
- 1.7. Deve suportar a monitoração de arquivos trafegados na internet (HTTPs, FTP, HTTP, SMTP) como também arquivos trafegados internamente entre servidores de arquivos usando SMB em todos os modos de implementação: sniffer, transparente e L3;
- 1.8. A solução deve possuir a capacidade de analisar em sand-box links (http e https) presentes no corpo de e-mails trafegados em SMTP e POP3. Deve ser gerado um relatório caso a abertura do link pela sandbox o identifique como site hospedeiro de exploits;
- 1.9. A análise de links em sandbox deve ser capaz de classificar sites falsos na categoria de phishing e atualizar a base de filtro de URL da solução;
- 1.10. Para ameaças trafegadas em protocolo SMTP e POP3, a solução deve ter a capacidade de mostrar nos relatórios o remetente, destinatário e assunto dos e-mails permitindo identificação ágil do usuário vítima do ataque;
- 1.11. O sistema de análise "In Cloud" ou local deve prover informações sobre as ações do Malware na máquina infectada, informações sobre quais aplicações são utilizadas para causar/propagar a infecção, detectar aplicações não confiáveis utilizadas pelo Malware, gerar assinaturas de Antivírus e Anti-spyware automaticamente, definir URLs não confiáveis utilizadas pelo novo Malware e prover informações sobre o usuário infectado (seu endereço ip e seu login de rede);
- 1.12. O sistema automático de análise "In Cloud" ou local deve emitir relatório com identificação de quais soluções de antivírus existentes no mercado possuem assinaturas para bloquear o malware;
- 1.13. Deve permitir exportar o resultado das análises de malwares de dia Zero em PDF e CSV a partir da própria interface de gerência;
- 1.14. Deve permitir o download dos malwares identificados a partir da própria interface de gerência;
- 1.15. Deve permitir visualizar os resultados das análises de malwares de dia zero nos diferentes sistemas operacionais suportados;
- 1.16. Deve permitir informar ao fabricante quanto a suspeita de ocorrências de falso-positivo e falso-negativo na análise de malwares de dia Zero a partir da própria interface de gerência.
- 1.17. Caso sejam necessárias licenças de sistemas operacional e softwares para execução de arquivos no ambiente controlado (sandbox), as mesmas devem ser fornecidas em sua totalidade, sem custos adicionais para a contratante;
- 1.18. Suportar a análise de arquivos executáveis, DLLs, ZIP e criptografados em SSL no ambiente controlado;

- 1.19. Suportar a análise de arquivos do pacote office (.doc, .docx, .xls, .xlsx, .ppt, .pptx), arquivos java (.jar e class), Android APKs MacOS (mach-O, DMG e PKG), Linux (ELF), RAR e 7-ZIP no ambiente de sandbox;
- 1.20. Permitir o envio de arquivos e links para análise no ambiente controlado de forma automática via API.
- 1.21. Deve permitir o envio para análise em sandbox de malwares bloqueados pelo antivírus da solução;

FILTRO DE URL

- 1.1. A plataforma de segurança deve possuir as seguintes funcionalidades de filtro de URL:
 - 1.1.1. Permite especificar política por tempo, ou seja, a definição de regras para um determinado horário ou período (dia, mês, ano, dia da semana e hora);
 - 1.1.2. Deve ser possível a criação de políticas por Usuários, Grupos de Usuários, Ips, Redes e Zonas de segurança.
 - 1.1.3. Deverá incluir a capacidade de criação de políticas baseadas na visibilidade e controle de quem está utilizando quais URLs através da integração com serviços de diretório, autenticação via ldap, Active Directory, E-directory e base de dados local.
 - 1.1.4. Permite popular todos os logs de URL com as informações dos usuários conforme descrito na integração com serviços de diretório;
 - 1.1.5. Suporta a capacidade de criação de políticas baseadas no controle por URL e Categoria de URL;
 - 1.1.6. Deve permitir bloquear o acesso a sites de busca (Google, Bing e Yahoo), caso a opção Safe Search esteja desabilitada. Deve ainda exibir pagina de bloqueio fornecendo instruções ao usuário de como habilitar a função;
 - 1.1.7. Deve suportar base ou cache de URLs local no appliance, evitando delay de comunicação/validação das URLs;
 - 1.1.8. Deve permitir classificar o nível de risco de URLs em, pelo menos, três níveis: baixo, médio e alto;
 - 1.1.9. A solução deve ter a capacidade de classificar sites em mais de uma categoria, de acordo com a necessidade;
 - 1.1.10. A categorização de URL deve analisar toda a URL e não somente até o nível de diretório;
 - 1.1.11. Deve suportar a criação categorias de URLs customizadas;
 - 1.1.12. Deve suportar a exclusão de URLs do bloqueio, por categoria;
 - 1.1.13. Deve permitir a customização de página de bloqueio;
 - 1.1.14. Deve proteger contra o roubo de credenciais, usuários e senhas identificadas através da integração com Active Directory submetidos em sites não corporativos. Deve ainda permitir criação de regra onde usuários do Active Directory só possam enviar informações de login para sites autorizados na solução;
 - 1.1.15. Deve permitir bloquear o acesso do usuário caso o mesmo tente fazer o envio de suas credenciais em sites classificados como phishing pelo filtro de URL da solução;
 - 1.1.16. Deve permitir o bloqueio e continuação (possibilitando que o usuário acesse um site potencialmente bloqueado informando o mesmo na tela de bloqueio e possibilitando a utilização de um botão "Continuar" para permitir ao usuário continuar acessando o site);
 - 1.1.17. Deve suportar a inclusão nos logs do produto de informações das atividades dos usuários;
 - 1.1.18. Deve salvar nos logs as informações dos seguintes campos do cabeçalho HTTP nos acessos a URLs: UserAgent, Referer, e X-Forwarded For;

IDENTIFICAÇÃO DE USUÁRIOS

- 1.2. Deve incluir a capacidade de criação de políticas baseadas na visibilidade e controle de quem está utilizando quais aplicações através da integração com serviços de diretório, autenticação via ldap, Active Directory, E-directory e base de dados local;
- 1.3. Deve permitir integração com Microsoft Active Directory para identificação de usuários e grupos permitindo granularidade de controle/políticas baseadas em usuários e grupos de usuários;
- 1.4. Deve permitir integração com Radius para identificação de usuários e grupos permitindo granularidade de controle/políticas baseadas em usuários e grupos de usuários;

- 1.5. Deve implementar a criação de políticas de segurança baseada em atributos específicos do Radius, incluindo mas não limitado a: baseado no sistema operacional do usuário remoto exigir autenticação padrão Windows e on-time password (OTP) para usuários Android;
- 1.6. Deve possuir integração com Ldap para identificação de usuários e grupos permitindo granularidade de controle/políticas baseadas em Usuários e Grupos de usuários;
 - 1.6.1.1. Deve suportar o recebimento eventos de autenticação de controladoras wireless, dispositivos 802.1x e soluções NAC via syslog, para a identificação de endereços IP e usuários;
- 1.7. Deve permitir o controle, sem instalação de cliente de software, em equipamentos que solicitem saída a internet para que antes de iniciar a navegação, expanda-se um portal de autenticação residente no firewall (Captive Portal);
- 1.8. Deve suportar a autenticação via Kerberos;
- 1.9. Deve suportar autenticação via Kerberos para administradores da plataforma de segurança, captive Portal e usuário de VPN SSL;
- 1.10. Deve identificar usuários através de leitura do campo x-forwarded-for, populando nos logs do firewall o endereço IP, bem como o usuário de rede responsável pelo acesso;
- 1.11. Deve permitir a criação de políticas de segurança baseadas em usuários de rede com reconhecimento dos mesmos através de leitura do campo x-forwarded-for;
- 1.12. O firewall deve operar/suportar Security Assertion Markup Language (SAML) 2.0, com single sign-on e single logout para as funcionalidades de Captive Portal e VPN SSL (client to server), permitindo login único e interativo para fornecer acesso automático a serviços autenticados, internos e externos à organização;
- 1.13. Deve implementar a criação de grupos customizados de usuários no firewall, baseado em atributos do LDAP/AD;
- 1.14. Deve possuir suporte a identificação de múltiplos usuários conectados em um mesmo endereço IP em servidores acessados remotamente, mesmo que não sejam servidores Windows.

FILTRO DE URL

- 1.15. A plataforma de segurança deve possuir as seguintes funcionalidades de filtro de URL:
 - 1.15.1. Permite especificar política por tempo, ou seja, a definição de regras para um determinado horário ou período (dia, mês, ano, dia da semana e hora);
 - 1.15.2. Deve ser possível a criação de políticas por Usuários, Grupos de Usuários, Ips, Redes e Zonas de segurança.
 - 1.15.3. Deverá incluir a capacidade de criação de políticas baseadas na visibilidade e controle de quem está utilizando quais URLs através da integração com serviços de diretório, autenticação via Ldap, Active Directory, E-directory e base de dados local.
 - 1.15.4. Permite popular todos os logs de URL com as informações dos usuários conforme descrito na integração com serviços de diretório;
 - 1.15.5. Suporta a capacidade de criação de políticas baseadas no controle por URL e Categoria de URL;
 - 1.15.6. Deve permitir bloquear o acesso a sites de busca (Google, Bing e Yahoo), caso a opção Safe Search esteja desabilitada. Deve ainda exibir pagina de bloqueio fornecendo instruções ao usuário de como habilitar a função;
 - 1.15.7. Deve suportar base ou cache de URLs local no appliance, evitando delay de comunicação/validação das URLs;
 - 1.15.8. Deve permitir classificar o nível de risco de URLs em, pelo menos, três níveis: baixo, médio e alto;
 - 1.15.9. A solução deve ter a capacidade de classificar sites em mais de uma categoria, de acordo com a necessidade;
 - 1.15.10. A categorização de URL deve analisar toda a URL e não somente até o nível de diretório;
 - 1.15.11. Deve suportar a criação categorias de URLs customizadas;
 - 1.15.12. Deve suportar a exclusão de URLs do bloqueio, por categoria;
 - 1.15.13. Deve permitir a customização de página de bloqueio;

- 1.15.14. Deve proteger contra o roubo de credenciais, usuários e senhas identificadas através da integração com Active Directory submetidos em sites não corporativos. Deve ainda permitir criação de regra onde usuários do Active Directory só possam enviar informações de login para sites autorizados na solução;
- 1.15.15. Deve permitir bloquear o acesso do usuário caso o mesmo tente fazer o envio de suas credenciais em sites classificados como phishing pelo filtro de URL da solução;
- 1.15.16. Deve permitir o bloqueio e continuação (possibilitando que o usuário acesse um site potencialmente bloqueado informando o mesmo na tela de bloqueio e possibilitando a utilização de um botão "Continuar" para permitir ao usuário continuar acessando o site);
- 1.15.17. Deve suportar a inclusão nos logs do produto de informações das atividades dos usuários;
- 1.15.18. Deve salvar nos logs as informações dos seguintes campos do cabeçalho HTTP nos acessos a URLs: UserAgent, Referer, e X-Forwarded For;

IDENTIFICAÇÃO DE USUÁRIOS

- 1.16. Deve incluir a capacidade de criação de políticas baseadas na visibilidade e controle de quem está utilizando quais aplicações através da integração com serviços de diretório, autenticação via ldap, Active Directory, E-directory e base de dados local;
- 1.17. Deve permitir integração com Microsoft Active Directory para identificação de usuários e grupos permitindo granularidade de controle/políticas baseadas em usuários e grupos de usuários;
- 1.18. Deve permitir integração com Radius para identificação de usuários e grupos permitindo granularidade de controle/políticas baseadas em usuários e grupos de usuários;
- 1.19. Deve implementar a criação de políticas de segurança baseada em atributos específicos do Radius, incluindo mas não limitado a: baseado no sistema operacional do usuário remoto exigir autenticação padrão Windows e on-time password (OTP) para usuários Android;
- 1.20. Deve possuir integração com ldap para identificação de usuários e grupos permitindo granularidade de controle/políticas baseadas em Usuários e Grupos de usuários;
 - 1.20.1.1. Deve suportar o recebimento eventos de autenticação de controladoras wireless, dispositivos 802.1x e soluções NAC via syslog, para a identificação de endereços IP e usuários;
- 1.21. Deve permitir o controle, sem instalação de cliente de software, em equipamentos que solicitem saída a internet para que antes de iniciar a navegação, expanda-se um portal de autenticação residente no firewall (Captive Portal);
- 1.22. Deve suportar a autenticação via Kerberos;
- 1.23. Deve suportar autenticação via Kerberos para administradores da plataforma de segurança, captive Portal e usuário de VPN SSL;
- 1.24. Deve identificar usuários através de leitura do campo x-forwarded-for, populando nos logs do firewall o endereço IP, bem como o usuário de rede responsável pelo acesso;
- 1.25. Deve permitir a criação de políticas de segurança baseadas em usuários de rede com reconhecimento dos mesmos através de leitura do campo x-forwarded-for;
- 1.26. O firewall deve operar/suportar Security Assertion Markup Language (SAML) 2.0, com single sign-on e single logout para as funcionalidades de Captive Portal e VPN SSL (client to server), permitindo login único e interativo para fornecer acesso automático a serviços autenticados, internos e externos à organização;
- 1.27. Deve implementar a criação de grupos customizados de usuários no firewall, baseado em atributos do LDAP/AD;
- 1.28. Deve possuir suporte a identificação de múltiplos usuários conectados em um mesmo endereço IP em servidores acessados remotamente, mesmo que não sejam servidores Windows.

QOS

- 1.29. Permitir controlar aplicações e tráfego cujo consumo possa ser excessivo e ter um alto consumo de largura de banda.
- 1.30. Suportar a criação de políticas de QoS por:
 - 1.30.1. Endereço de origem
 - 1.30.2. Endereço de destino
 - 1.30.3. Por usuário e grupo do LDAP/AD.
 - 1.30.4. Por aplicações;
 - 1.30.5. Por porta;
- 1.31. O QoS deve possibilitar a definição de classes por:
 - 1.31.1. Banda Garantida
 - 1.31.2. Banda Máxima
 - 1.31.3. Fila de Prioridade.
- 1.32. Suportar priorização RealTime de protocolos de voz (VOIP) como H.323, SIP, SCCP, MGCP e aplicações como Skype.
- 1.33. Suportar marcação de pacotes Diffserv, inclusive por aplicação;
- 1.34. Deve implementar QOS (traffic-shapping), para pacotes marcados por outros ativos na rede (DSCP). A priorização e limitação do tráfego deve ser efetuada nos dois sentidos da conexão (inbound e outbound);
- 1.35. Disponibilizar estatísticas RealTime para classes de QoS.
- 1.36. Deve suportar QOS (traffic-shapping), em interface agregadas;
- 1.37. Deverá permitir o monitoramento do uso que as aplicações fazem por bytes e sessões.

FILTRO DE DADOS

- 1.38. Permite a criação de filtros para arquivos e dados pré-definidos;
- 1.39. Os arquivos devem ser identificados por extensão e assinaturas;
- 1.40. Permite identificar e opcionalmente prevenir a transferência de vários tipos de arquivos (MS Office, PDF, etc) identificados sobre aplicações (P2P, InstantMessaging, SMB, etc);
- 1.41. Suportar identificação de arquivos compactados e a aplicação de políticas sobre o conteúdo desses tipos de arquivos;
- 1.42. Permitir identificar e opcionalmente prevenir a transferência de informações sensíveis, incluindo, mas não limitado a número de cartão de crédito, possibilitando a criação de novos tipos de dados via expressão regular;
- 1.43. Permitir listar o número de aplicações suportadas para controle de dados;
- 1.44. Permitir listar o número de tipos de arquivos suportados para controle de dados;

VPN

- 1.45. Deve suportar VPN Site-to-Site e Client-To-Site;
- 1.46. Deve suportar IPSec VPN;
- 1.47. Deve suportar SSL VPN;
- 1.48. A VPN IPSEc deve suportar:
 - 1.48.1. 3DES;

- 1.48.2. Autenticação MD5 e SHA-1;
- 1.48.3. Diffie-Hellman Group 1, Group 2, Group 5 e Group 14;
- 1.48.4. Algoritmo Internet Key Exchange (IKEv1 e v2);
- 1.48.5. AES 128, 192 e 256 (Advanced Encryption Standard)
- 1.48.6. Autenticação via certificado IKE PKI.

1.49. Deve possuir interoperabilidade com os seguintes fabricantes:

- 1.49.1. Cisco;
- 1.49.2. Checkpoint;
- 1.49.3. Juniper;
- 1.49.4. Palo Alto Networks;
- 1.49.5. Fortinet;
- 1.49.6. Sonic Wall;

1.50. Deve permitir habilitar, desabilitar, reiniciar e atualizar IKE gateways e túneis de VPN IPSEC a partir da interface gráfica da solução, facilitando o processo de troubleshooting;

1.51. A VPN SSL deve suportar:

- 1.51.1. O usuário realizar a conexão por meio de cliente instalado no sistema operacional do equipamento ou por meio de interface WEB;
- 1.51.2. A funcionalidades de VPN SSL devem ser atendidas com ou sem o uso de agente;
- 1.51.3. Atribuição de endereço IP nos clientes remotos de VPN SSL;
- 1.51.4. Deve permitir a atribuição de IPs fixos nos usuários remotos de VPN SSL;
- 1.51.5. Deve permitir a criação de rotas de acesso e faixas de endereços IP atribuídas a clientes remotos de VPN de forma customizada por usuário AD/LDAP e grupo de usuário AD/LDAP;
- 1.51.6. Deve permitir que todo o tráfego dos usuários remotos de VPN seja escoado para dentro do túnel de VPN, impedindo comunicação direta com dispositivos locais como proxies;
- 1.51.7. Atribuição de DNS nos clientes remotos de VPN;
- 1.51.8. Deve permitir que seja definido métodos de autenticação distintos por sistema operacional do dispositivo remoto de VPN (Android, IOS, Mac, Windows e Chrome OS);
- 1.51.9. A solução de VPN deve verificar se o client que está realizando a conexão é o mesmo para o qual o certificado foi emitido inicialmente. O acesso deve ser bloqueado caso o dispositivo não seja o correto;
- 1.51.10. Deve possuir lista de bloqueio para dispositivos que forem reportados com roubado ou perdido pelo usuário;
- 1.51.11. Deve haver a opção de ocultar o agente de VPN instalado no cliente remoto, tornando o mesmo invisível para o usuário;
- 1.51.12. Deve exibir mensagens de notificação customizada toda vez que um usuário remoto se conectar a VPN. Deve permitir que o usuário desabilite a exibição da mensagem nas conexões seguintes;
- 1.51.13. Deve avisar ao usuário remoto de VPN quanto a proximidade da expiração de senha LDAP. Deve permitir também a customização da mensagem com informações relevantes para o usuário;
- 1.51.14. Deve permitir criar políticas de controle de aplicações, IPS, Antivírus, Antispyware e filtro de URL para tráfego dos clientes remotos conectados na VPN SSL;
- 1.51.15. A VPN SSL deve suportar proxy arp e uso de interfaces PPPOE;
- 1.51.16. Suportar autenticação via Radius, AD/LDAP, OTP (One Time Password), certificado e base de usuários local;
- 1.51.17. Deve permitir a distribuição de certificado para o usuário de remoto através do portal de VPN de forma automatizada;
- 1.51.18. Deve possuir lista de bloqueio para dispositivos em casos quando, por exemplo, o usuário reportar que o dispositivo foi perdido ou roubado;
- 1.51.19. Permite estabelecer um túnel VPN client-to-site do cliente a plataforma de segurança, fornecendo uma solução de single-sign-on aos usuários, integrando-se com as ferramentas de Windows-logon;
- 1.51.20. Suporta leitura e verificação de CRL (certificate revocation list);
- 1.51.21. Permite a aplicação de políticas de segurança e visibilidade para as aplicações que circulam dentro dos túneis SSL;

- 1.51.22. O agente de VPN a ser instalado nos equipamentos desktop e laptops, deve ser capaz de ser distribuído de maneira automática via Microsoft SMS, Active Directory e ser descarregado diretamente desde o seu próprio portal, o qual residirá no centralizador de VPN;
- 1.51.23. O agente deverá comunicar-se com o portal para determinar as políticas de segurança do usuário;
- 1.51.24. Deve permitir que a conexão com a VPN SSL seja estabelecida das seguintes formas:
- 1.51.24.1. Antes do usuário autenticar na estação;
- 1.51.24.2. Após autenticação do usuário na estação;
- 1.51.24.3. Sob demanda do usuário;
- 1.51.25. Deve Manter uma conexão segura com o portal durante a sessão.
- 1.51.26. O agente de VPN SSL client-to-site deve ser compatível com pelo menos: Windows XP, Vista Windows 7, Windows 8, Mac OS e Chrome OS;
- 1.51.27. O portal de VPN deve enviar ao cliente remoto, a lista de gateways de VPN ativos para estabelecimento da conexão, os quais devem poder ser administrados centralmente;
- 1.51.28. Deve haver a opção de o cliente remoto escolher manualmente o gateway de VPN e de forma automática através da melhor rota entre os gateways disponíveis com base no tempo de resposta mais rápido;
- 1.51.29. Deve possuir a capacidade de identificar se a origem da conexão de VPN é externa ou interna;

GRUPO	ITEM	DESCRIÇÃO	QTD
1	1	<p>FIREWALL TIPO 1 COM SUPORTE, GARANTIA E LICENÇAS DE PROTEÇÃO COM VIGÊNCIA DE 36 MESES.</p> <p>Características técnicas mínimas:</p> <ol style="list-style-type: none"> Throughput de 16 Gbps com a funcionalidade de controle de aplicação habilitada para todas as assinaturas que o fabricante possuir; Throughput de 8 Gbps com as seguintes funcionalidades habilitadas simultaneamente para todas as assinaturas que a plataforma de segurança possuir devidamente ativadas e atuantes: controle de aplicação IPS, Antivírus e Antispyware. Caso o fabricante divulgue múltiplos números de desempenho para qualquer uma destas funcionalidades, somente o de menor valor será aceito; Os throughputs devem ser comprovados por documento de domínio público do fabricante. A ausência de tais documentos comprobatórios reservará ao órgão o direito de aferir a performance dos equipamentos em bancada, assim como atendimento de todas as funcionalidades especificadas neste edital. Caso seja comprovado o não atendimento das especificações mínimas nos testes de bancada, serão considerados inabilitados e sujeitos às sanções previstas em lei; Os documentos públicos devem comprovar os throughputs aferidos com tráfego HTTP ou blend de protocolos definidos pelo fabricante como tráfego real (real-word traffic blend); Não será aceito aceleração de pacotes na placa de rede limitando a análise somente até camada 4. Suporte a, no mínimo, 3.500.000 de conexões simultâneas; Suporte a, no mínimo, 100.000 novas conexões HTTP por segundo; Possuir fonte 120/240 AC ou DC, redundante e hot-swappable; Possuir cooler hot-swappable; Possuir disco Solid State Drive (SSD) redundante de, no mínimo, 240 GB. Possuir discos de, no mínimo, 2 TB em RAID 1 para armazenamento de logs interno ou externo a solução de firewall; No mínimo, 04 (quatro) interfaces de rede 1 Gbps em portas cobre; 	2

	<p>10. No mínimo, 08 (oito) interfaces de rede 1 Gbps SFP;</p> <p>11. No mínimo, 08 (oito) interfaces de rede 10 Gbps SFP+;</p> <p>12. No mínimo, 04 (quatro) interfaces de rede 40 Gbps QSFP+;</p> <p>13. 2 (duas) Gbps interfaces dedicadas para alta disponibilidade sendo pelo menos uma do tipo 40 Gbps QSFP+;</p> <p>14. 1 (uma) interface de rede 1 Gbps dedicada para gerenciamento;</p> <p>15. 1 (uma) interface do tipo console ou similar;</p> <p>16. Suporte a, no mínimo, 60 (sessenta) zonas de segurança;</p> <p>17. Estar licenciada para ou suportar sem o uso de licença, 10.000 (dez mil) clientes de VPN SSL simultâneos;</p> <p>18. Estar licenciada para ou suportar sem o uso de licença, 3.000 (três mil) túneis de VPN IPSEC simultâneos;</p> <p>19. Deve suportar, no mínimo, 10 sistemas virtuais lógicos (Contextos) no firewall Físico;</p> <p>20. Os contextos virtuais devem suportar as funcionalidades nativas do gateway de proteção incluindo: Firewall, IPS, Antivírus, Anti-Spyware, Filtro de URL, Filtro de Dados VPN, Controle de Aplicações, QOS, NAT e Identificação de usuários;</p> <p>21. Na data da proposta, nenhum dos modelos ofertados poderão estar listados no site do fabricante em listas de end-of-life e end-of-sale.</p> <p>22. Conforme disposto no item I do artigo 15 da lei 8.666, de 21 de junho de 1993 (I - Atender ao princípio de padronização, que imponha compatibilidade técnica e de desempenho, observadas, quando for o caso, as condições de manutenção, assistência técnica e garantia oferecidas), estes equipamentos, por questões de compatibilidade, gerência, suporte e garantia, devem ser do mesmo fabricante dos equipamentos deste grupo/lote;</p>	
2	<p>FIREWALL TIPO 2 COM SUPORTE, GARANTIA E LICENÇAS DE PROTEÇÃO COM VIGÊNCIA DE 36 MESES.</p> <p>Características técnicas mínimas:</p> <p>1. Throughput de 8 Gbps com a funcionalidade de controle de aplicação habilitada para todas as assinaturas que o fabricante possuir;</p> <p>2. Throughput de 4 Gbps com as seguintes funcionalidades habilitadas simultaneamente para todas as assinaturas que a plataforma de segurança possuir devidamente ativadas e atuantes: controle de aplicação IPS, Antivírus e Antispyware. Caso o fabricante divulgue múltiplos números de desempenho para qualquer uma destas funcionalidades, somente o de menor valor será aceito;</p> <p>2.1. Os throughputs devem ser comprovados por documento de domínio público do fabricante. A ausência de tais documentos comprobatórios reservará ao órgão o direito de aferir a performance dos equipamentos em bancada, assim como atendimento de todas as funcionalidades especificadas neste edital. Caso seja comprovado o não atendimento das especificações mínimas nos testes de bancada, serão considerados inabilitados e sujeitos as sanções previstas em lei;</p> <p>2.2. Os documentos públicos devem comprovar os throughputs aferidos com tráfego HTTP ou blend de protocolos definidos pelo fabricante como tráfego real (real-word traffic blend ou similar);</p> <p>2.3. Não será aceito aceleração de pacotes na placa de rede limitando a análise somente até camada 4.</p> <p>3. Suporte a, no mínimo, 2.000.000 conexões simultâneas;</p>	2

		<p>4. Suporte a, no mínimo, 50.000 novas conexões por segundo;</p> <p>5. Possuir fonte 120/240 AC ou DC, redundante e hot-swappable;</p> <p>6. Possuir cooler hot-swappable;</p> <p>7. Possuir disco Solid State Drive (SSD) de, no mínimo, 240 GB;</p> <p>8. 12 (doze) interfaces de rede 1 Gbps 10/100/1000 base-TX ou SFP;</p> <p>9. 8 (oito) interfaces de rede 10 Gbps SFP+;</p> <p>10. 4 (quatro) interfaces de rede 40 Gbps QSFP+;</p> <p>11. 2 (duas) Gbps interfaces dedicadas para alta disponibilidade sem pelo menos uma do tipo 10Gbps SFP+;</p> <p>12. 1 (uma) interface de rede 1 Gbps dedicada para gerenciamento;</p> <p>13. 1 (uma) interface do tipo console ou similar;</p> <p>14. Suporte a, no mínimo, 30 (trinta) zonas de segurança;</p> <p>15. Estar licenciada para ou suportar sem o uso de licença, 2.000 (dois mil) clientes de VPN SSL simultâneos;</p> <p>16. Estar licenciada para ou suportar sem o uso de licença, 2.000 túneis de VPN IPSEC simultâneos;</p> <p>17. Deve suportar, no mínimo, 1 sistema virtual lógico (Contexto) no firewall Físico;</p> <p>18. Deve permitir expansão com aquisição futura de licenças a até 6 sistemas virtuais lógicos (Contextos) no firewall Físico;</p> <p>19. Os contextos virtuais devem suportar as funcionalidades nativas do gateway de proteção incluindo: Firewall, IPS, Antivírus, Anti-Spyware, Filtro de URL, Filtro de Dados, VPN, Controle de Aplicações, QOS, NAT e Identificação de usuários;</p> <p>20. Na data da proposta, nenhum dos modelos ofertados poderão estar listados no site do fabricante em listas de end-of-life e end-of-sale.</p> <p>21. Conforme disposto no item I do artigo 15 da lei 8.666, de 21 de junho de 1993 (I - Atender ao princípio de padronização, que imponha compatibilidade técnica e de desempenho, observadas, quando for o caso, as condições de manutenção, assistência técnica e garantia oferecidas), estes equipamentos, por questões de compatibilidade, gerência, suporte e garantia, devem ser do mesmo fabricante dos equipamentos deste grupo/lote;</p>	
	3	<p>SERVIÇOS DE INSTALAÇÃO DE FIREWALL</p> <p>A Licitante Vencedora deverá prestar serviços de instalação e configuração da solução, que compreendem, entre outros, os seguintes procedimentos:</p> <p>1) Reunião de alinhamento para criação do escopo do projeto previamente a instalação;</p> <p>2) Instalação física de todos os equipamentos (hardware) e licenças (softwares) adquiridos no local determinado pela equipe responsável pelo projeto por parte da contratante (DTI). Quando aplicável, considerar instalação em modo Alta Disponibilidade (ativo/passivo);</p> <p>3) Análise da topologia e arquitetura da rede, considerando todos equipamentos já existentes e instalados;</p> <p>4) Análise do acesso à Internet, sites remotos, serviços de rede oferecidos aos funcionários e aos usuários externos;</p> <p>5) Migração das regras de firewall existentes e aplicáveis à solução ofertada, considerando a adequação às políticas de aplicações em camada 7;</p> <p>6) Análise do posicionamento de qualquer outro equipamento ou sistema relevante na segurança de qualquer perímetro protegido pela solução;</p> <p>7) Configuração do sistema de firewall, VPN, IPS, Filtro URL, Anti-vírus e Anti-malware de acordo com as exigências levantadas;</p> <p>8) Toda configuração de sistema (políticas gerais, objetos, itens de administração) deverá ser realizada de acordo com as melhores práticas recomendadas pelo fabricante da solução ofertada, além de compreender as</p>	4

		<p>principais disciplinas de funcionamento seguro dos frameworks CIS e NIST Framework. O fabricante da solução ofertada deverá disponibilizar ferramenta gratuita (ou incluir nos custos de serviço) para acompanhamento da evolução da parametrização de proteção dos firewalls a fim de garantir a melhor eficiência da solução durante o período de vigência das licenças;</p> <p>9) Configuração do sistema de gerenciamento centralizado considerando adição dos novos appliances;</p> <p>10) Repasse de informação das configurações realizadas no formato hands-on de 4 horas para o DTI após validação da migração;</p> <p>11) Deve haver geração de relatório com as configurações efetuadas e as decisões tomadas em formato legível e tecnicamente fundamentado;</p> <p>12) Os serviços de instalação e configuração deverá ser realizado por técnico certificado oficialmente pelo fabricante da solução ofertada ou pelo próprio fabricante;</p>	
	4	<p>TREINAMENTO OFICIAL DE FIREWALL DE PRÓXIMA GERAÇÃO</p> <p>4.1. A Licitante Vencedora deverá disponibilizar vouchers para treinamento oficial do fabricante;</p> <p>4.2. O treinamento deve ser ministrado abrangendo teoria e prática de implantação, configuração, administração e solução de problemas no ambiente deste órgão, bem como assuntos teóricos relacionados;</p> <p>4.3. Deve conter no mínimo a seguinte ementa:</p> <ul style="list-style-type: none"> • Arquitetura e Plataforma; • Configuração Inicial; • Configuração de Interface; • Políticas de Segurança e NAT; • Identificação de Aplicações; • Identificação de Conteúdo Básico; • Filtro URL; • De-criptografia; • Sandboxing de ameaças avançadas; • Identificação de Usuário; • VPN; • Monitoramento e Relatórios; • Alta Disponibilidade (redundância); • Demais assuntos pertinentes a solução; <p>4.4. Deve ser emitido um único certificado de conclusão cobrindo todo o curso, sendo um para cada participante;</p> <p>4.5. O treinamento deverá ser ministrado pelo próprio fabricante ou por um parceiro nacional, capacitado, certificado e autorizado pelo fabricante a ministrar treinamentos oficiais.</p> <p>4.6. O treinamento deve estar disponível preferencialmente na modalidade presencial na sede da Contratante;</p> <p>4.7. O fabricante ou autorizada fornecerá os materiais didáticos para ministrar o curso.</p>	4

7.1. Requisitos de Negócio

- Aquisição de solução de firewall de próxima geração, provendo visibilidade detalhada e controle do tráfego e proteção da rede;
- Adequação às legislações vigentes, tais como LGPD – Lei Geral de Proteção de Dados (Lei nº 13.709/2018) e Marco Civil da Internet Lei nº 12.965/2014);
- Manter a integridade dos dados e das informações sensíveis dos sistemas da universidade;
- Melhorar o nível de qualidade de serviço das aplicações internas da universidade;
- Melhorar substancialmente o nível de segurança da informação da universidade;
- Permitir ao time de segurança da informação ter visibilidade das aplicações e os riscos que elas trazem

para o ambiente.

7.2. Requisitos de Capacitação

Os técnicos da envolvidos por parte da Contratante deverão realizar treinamento oficial do fabricante conforme especificado no item 4 deste termo de referência.

7.3. Requisitos Legais

Atender, quando aplicável, as diretrizes da Portaria nº 170 de abril de 2012 do Instituto Nacional de Metrologia, Qualidade e Tecnologia - INMETRO.

7.4. Requisitos de Manutenção

- 1) Todos os itens deste processo devem possuir garantia do fabricante ou autorizada no Brasil com validade mínima de 36 (trinta e seis) meses;
- 2) Durante o prazo de garantia, deve ser possível realizar a atualização de sistema operacional dos equipamentos para obter novas funcionalidades e correção de bugs;
- 3) Durante o prazo de garantia, deve ser possível realizar a atualização das assinaturas de proteção da solução;
- 4) Em caso de defeitos de fabricação, a garantia deve incluir envio de peças ou equipamentos de reposição nos locais especificados neste edital, obedecendo a modalidade NBD (Next Business Day);
- 5) Os chamados poderão ser abertos diretamente com a Licitante Vencedora ou autorizada oficial do fabricante no Brasil através de ligação telefônica gratuita (0800) no idioma português, website e e-mail durante a vigência da garantia. O suporte deverá ser na modalidade de 24x7 (24 horas por dia, 7 dias por semana);
- 6) O suporte deverá ter no mínimo o seguinte tempo de resposta para os níveis de severidade abaixo:
 - a. Crítico: significa que o produto ficou inoperante ou ocorreu falha de grande impacto e o sistema está parado. Para este nível de severidade o atendimento deve ser imediato e com tempo de resposta de até 1 (uma) hora para resolução total ou encontro de solução temporária de contorno. Neste caso o chamado deverá ser aberto via telefone (0800);
 - b. Alta: impacto moderado no sistema, travamento, ou parada de ambiente parcial. Para este nível de severidade o tempo de resposta deve ser de até 2 (duas) horas, em horário comercial, para resolução total ou encontro de solução temporária de contorno;
 - c. Média: Redução de performance do equipamento ou aplicação de solução temporária de contorno bem-sucedida. Para este nível de severidade o tempo de resposta deve ser de até 4 (quatro) horas, em horário comercial, para resolução total ou encontro de solução temporária de contorno;
 - d. Baixa: dúvidas de configuração ou anomalia de baixo impacto. Para este nível de severidade o tempo de resposta deve ser de até 8 (oito) horas, em horário comercial.

7.5. Requisitos Temporais

O prazo de entrega de produtos deverá ocorrer em até no máximo 90 (noventa) dias corridos a partir da data de assinatura do contrato.

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

A implantação completa da solução deve ser concluída em até 30 (trinta) dias corridos após a entrega do objeto.

7.6. Requisitos de Segurança

A Licitante Vencedora deverá submeter-se aos procedimentos de segurança existentes ou que possam ser criados durante a vigência do contrato. Os procedimentos deverão ser observados sempre que for necessária a presença nas dependências da Contratante.

7.7. Requisitos Sociais, Ambientais e Culturais

A documentação e os manuais da solução deverão ser apresentados no idioma Português (Brasil), eventualmente poderão ser apresentados em inglês.

Todos os contatos para gerenciamento de chamados e suporte técnico deverão ser realizados em Português (Brasil).

7.8. Requisitos de Arquitetura Tecnológica

Conforme disposto no item I do artigo 15 da lei 8.666, de 21 de junho de 1993 (I - Atender ao princípio de padronização, que imponha compatibilidade técnica e de desempenho, observadas, quando for o caso, as condições de manutenção, assistência técnica e garantia oferecidas), os equipamentos e softwares, por questões de compatibilidade, gerência, suporte e garantia, devem ser do mesmo fabricante.

7.9. Requisitos de Projeto e de Implementação

Antes de iniciar a implantação da solução a Licitante Vencedora deve apresentar um projeto e cronograma para instalação da solução. O projeto e o cronograma devem ser aprovados pela Contratante.

7.10. Requisitos de Implantação

A implantação deverá ser realizada por profissionais especializados da Licitante Vencedora, que possuam certificação do fabricante da solução adquirida que lhes confira as competências necessárias para a realização dos respectivos serviços de implantação, ou pelo próprio fabricante.

Deverá abranger a configuração de quaisquer funcionalidades suportadas pelos equipamentos. Estas informações serão documentadas no termo de abertura do projeto a ser elaborado pela LICITANTE VENCEDORA após alinhamento do escopo de trabalho definido entre LICITANTE VENCEDORA e CONTRATANTE.

7.11. Requisitos de Garantia

Toda solução deste termo de referência deverá considerar período de garantia por um prazo de até 36 meses, para hardware e licenças de software.

Os serviços de garantia deverão ser prestados pelo próprio fabricante da solução ofertada ou por empresa autorizada oficialmente pelo fabricante a prestar este tipo de serviço no Brasil.

Como comprovação de autorizada, deverá ser apresentado documento com informações da empresa prestadora da assistência técnica com sua identificação, endereço, CNPJ, responsável técnico e região de atuação.

7.12. Requisitos de Experiência Profissional

Os serviços de instalação e configuração dos itens relacionados nesta termo de referência deverão ser executados por técnicos capacitados com certificação oficial do fabricante.

A Licitante Vencedora deverá possuir, pelo menos, dois técnicos certificados oficialmente pelo fabricante da solução.

7.14. Requisitos de Metodologia de Trabalho

A metodologia de trabalho relacionado aos serviços prestados deverá observar os preceitos do ITIL V4.

7.15. Requisitos de Segurança da Informação

1. A solução Licitante Vencedora deverá respeitar a adequação à legislação vigente, tais como LGPD – Lei Geral de Proteção de Dados (Lei nº 13.709/2018) e Marco Civil da Internet Lei nº 12.965/2014).
2. A solução Licitante Vencedora deverá observar a Norma Brasileira ABNT NBR ISO/IEC 27002.
3. A Licitante Vencedora deverá manter a integridade da rede de dados e das informações da universidade.
4. A Licitante Vencedora deverá respeitar a Política de Segurança da Informação e Comunicações (POSIC) da Universidade Federal de Santa Maria bem como demais políticas e normas que poderão ser instituídas durante a vigência do contrato.
5. A Licitante Vencedora deverá guardar sigilo de todos os dados e informações a que tiver acesso, não podendo cedê-los a terceiros ou divulgá-los de qualquer forma.
6. Qualquer unidade de armazenamento, tais como SSDs, HDDs e memórias, utilizadas deverão permanecer em posse de Contratante mesmo após o uso, após dano ou após o término do contrato. Caso seja necessária a remoção de alguma unidade de armazenamento, esta ação deve ser realizada no prédio do CPD/UFSM e imediatamente entregue a Contratante.

8 – RESPONSABILIDADES

8.1. Deveres e responsabilidades da CONTRATANTE

- a) Nomear Gestor e Fiscais Técnico, Administrativo e Requisitante do contrato para acompanhar e fiscalizar a execução dos contratos;
- b) Encaminhar formalmente a demanda por meio de Ordem de Serviço ou de Fornecimento de Bens, de acordo com os critérios estabelecidos no Termo de Referência ou Projeto Básico;
- c) Receber o objeto fornecido pela Licitante Vencedora que esteja em conformidade com a proposta aceita, conforme inspeções realizadas;
- d) Aplicar à Licitante Vencedora as sanções administrativas regulamentares e contratuais cabíveis, comunicando ao órgão gerenciador da Ata de Registro de Preços, quando aplicável;
- e) Liquidar o empenho e efetuar o pagamento à Licitante Vencedora, dentro dos prazos preestabelecidos em contrato;
- f) Comunicar à Licitante Vencedora todas e quaisquer ocorrências relacionadas com o fornecimento da solução de TIC;
- g) Definir produtividade ou capacidade mínima de fornecimento da solução de TIC por parte da Licitante Vencedora, com base em pesquisas de mercado, quando aplicável; e
- h) Prever que os direitos de propriedade intelectual e direitos autorais da solução de TIC sobre os diversos artefatos e produtos produzidos em decorrência da relação contratual, incluindo a documentação, o código-fonte de aplicações, os modelos de dados e as bases de dados, pertençam à Administração.

8.2. Deveres e responsabilidades da LICITANTE VENCEDORA

- a) Indicar formalmente preposto apto a representá-lo junto à contratante, que deverá responder pela fiel execução do contrato;
- b) Atender prontamente quaisquer orientações e exigências da Equipe de Fiscalização do Contrato, inerentes à execução do objeto contratual;
- c) Efetuar a entrega do objeto em perfeitas condições, conforme especificações, prazo e local constantes no Edital e seus anexos, acompanhado da respectiva nota fiscal, na qual constarão as indicações referentes a: marca, fabricante, modelo, procedência e prazo de garantia ou validade;
- d) Fornecer equipamentos novos e realizar os serviços de instalação com a qualidade adequada;
- e) Reparar quaisquer danos diretamente causados à contratante ou a terceiros por culpa ou dolo de seus representantes legais, prepostos ou empregados, em decorrência da relação contratual, não excluindo ou reduzindo a responsabilidade da fiscalização ou o acompanhamento da execução dos serviços pela contratante;
- f) Propiciar todos os meios necessários à fiscalização do contrato pela contratante, cujo representante terá poderes para sustar o fornecimento, total ou parcial, em qualquer tempo, sempre que considerar a medida necessária;
- g) Manter, durante toda a execução do contrato, as mesmas condições da habilitação;
- h) Quando especificada, manter, durante a execução do contrato, equipe técnica composta por profissionais devidamente habilitados, treinados e qualificados para fornecimento da solução de TIC;
- i) Quando especificado, manter a produtividade ou a capacidade mínima de fornecimento da solução de TIC durante a execução do contrato; e
- j) Ceder os direitos de propriedade intelectual e direitos autorais da solução de TIC sobre os diversos artefatos e produtos produzidos em decorrência da relação contratual, incluindo a documentação, os modelos de dados e as bases de dados à Administração.

9 – MODELO DE EXECUÇÃO DO CONTRATO

9.1. Rotinas de Execução

- A. Realização de reunião inicial,

- B. Apresentação de projeto e cronograma de instalação pela Licitante Vencedora;
- C. Aprovação do projeto e cronograma de instalação pela Contratante;
- D. Entrega do(s) equipamento(s) respeitando o disposto no item 4.5 deste Termo de Referência;
- E. Verificação do(s) equipamento(s) recebidos com base nos requisitos deste Termo de Referência;
- F. Configuração e instalação do(s) equipamento(s) conforme o projeto;
- G. Ativação das licenças cuja duração deverá ser contada a partir do momento de ativação;
- H. Teste em ambiente de produção da UFSM dos requisitos e funcionalidades contidos neste Termo de Referência.
- I. Validação e aceite da UFSM.

A reunião inicial poderá ser realizada de forma remota ou presencial.

O(s) equipamento(s) deverão ser entregues e instalados no Centro de Processamento de Dados da Universidade de Santa Maria (Avenida Roraima, 1000, Prédio 48 - Camobi, RS, 97105-900).

O teste em ambiente de produção deve levar em conta um período normal de tráfego da UFSM, não podendo ser realizado durante férias ou outro período de baixa demanda. Se necessário, poderá ser realizado um teste de validação da capacidade máxima de tráfego utilizando uma ferramenta própria para este fim. Após 30 dias úteis de pleno funcionamento da solução será dado o aceite da UFSM para o serviço de instalação e configuração do(s) equipamento(s).

9.2. Quantidade mínima de bens ou serviços para comparação e controle

Não se aplica.

9.3. Mecanismos formais de comunicação

As questões administrativas formais ocorridas durante a execução do contrato serão tratadas através de ofício. Questões administrativas ou operacionais cotidianas durante a execução do contrato poderão ser tratadas através de mensagem eletrônica (e-mail), telefone ou aplicativo de mensagens.

9.4. Manutenção de Sigilo e Normas de Segurança

A Licitante Vencedora deverá manter sigilo absoluto sobre quaisquer dados e informações contidos em quaisquer documentos e mídias, incluindo os equipamentos e seus meios de armazenamento, de que venha a ter conhecimento durante a execução dos serviços, não podendo, sob qualquer pretexto, divulgar, reproduzir ou utilizar, sob pena de lei, independentemente da classificação de sigilo conferida pelo Contratante a tais documentos.

O **Termo de Compromisso**, contendo declaração de manutenção de sigilo e respeito às normas de segurança vigentes na entidade, a ser assinado pelo representante legal da Licitante Vencedora, encontra-se no ANEXO I.

10 – MODELO DE GESTÃO DO CONTRATO

10.1. Critérios de Aceitação

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

O aceite do bem somente será dado após comprovação da entrega e o efetivo cumprimento de todas as exigências presentes nas especificações técnicas deste termo de referência.

Será consultado diretamente no site do fabricante do equipamento manuais e toda documentação pública disponível para comprovação do pleno atendimento aos requisitos deste edital. Em caso de dúvidas ou divergência na comprovação da especificação técnica, este órgão poderá solicitar amostra do equipamento ofertado, sem ônus ao processo, para comprovação técnica de funcionalidades. Esta amostra deverá ocorrer em até 15 (quinze) dias úteis após a solicitação deste órgão. Para a amostra, a empresa deverá apresentar o mesmo modelo do equipamento ofertado no certame, com técnicos certificados na solução para

configuração e comprovação dos itens pendentes, nas dependências deste órgão.

10.2. Procedimentos de Teste e Inspeção

Na fase de aprovação da proposta técnica comercial durante a fase licitatória:

1. Será utilizado um método comparativo entre os requisitos da solução e os prospectos do fabricante.

Na fase de implantação da solução:

1. Após instalação e configuração da solução os itens constantes no Termo de Referência serão testados na solução a fim de verificar se as especificações são atendidas.
2. O aceite do bem somente será dado após comprovação da entrega e o efetivo cumprimento de todas as exigências da presente nas especificações técnicas deste termo de referência.

10.3. Níveis Mínimos de Serviço Exigidos

Os chamados poderão ser abertos diretamente com a Licitante Vencedora ou autorizada oficial do fabricante no Brasil através de ligação telefônica gratuita (0800) no idioma Português (Brasil), website e e-mail durante a vigência da garantia. O suporte deverá ser na modalidade de 24x7 (24 horas por dia, 7 dias por semana).

O suporte deverá ter no mínimo o seguinte tempo de resposta para os níveis de severidade abaixo:

Crítico: significa que o produto ficou inoperante ou ocorreu falha de grande impacto e o sistema está parado. Para este nível de severidade o atendimento deve ser imediato e com tempo de resposta de até 1 (uma) hora para resolução total ou encontro de solução temporária de contorno. Neste caso o chamado deverá ser aberto via telefone (0800);

Alta: impacto moderado no sistema, travamento, ou parada de ambiente parcial. Para este nível de severidade o tempo de resposta deve ser de até 2 (duas) horas, em horário comercial, para resolução total ou encontro de solução temporária de contorno;

Média: Redução de performance do equipamento ou aplicação de solução temporária de contorno bem-sucedida. Para este nível de severidade o tempo de resposta deve ser de até 4 (quatro) horas, em horário comercial, para resolução total ou encontro de solução temporária de contorno;

Baixa: dúvidas de configuração ou anomalia de baixo impacto. Para este nível de severidade o tempo de resposta deve ser de até 8 (oito) horas, em horário comercial.

SERVIÇO PÚBLICO FEDERAL**UNIVERSIDADE FEDERAL DE SANTA MARIA****CONTRATO Nº ____/____**

A UNIVERSIDADE FEDERAL DE SANTA MARIA, CNPJ 95.591.764/0001-05, sediada na Cidade Universitária, em Santa Maria, neste ato representada pelo Vice-Reitor, Prof. LUCIANO SCHUCH e a empresa _____, com sede na _____, Bairro _____, CEP _____, em _____ – _____, inscrita no CNPJ sob o nº _____, neste ato representada pelo Sr. _____, a seguir denominadas CONTRATANTE e CONTRATADA, respectivamente, com a finalidade da **CONTRATAÇÃO PARA A INSTALAÇÃO E AQUISIÇÃO DO EQUIPAMENTO DE SOLUÇÃO DE FIREWALL DE PRÓXIMA GERAÇÃO PARA SEGURANÇA DE INFORMAÇÃO PARA O CENTRO DE PROCESSAMENTO DE DADOS DA UNIVERSIDADE FEDERAL DE SANTA MARIA – UFSM**, de acordo com o que prescreve a Lei 8.666/93, alterada por Legislação Posterior, e Decreto 4.485, de 25 de novembro de 2002, e em face do que consta no **processo 23081.021471/2020-56** e da proposta da licitante vencedora do **Pregão Eletrônico 052/2020**, que é parte integrante deste, firmam o presente CONTRATO, para o fim acima e de acordo com o seguinte:

**CLÁUSULA PRIMEIRA
DO OBJETO**

A CONTRATADA compromete-se na implantação de solução de firewall de próxima geração para segurança da informação de perímetro que possibilite a visibilidade e controle de tráfego e aplicações em camada 7, filtragem de conteúdo web, prevenção contra ataques e ameaças avançadas e modernas, filtro de dados, VPN e controle granular de banda de rede, compreendendo fornecimento de equipamentos e softwares integrados em forma de appliance conforme quantidades e exigências estabelecidas neste instrumento, conforme relação em anexo ao contrato.

SUBCLÁUSULA PRIMEIRA

O prazo de entrega do equipamento deverá ocorrer em até no máximo 90 (noventa) dias corridos a partir da data de assinatura do contrato.

SUBCLÁUSULA SEGUNDA

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

SUBCLÁUSULA TERCEIRA

A implantação completa da solução deve ser concluída em até 30 (trinta) dias corridos após a entrega do objeto.

SUBCLÁUSULA QUARTA

Os equipamentos deverão ser entregues, em horário de expediente externo da UFSM, na Divisão de Patrimônio, localizada no Campus Universitário, Bairro Camobi, cidade de Santa Maria/RS.

SUBCLÁUSULA QUINTA

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

aceitos equipamentos com caixas violadas.

SUBCLÁUSULA SEXTA

A CONTRATANTE reserva-se ao direito de, a qualquer momento, aumentar ou reduzir o fornecimento do objeto deste CONTRATO nos limites da Lei 8.666/93, art. 65, § 1º.

SUBCLÁUSULA OITAVA

A contratada não poderá transferir a terceiros o objeto licitado.

CLÁUSULA SEGUNDA DA GARANTIA

A CONTRATADA deverá apresentar para toda solução a garantia por um prazo de até 36 meses anos, para hardware e licenças de software.

SUBCLÁUSULA PRIMEIRA

Os serviços de garantia deverão ser prestados pelo próprio fabricante da solução ofertada ou por empresa autorizada oficialmente pelo fabricante a prestar este tipo de serviço no Brasil.

SUBCLÁUSULA SEGUNDA

Como comprovação de autorizada, deverá ser apresentado documento com informações da empresa prestadora da assistência técnica com sua identificação, endereço, CNPJ, responsável técnico e região de atuação.

CLÁUSULA TERCEIRA REQUISITOS DE EXPERIENCIA PROFISSIONAL

Os serviços de instalação e configuração dos itens relacionados no termo de referência em anexo ao contrato deverão ser executados por técnicos capacitados com certificação oficial do fabricante. A contratada deverá possuir, pelo menos, dois técnicos certificados oficialmente pelo fabricante da solução.

CLÁUSULA QUARTA DOS REQUISITOS DE METODOLOGIA DE TRABALHO

A metodologia de trabalho relacionado aos serviços prestados deverá observar os preceitos do ITIL V4.

CLÁUSULA QUINTA DOS REQUISITOS DE NEGÓCIO

- Aquisição de solução de firewall de próxima geração, provendo visibilidade detalhada e controle do tráfego e proteção da rede;
- Adequação às legislações vigentes, tais como LGPD – Lei Geral de Proteção de Dados (Lei nº 13.709/2018) e Marco Civil da Internet Lei nº 12.965/2014);
- Manter a integridade dos dados e das informações sensíveis dos sistemas da universidade;
- Melhorar o nível de qualidade de serviço das aplicações internas da universidade;
- Melhorar substancialmente o nível de segurança da informação da universidade;

- Permitir ao time de segurança da informação ter visibilidade das aplicações e os riscos que elas trazem para o ambiente.

CLÁUSULA SEXTA DOS REQUISITOS DE CAPACITAÇÃO

Os técnicos da envolvidos por parte da Contratante deverão realizar treinamento oficial do fabricante conforme especificado no item 4 deste termo de referência.

CLÁUSULA SÉTIMA DOS REQUISITOS LEGAIS

Atender, quando aplicável, as diretrizes da Portaria nº 170 de abril de 2012 do Instituto Nacional de Metrologia, Qualidade e Tecnologia - INMETRO.

CLÁUSULA OITAVA DOS REQUISITOS DE MANUTENCAO

- Todos os itens deste processo devem possuir garantia do fabricante ou autorizada no Brasil com validade mínima de 36 (trinta e seis) meses;
- Durante o prazo de garantia, deve ser possível realizar a atualização de sistema operacional dos equipamentos para obter novas funcionalidades e correção de bugs;
- Durante o prazo de garantia, deve ser possível realizar a atualização das assinaturas de proteção da solução;
- Em caso de defeitos de fabricação, a garantia deve incluir envio de peças ou equipamentos de reposição nos locais especificados neste edital, obedecendo a modalidade NBD (Next Business Day);
- Os chamados poderão ser abertos diretamente com a contratada ou autorizada oficial do fabricante no Brasil através de ligação telefônica gratuita (0800) no idioma português, website e e-mail durante a vigência da garantia. O suporte deverá ser na modalidade de 24x7 (24 horas por dia, 7 dias por semana);
- O suporte deverá ter no mínimo o seguinte tempo de resposta para os níveis de severidade abaixo:
 - Crítico: significa que o produto ficou inoperante ou ocorreu falha de grande impacto e o sistema está parado. Para este nível de severidade o atendimento deve ser imediato e com tempo de resposta de até 1 (uma) hora para resolução total ou encontro de solução temporária de contorno. Neste caso o chamado deverá ser aberto via telefone (0800);
 - Alta: impacto moderado no sistema, travamento, ou parada de ambiente parcial. Para este nível de severidade o tempo de resposta deve ser de até 2 (duas) horas, em horário comercial, para resolução total ou encontro de solução temporária de contorno;
 - Média: Redução de performance do equipamento ou aplicação de solução temporária de contorno bem-sucedida. Para este nível de severidade o tempo de resposta deve ser de

até 4 (quatro) horas, em horário comercial, para resolução total ou encontro de solução temporária de contorno;

- Baixa: dúvidas de configuração ou anomalia de baixo impacto. Para este nível de severidade o tempo de resposta deve ser de até 8 (oito) horas, em horário comercial.

CLÁUSULA NONA REQUISITOS DE SEGURANÇA

A Contratada deverá submeter-se aos procedimentos de segurança existentes ou que possam ser criados durante a vigência do contrato. Os procedimentos deverão ser observados sempre que for necessária a presença nas dependências da Contratante.

CLÁUSULA DÉCIMA DOS REQUISITOS SOCIAIS, AMBIENTAIS E CULTURAIS

A documentação e os manuais da solução deverão ser apresentados no idioma Português (Brasil), eventualmente poderão ser apresentados em inglês.

Todos os contatos para gerenciamento de chamados e suporte técnico deverão ser realizados em Português (Brasil).

CLÁUSULA DÉCIMA PRIMEIRA DOS REQUISITOS DE ARQUITETURA TECNOLÓGICA

Conforme disposto no item I do artigo 15 da lei 8.666, de 21 de junho de 1993 (I - Atender ao princípio de padronização, que imponha compatibilidade técnica e de desempenho, observadas, quando for o caso, as condições de manutenção, assistência técnica e garantia oferecidas), os equipamentos e softwares, por questões de compatibilidade, gerência, suporte e garantia, devem ser do mesmo fabricante.

CLÁUSULA DÉCIMA SEGUNDA REQUISITOS DE PROJETO E DE IMPLANTAÇÃO

Antes de iniciar a implantação da solução a Contratada deve apresentar um projeto e cronograma para instalação da solução. O projeto e o cronograma devem ser aprovados pela Contratante.

CLÁUSULA DÉCIMA TERCEIRA DOS REQUISITOS DA IMPLANTAÇÃO

A implantação deverá ser realizada por profissionais especializados da contratada, que possuam certificação do fabricante da solução adquirida que lhes confira as competências necessárias para a realização dos respectivos serviços de implantação, ou pelo próprio fabricante.

SUBCLÁUSULA PRIMEIRA

Deverá abranger a configuração de quaisquer funcionalidades suportadas pelos equipamentos. Estas informações serão documentadas no termo de abertura do projeto a ser elaborado pela CONTRATADA após alinhamento do escopo de trabalho definido entre CONTRATADA e CONTRATANTE.

CLÁUSULA DÉCIMA QUARTA DOS REQUISITOS DE EXPERIÊNCIA PROFISSIONAL

Os serviços de instalação e configuração dos itens relacionados nesta termo de referência deverão ser executados por técnicos capacitados com certificação oficial do fabricante.

A contratada deverá possuir, pelo menos, dois técnicos certificados oficialmente pelo fabricante da solução.

CLÁUSULA DÉCIMA QUINTA DOS REQUISITOS DE METODOLOGIA DE TRABALHO

A metodologia de trabalho relacionado aos serviços prestados deverá observar os preceitos do ITIL V4.

CLÁUSULA DÉCIMA SEXTA DOS REQUISITOS DE SEGURANÇA DA INFORMAÇÃO

-A solução contratada deverá respeitar a adequação à legislação vigente, tais como LGPD – Lei Geral de Proteção de Dados (Lei nº 13.709/2018) e Marco Civil da Internet Lei nº 12.965/2014).

-A solução contratada deverá observar a Norma Brasileira ABNT NBR ISO/IEC 27002.

-A Contratada deverá manter a integridade da rede de dados e das informações da universidade.

-A Contratada deverá respeitar a Política de Segurança da Informação e Comunicações (POSIC) da Universidade Federal de Santa Maria bem como demais políticas e normas que poderão ser instituídas durante a vigência do contrato.

-A Contratada deverá guardar sigilo de todos os dados e informações a que tiver acesso, não podendo cedê-los a terceiros ou divulgá-los de qualquer forma.

-Qualquer unidade de armazenamento, tais como SSDs, HDDs e memórias, utilizadas deverão permanecer em posse de Contratante mesmo após o uso, após dano ou após o término do contrato. Caso seja necessária a remoção de alguma unidade de armazenamento, esta ação deve ser realizada no prédio do CPD/UFSM e imediatamente entregue a Contratante.

CLÁUSULA DÉCIMA SÉTIMA DEVERES E RESPONSABILIDADE DA CONTRATANTE

-Nomear Gestor e Fiscais Técnico, Administrativo e Requisitante do contrato para acompanhar e fiscalizar a execução dos contratos;

- Encaminhar formalmente a demanda por meio de Ordem de Serviço ou de Fornecimento de Bens, de acordo com os critérios estabelecidos no Termo de Referência ou Projeto Básico;

- Receber o objeto fornecido pela contratada que esteja em conformidade com a proposta aceita, conforme inspeções realizadas;

- Aplicar à contratada as sanções administrativas regulamentares e contratuais cabíveis, comunicando ao órgão gerenciador da Ata de Registro de Preços, quando aplicável;

- Liquidar o empenho e efetuar o pagamento à contratada, dentro dos prazos preestabelecidos em contrato;
- Comunicar à contratada todas e quaisquer ocorrências relacionadas com o fornecimento da solução de TIC;
- Definir produtividade ou capacidade mínima de fornecimento da solução de TIC por parte da contratada, com base em pesquisas de mercado, quando aplicável; e
- Prever que os direitos de propriedade intelectual e direitos autorais da solução de TIC sobre os diversos artefatos e produtos produzidos em decorrência da relação contratual, incluindo a documentação, o código-fonte de aplicações, os modelos de dados e as bases de dados, pertençam à Administração.

CLÁUSULA DÉCIMA OITAVA DEVERES E RESPONSABILIDADE DA CONTRATADA

- Indicar formalmente preposto apto a representá-lo junto à contratante, que deverá responder pela fiel execução do contrato; Atender prontamente quaisquer orientações e exigências da Equipe de Fiscalização do Contrato, inerentes à execução do objeto contratual;
- Efetuar a entrega do objeto em perfeitas condições, conforme especificações, prazo e local constantes no Edital e seus anexos, acompanhado da respectiva nota fiscal, na qual constarão as indicações referentes a: marca, fabricante, modelo, procedência e prazo de garantia ou validade; Fornecer equipamentos novos e realizar os serviços de instalação com a qualidade adequada;
- Reparar quaisquer danos diretamente causados à contratante ou a terceiros por culpa ou dolo de seus representantes legais, prepostos ou empregados, em decorrência da relação contratual, não excluindo ou reduzindo a responsabilidade da fiscalização ou o acompanhamento da execução dos serviços pela contratante;
- Propiciar todos os meios necessários à fiscalização do contrato pela contratante, cujo representante terá poderes para sustar o fornecimento, total ou parcial, em qualquer tempo, sempre que considerar a medida necessária;
- Manter, durante toda a execução do contrato, as mesmas condições da habilitação;
- Quando especificada, manter, durante a execução do contrato, equipe técnica composta por profissionais devidamente habilitados, treinados e qualificados para fornecimento da solução de TIC;
- Quando especificado, manter a produtividade ou a capacidade mínima de fornecimento da solução de TIC durante a execução do contrato; e ceder os direitos de propriedade intelectual e direitos autorais da solução de TIC sobre os diversos artefatos e produtos produzidos em decorrência da relação contratual, incluindo a documentação, os modelos de dados e as bases de dados à Administração.

CLÁUSULA DÉCIMA NONA ROTINAS DE EXECUÇÃO

- Realização de reunião inicial,
- Apresentação de projeto e cronograma de instalação pela Contratada;
- Aprovação do projeto e cronograma de instalação pela Contratante;
- Entrega do(s) equipamento(s) respeitando o disposto no item 4.5 deste Termo de Referência;

- Verificação do(s) equipamento(s) recebidos com base nos requisitos deste Termo de Referência;
- Configuração e instalação do(s) equipamento(s) conforme o projeto;
- Ativação das licenças cuja duração deverá ser contada a partir do momento de ativação;
- Teste em ambiente de produção da UFSM dos requisitos e funcionalidades contidos neste Termo de Referência.
- Validação e aceite da UFSM.

SUBCLÁUSULA PRIMEIRA

A reunião inicial poderá ser realizada de forma remota ou presencial. O(s) equipamento(s) deverão ser entregues e instalados no Centro de Processamento de Dados da Universidade de Santa Maria (Avenida Roraima, 1000, Prédio 48 - Camobi, RS, 97105-900). O teste em ambiente de produção deve levar em conta um período normal de tráfego da UFSM, não podendo ser realizado durante férias ou outro período de baixa demanda. Se necessário, poderá ser realizado um teste de validação da capacidade máxima de tráfego utilizando uma ferramenta própria para este fim. Após 30 dias úteis de pleno funcionamento da solução será dado o aceite da UFSM para o serviço de instalação e configuração do(s) equipamento(s).

CLÁUSULA VIGÉSIMA

Quantidade mínima de bens ou serviços para comparação e controle não se aplica.

CLÁUSULA VIGÉSIMA PRIMEIRA

DOS MECANISMOS FORMAIS DE COMUNICAÇÃO

As questões administrativas formais ocorridas durante a execução do contrato serão tratadas através de ofício. Questões administrativas ou operacionais cotidianas durante a execução do contrato poderão ser tratadas através de mensagem eletrônica (e-mail), telefone ou aplicativo de mensagens.

CLÁUSULA VIGÉSIMA SEGUNDA

DA MANUTENÇÃO DE SIGILO E NORMAS DE SEGURANÇA

A Contratada deverá manter sigilo absoluto sobre quaisquer dados e informações contidos em quaisquer documentos e mídias, incluindo os equipamentos e seus meios de armazenamento, de que venha a ter conhecimento durante a execução dos serviços, não podendo, sob qualquer pretexto, divulgar, reproduzir ou utilizar, sob pena de lei, independentemente da classificação de sigilo conferida pelo Contratante a tais documentos.

SUBCLÁUSULA PRIMEIRA

O **Termo de Compromisso**, contendo declaração de manutenção de sigilo e respeito às normas de segurança vigentes na entidade, a ser assinado pelo representante legal da Contratada, encontra-se no ANEXO II.

CLÁUSULA VIGÉSIMA TERCEIRA OS CRITÉRIOS DE ACEITAÇÃO

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

SUBCLÁUSULA PRIMEIRA

O aceite do bem somente será dado após comprovação da entrega e o efetivo cumprimento de todas as exigências presentes nas especificações técnicas deste termo de referência.

SUBCLÁUSULA SEGUNDA

Será consultado diretamente no site do fabricante do equipamento manuais e toda documentação pública disponível para comprovação do pleno atendimento aos requisitos deste edital. Em caso de dúvidas ou divergência na comprovação da especificação técnica, este órgão poderá solicitar amostra do equipamento ofertado, sem ônus ao processo, para comprovação técnica de funcionalidades. Esta amostra deverá ocorrer em até 15 (quinze) dias úteis após a solicitação deste órgão. Para a amostra, a empresa deverá apresentar o mesmo modelo do equipamento ofertado no certame, com técnicos certificados na solução para configuração e comprovação dos itens pendentes, nas dependências deste órgão.

CLÁUSULA VIGÉSIMA QUARTA PROCEDIMENTOS DE TESTES DE INSPEÇÃO

Na fase de aprovação da proposta técnica comercial durante a fase licitatória:

- Será utilizado um método comparativo entre os requisitos da solução e os prospectos do fabricante.

- Após instalação e configuração da solução os itens constantes no Termo de Referência serão testados na solução a fim de verificar se as especificações são atendidas.

- O aceite do bem somente será dado após comprovação da entrega e o efetivo cumprimento de todas as exigências da presente nas especificações técnicas deste termo de referência.

CLÁUSULA VIGÉSIMA QUINTA DOS NÍVEIS MÍNIMOS DE SERVIÇOS EXIGIDOS

Os chamados poderão ser abertos diretamente com a contratada ou autorizada oficial do fabricante no Brasil através de ligação telefônica gratuita (0800) no idioma Português (Brasil), website e e-mail durante a vigência da garantia. O suporte deverá ser na modalidade de 24x7 (24 horas por dia, 7 dias por semana). O suporte deverá ter no mínimo o seguinte tempo de resposta para os níveis de severidade abaixo:

SUBCLÁUSULA PRIMEIRA

Crítico:significa que o produto ficou inoperante ou ocorreu falha de grande impacto e o sistema está parado. Para este nível de severidade o atendimento deve ser imediato e com tempo de resposta de até 1 (uma) hora para resolução total ou encontro de solução temporária de contorno. Neste caso o chamado deverá ser aberto via telefone (0800);

Alta:impacto moderado no sistema, travamento, ou parada de ambiente parcial. Para este nível de severidade o tempo de resposta deve ser de até 2 (duas) horas, em horário comercial, para resolução total ou encontro de solução temporária de contorno;

Média:Redução de performance do equipamento ou aplicação de solução temporária de contorno bem-sucedida. Para este nível de severidade o tempo de resposta deve ser de até 4 (quatro) horas, em horário comercial, para resolução total ou encontro de solução temporária de contorno;

Baixa:dúvidas de configuração ou anomalia de baixo impacto. Para este nível de severidade o tempo de resposta deve ser de até 8 (oito) horas, em horário comercial.

CLÁUSULA VIGÉSIMA SEXTA DA VIGÊNCIA DO CONTRATO

O contrato vigorará por **36 (trinta e seis) meses**, contados a partir da data da sua assinatura, podendo ser prorrogado por períodos iguais e sucessivos, limitado a 60(sessenta) meses desde que haja preços e condições mais vantajosas para a Administração, nos termos do Inciso II, Art. 57, Lei nº 8.666, de 1993.

SUBCLÁUSULA PRIMEIRA

A prorrogação do contrato dependerá da verificação da manutenção da necessidade, economicidade e oportunidade da contratação, acompanhada de a realização de pesquisa de mercado que demonstre a vantajosidade dos preços contratados para a Administração

CLÁUSULA VIGÉSIMA OITAVA DO VALOR DO CONTRATO

Importa a presente contratação no valor total de R\$ _____ (_____), conforme preços detalhados no anexo a este contrato, que faz parte deste, como se aqui estivesse transcrito.

CLÁUSULA VIGÉSIMA NONA DO PAGAMENTO

A CONTRATANTE efetuará o pagamento, mediante apresentação da Nota Fiscal/Fatura, discriminando os equipamentos instalados bem como os serviços efetivamente executados; devidamente certificada pelo Centro de Processamento de Dados da Universidade Federal de Santa Maria/UFSM, pelo gestor deste contrato ou seu substituto, no prazo máximo de até 30 (trinta) dias úteis, a contar da data de entrega/instalação na UFSM, desde que não haja impedimento legal.

SUBCLÁUSULA PRIMEIRA

O valor do pagamento será atualizado monetariamente pela variação do INPC/IBGE, ocorrida no período, a partir da data do prazo final do adimplemento da obrigação até o efetivo pagamento.

CLÁUSULA TRIGÉSIMA DOS RECURSOS ORÇAMENTÁRIOS

Para atender as despesas decorrentes do presente CONTRATO a CONTRATANTE emitiu a Nota de Empenho nº 2020NE_____, em anexo ao presente contrato independente de transcrição.

CLÁUSULA TRIGÉSIMA PRIMEIRA DO GESTOR DO CONTRATO

O Servidor Gustavo Zanini Kantorki **SIAPÉ,1108102**, **lotado no** CENTRO DE PROCESSAMENTOS DE DADOS da Universidade Federal de Santa Maria, fica indicados como gestor, na forma do art. 67 da Lei nº 8.666/93, para acompanhar e fiscalizar a execução do presente Contrato.

CLÁUSULA TRIGÉSIMA SEGUNDA DAS PENALIDADES

As penalidades pela inexecução (artigo 77 da Lei 8.666/93) encontram-se previstas nos artigos 86 e 87 do mesmo diploma legal.

SUBCLÁUSULA PRIMEIRA

A advertência verbal ou escrita será aplicada, independentemente de outras sanções cabíveis, quando houver afastamento das condições contratuais ou das condições técnicas estabelecidas.

SUBCLÁUSULA SEGUNDA

As penalidades a que está sujeita a CONTRATADA, a teor do que reza o art. 87 da Lei 8.666/93, são as seguintes:

- I) advertência;
- II) multa;
- III) suspensão temporária de participação em licitações; e
- IV) impedimento de contratar com a Administração por prazo não superior a 02 (dois) anos e;
- V) declaração de inidoneidade para licitar ou contratar com a Administração.

CLÁUSULA TRIGÉSIMA TERCEIRA DAS MULTAS

A multa em caso de atraso na entrega das mercadorias solicitadas será de 0,5% (cinco décimos por cento) ao dia sobre o valor do produto/serviços não entregue.

SUBCLÁUSULA PRIMEIRA

CONTRATADA incorrerá em atraso na entrega do objeto licitado se não fornecer o produto a partir do 1º (primeiro) dia após o prazo estipulado na Subcláusula Primeira da Cláusula Primeira deste Contrato.

SUBCLÁUSULA SEGUNDA

A multa por atraso no cumprimento da Subcláusula Primeira da Cláusula Primeira do presente contrato será de 0,5% (cinco décimos por cento) ao dia sobre o valor do equipamento não entregue e/ou não instalado.

SUBCLÁUSULA TERCEIRA

A Multa em caso de inadimplemento da CONTRATADA será de 20% (vinte por cento) sobre o valor contratado que deixar de ser entregue.

SUBCLÁUSULA QUARTA

A CONTRATADA também será considerada inadimplente se não cumprir com todas as obrigações contidas no contrato, ficando sujeita às penalidades e às multas descritas acima, sem prejuízo do processo administrativo.

CLÁUSULA TRIGÉSIMA QUARTA DA GARANTIA CONTRATUAL

Para garantia da boa execução dos termos deste Contrato e pagamento de eventuais multas, a CONTRATADA cauciona a importância de R\$ _____ (_____), equivalente a 5% (cinco por cento) do valor do contrato, mediante

SUBCLÁUSULA PRIMEIRA

Esta garantia será restituída à CONTRATADA, de forma integral ou o que dela restar, após o término do contrato.

CLÁUSULA TRIGÉSIMA QUINTA DA RESCISÃO ADMINISTRATIVA

A CONTRATADA reconhece, na hipótese de rescisão administrativa, prevista no artigo 77 da Lei 8.666/93, os direitos da CONTRATANTE, conforme prevê o art. 55, inciso IX, do mesmo diploma legal.

CLÁUSULA TRIGESIMA SEXTA DAS CONDIÇÕES DE QUALIFICAÇÃO E HABILITAÇÃO

A CONTRATADA obriga-se a manter, durante a vigência deste CONTRATO, as condições de qualificação e habilitação exigidas na Lei 8.666/93. A qualquer tempo a CONTRATANTE poderá solicitar a comprovação da habilitação e qualificações em questão, conforme art. 55, inciso XIII da referida Lei.

CLÁUSULA TRIGÉSIMA OITAVA ANTICORRUPÇÃO LEI Nº. 12.846/2013

Para a execução deste contrato, nenhuma das partes poderá oferecer dar ou se comprometer a dar a quem quer que seja, ou aceitar ou se comprometer a aceitar de quem quer que seja, tanto por conta própria quanto através de outrem, qualquer pagamento, doação, compensação, vantagens financeiras ou não financeiras ou benefícios de qualquer espécie que constituam prática ilegal ou de corrupção sob as leis de qualquer país, seja de forma direta ou indireta quanto ao objeto deste contrato, ou de outra forma que não relacionada a este contrato, devendo garantir, ainda, que seus prepostos e colaboradores ajam da mesma forma.

CLÁUSULA TRIGÉSIMA NONA
DO FORO

As partes elegem o foro da Justiça Federal, na cidade de Santa Maria, para dirimir as questões oriundas deste CONTRATO.

E, para constar, lavrou-se o presente TERMO DE CONTRATO, que lido e achado conforme, vai assinado pelas partes CONTRATANTES, na presença das testemunhas abaixo firmadas, maiores e capazes.

Santa Maria, ____ de _____ de 2020.

CONTRATANTE

CONTRATADA

TESTEMUNHA

TESTEMUNHA



ANEXO AO CONTRATO...../2020**2. OBJETO DA LICITAÇÃO**

Esta licitação tem por objeto o Registro de Preços para contratação de solução de firewall de próxima geração para segurança da informação de perímetro que possibilite a visibilidade e controle de tráfego e aplicações em camada 7, filtragem de conteúdo web, prevenção contra ataques e ameaças avançadas e modernas, filtro de dados, VPN e controle granular de banda de rede, compreendendo fornecimento de equipamentos e softwares integrados em forma de appliance conforme quantidades e exigências estabelecidas neste instrumento.

2. Bens e serviços que compõem a solução

GRUPO	Id.	Descrição do Bem ou Serviço	Código CATMAT/CATSER	QTD	Métrica ou Unidade
1	1	FIREWALL TIPO 1 COM SUPORTE, GARANTIA E LICENÇAS DE PROTEÇÃO COM VIGÊNCIA DE 03 ANOS	150100	2	Peça
	2	FIREWALL TIPO 2 COM SUPORTE, GARANTIA E LICENÇAS DE PROTEÇÃO COM VIGÊNCIA DE 03 ANOS	150100	2	Peça
	3	SERVIÇOS DE INSTALAÇÃO DE FIREWALL	5390	4	Serviço
	4	TREINAMENTO OFICIAL DE FIREWALL DE PRÓXIMA GERAÇÃO	3840	4	Serviço

3. Estimativa da demanda

GRUPO	Item	Descrição	Valor unitário máximo
1	1	FIREWALL TIPO 1 COM SUPORTE, GARANTIA E LICENÇAS DE PROTEÇÃO COM VIGÊNCIA DE 36 MESES.	R\$
	2	FIREWALL TIPO 2 COM SUPORTE, GARANTIA E LICENÇAS DE PROTEÇÃO COM VIGÊNCIA DE 36 MESES.	R\$
	3	SERVIÇOS DE INSTALAÇÃO DE FIREWALL	R\$
	4	TREINAMENTO OFICIAL DE FIREWALL DE PRÓXIMA GERAÇÃO	R\$

4. OS PREÇOS

Id.	Descrição do Bem ou Serviço	Qtd	Unidade de medida	Valor unitário	Valor total
1	FIREWALL TIPO 1 COM SUPORTE, GARANTIA E LICENÇAS DE PROTEÇÃO COM VIGÊNCIA DE 36 MESES	2	Peça	R\$	R\$
2	FIREWALL TIPO 2 COM SUPORTE, GARANTIA E LICENÇAS DE	2	Peça	R\$	R\$

	PROTEÇÃO COM VIGÊNCIA DE 36 MESES				
3	SERVIÇOS DE INSTALAÇÃO DE FIREWALL	4	Serviço	R\$	R\$
4	TREINAMENTO OFICIAL DE FIREWALL DE PRÓXIMA GERAÇÃO	4	Serviço	R\$	R\$

5. Parcelamento da Solução de TIC

Os equipamentos, licenças e serviços que constituem a solução aqui proposta se interagem entre si de forma a convergir para um sistema unificado, de modo que o fornecimento parcelado inviabilizaria a implantação de tecnologia capaz de atender as necessidades deste órgão.

A eventual divisão do objeto em grupos diversos poderia ocasionar uma situação onde um proponente "A", por não conhecer a solução, não teria condições de fornecer eventual licenciamento correto para tal ou mesmo propor equipamentos compatíveis. Ante ao exposto, é evidente que o agrupamento do objeto, de maneira a compor uma solução unificada, é necessário a fim de evitar eventuais problemas de compatibilidade.

Ademais, lidar com um único fornecedor diminui o custo administrativo de gerenciamento de todo o processo de contratação. O aumento da eficiência administrativa do setor público passa pela otimização do gerenciamento de seus contratos de fornecimento. Essa eficiência administrativa também é de estatura constitucional e deve ser buscada pela administração pública.

Por fim, o agrupamento em lote de todos os itens deste processo visa garantir a otimização dos prazos de execução, viabilizando a sincronia nos fornecimentos e serviços de instalações e treinamento, evitando assim que um fornecedor venha a prejudicar a execução de outro.

5.1. Resultados e Benefícios a Serem Alcançados

1-Adequação às legislações vigentes, tais como LGPD – Lei Geral de Proteção de Dados (Lei nº 13.709/2018) e Marco Civil da Internet Lei nº 12.965/2014);

2-Maior visibilidade do tráfego de rede e aplicações em camada 7, possibilitando a detecção e proteção em tempo real contra ameaças;

3-Proteção do ambiente de rede contra ameaças tipo worms, vírus, malwares entre outras pragas virtuais, atendendo às exigências do Marco Civil da Internet.

4-Geração de relatórios diversos para rápida análise de informações sobre tráfego, aplicações, ameaças, etc.

5-Implantação de controle de acesso à rede, possibilitando a rastreabilidade de usuários e endereços IP, atendendo ao Marco Civil da Internet Lei nº 12.965/2014;

6-Melhoria da qualidade da internet disponibilizada, diminuindo perda e tempo de transmissão de pacotes;

7-Criação de políticas e medidas de segurança para proteção da rede contra ataques e/ou invasões.

6 – ESPECIFICAÇÃO DOS REQUISITOS DA CONTRATAÇÃO

Aquisição de solução de proteção de rede com características de Next Generation Firewall (NGFW) para segurança de informação perimetral que inclui filtro de pacote, controle de aplicação, administração de largura de banda (QoS), VPN IPSec e SSL, IPS, prevenção contra ameaças de vírus, spywares e malwares "Zero Day", Filtro de URL, bem como controle de transmissão de dados e acesso à internet compondo uma plataforma de segurança integrada e robusta.

6.1 CARACTERÍSTICAS GERAIS COMUNS AOS ITENS 1 E 2

1.52. A solução deve consistir em appliance de proteção de rede com funcionalidades de Next Generation Firewall (NGFW), e console de gerência e monitoração;

1.53. Por funcionalidades de NGFW entende-se: reconhecimento de aplicações, prevenção de ameaças, identificação de usuários e controle granular de permissões;

- 1.54. As funcionalidades de proteção de rede que compõe a plataforma de segurança, podem funcionar em múltiplos appliances desde que obedeçam a todos os requisitos desta especificação;
- 1.55. A plataforma deve ser otimizada para análise de conteúdo de aplicações em camada 7;
- 1.56. O hardware e software que executem as funcionalidades de proteção de rede, bem como a console de gerência e monitoração, devem ser do tipo appliance. Não serão aceitos equipamentos servidores e sistema operacional de uso genérico;
- 1.57. Todos os equipamentos fornecidos devem ser próprios para montagem em rack 19", incluindo kit tipo trilho para adaptação se necessário e cabos de alimentação;
- 1.58. O software deverá ser fornecido em sua versão mais atualizada;
- 1.59. Os dispositivos de proteção de rede devem possuir pelo menos as seguintes funcionalidades:
- 1.59.1. Suporte a 4094 VLAN Tags 802.1q;
 - 1.59.2. Agregação de links 802.3ad e LACP;
 - 1.59.3. Policy based routing ou policy based forwarding;
 - 1.59.4. Roteamento multicast (PIM-SM);
 - 1.59.5. DHCP Relay;
 - 1.59.6. DHCP Server;
 - 1.59.7. Jumbo Frames;
 - 1.59.8. Suporte a criação de objetos de rede que possam ser utilizados como endereço IP de interfaces L3
- 1.60. Suportar sub-interfaces ethernet lógicas;
- 1.60.1. Suporte a, no mínimo, 10 (dez) roteadores virtuais na mesma instância de firewall;
- 1.61. O firewall deve ter a capacidade de testar o funcionamento de rotas estáticas e rota default com a definição de um endereço IP de destino que deve estar comunicável através de uma rota. Caso haja falha na comunicação o firewall deve ter a capacidade de usar rota alternativa para estabelecer a comunicação;
- 1.62. Deve suportar os seguintes tipos de NAT:
- 1.62.1. Nat dinâmico (Many-to-1);
 - 1.62.2. Nat dinâmico (Many-to-Many);
 - 1.62.3. Nat estático (1-to-1);
 - 1.62.4. NAT estático (Many-to-Many);
 - 1.62.5. Nat estático bidirecional 1-to-1;
 - 1.62.6. Tradução de porta (PAT);
 - 1.62.7. NAT de Origem;
 - 1.62.8. NAT de Destino;
 - 1.62.9. Suportar NAT de Origem e NAT de Destino simultaneamente;
 - 1.62.10. Deve implementar Network Prefix Translation (NPTv6), prevenindo problemas de roteamento assimétrico;
 - 1.62.11. Deve implementar balanceamento de link através de políticas por usuário e grupos de usuários do LDAP/AD;
 - 1.62.12. Deve implementar balanceamento de link através de políticas por aplicação e porta de destino;
 - 1.62.13. Deve implementar o protocolo Link Layer Discovery (LLDP), permitindo que o appliance e outros ativos da rede se comuniquem para identificação da topologia da rede em que estão conectados e a função dos mesmos facilitando o processo de troubleshooting. As informações aprendidas e armazenadas pelo appliance devem ser acessíveis via SNMP;
 - 1.62.14. Enviar log para sistemas de monitoração externos, simultaneamente;
 - 1.62.15. Deve haver a opção de enviar logs para os sistemas de monitoração externos via protocolo TCP e SSL;
 - 1.62.16. Deve permitir configurar certificado caso necessário para autenticação no sistema de monitoração externo de logs;
 - 1.62.17. Proteção contra anti-spoofing;
 - 1.62.18. Deve permitir bloquear sessões TCP que usem variações do 3-way hand-shake, como 4 way e 5 way split hand-shake, prevenindo desta forma possíveis tráfegos maliciosos;
 - 1.62.19. Deve permitir bloquear conexões que contenham dados no payload de pacotes TCP-SYN e SYN-ACK durante o three-way handshake;

- 1.62.20. Deve exibir nos logs de tráfego o motivo para o término da sessão no firewall, incluindo sessões finalizadas onde houver de-criptografia de SSL e SSH;
- 1.62.21. Suportar no mínimo as seguintes funcionalidades em IPv6: SLAAC (address auto configuration), NAT64, Identificação de usuários a partir do LDAP/AD, Captive Portal, IPv6 over IPv4 IPSec, Regras de proteção contra DoS (Denial of Service), De-criptografia SSL e SSH, PBF (Policy Based Forwarding), QoS, DHCPv6 Relay, IPSec, VPN SSL, Ativo/Ativo, Ativo/Passivo, SNMP, NTP, SYSLOG, DNS, Neighbor Discovery (ND), Recursive DNS Server (RDNS), DNS Search List (DNSSL) e controle de aplicação;
- 1.62.22. O dispositivos de proteção devem ter a capacidade de operar de forma simultânea em uma única instância de firewall, mediante o uso de suas interfaces físicas nos seguintes modos: Modo sniffer (monitoramento e análise do tráfego de rede), camada 2 (L2) e camada 3 (L3);
- 1.62.22.1. Modo Sniffer, para inspeção via porta espelhada do tráfego de dados da rede;
- 1.62.22.2. Modo Camada – 2 (L2), para inspeção de dados em linha e ter visibilidade e controle do tráfego em nível de aplicação;
- 1.62.22.3. Modo Camada – 3 (L3), para inspeção de dados em linha e ter visibilidade e controle do tráfego em nível de aplicação operando como default gateway das redes protegidas;
- 1.62.23. Modo misto de trabalho Sniffer, L2 e L3 em diferentes interfaces físicas;
- 1.63. Suporte a configuração de alta disponibilidade Ativo/Passivo e Ativo/Ativo:
 - 1.63.1. Em modo transparente;
 - 1.63.2. Em layer 3;
- 1.64. A configuração em alta disponibilidade deve sincronizar:
 - 1.64.1. Sessões;
 - 1.64.2. Configurações, incluindo, mas não limitado a políticas de Firewall, NAT, QOS e objetos de rede;
 - 1.64.3. Certificados de-criptografados;
 - 1.64.4. Associações de Segurança das VPNs;
 - 1.64.5. Tabelas FIB;
 - 1.64.6. O HA (modo de Alta-Disponibilidade) deve possibilitar monitoração de falha de link.
- 1.65. As funcionalidades de controle de aplicações, VPN IPSec e SSL, QOS, SSL e SSH Decryption e protocolos de roteamento dinâmico devem operar em caráter permanente, podendo ser utilizadas por tempo indeterminado, mesmo que não subsista o direito de receber atualizações ou que não haja contrato de garantia de software com o fabricante.

CONTROLE POR POLÍTICA DE FIREWALL

- 1.20. Deverá suportar controles por zona de segurança.
- 1.21. Deverá suportar controles de políticas por porta e protocolo.
- 1.22. Deverá suportar controle de políticas por aplicações, grupos estáticos de aplicações, grupos dinâmicos de aplicações (baseados em características e comportamento das aplicações) e categorias de aplicações.
- 1.23. Deverá suportar controle de políticas por usuários, grupos de usuários, IPs, redes e zonas de segurança.
- 1.24. Deve suportar a consulta a fontes externas de endereços IP, domínios e URLs podendo ser adicionados nas políticas de firewall para bloqueio ou permissão do tráfego;
 - 1.24.1. Deve permitir autenticação segura através de certificado nas fontes externas de endereços IP, domínios e URLs;
 - 1.24.2. Deve permitir consultar e criar exceção para objetos das listas externas a partir da interface de gerência do próprio firewall;
- 1.25. Controle, inspeção e de-criptografia de SSL por política para tráfego de entrada (Inbound) e Saída (Outbound).
- 1.26. Deve suportar offload de certificado em inspeção de conexões SSL de entrada (Inbound);
- 1.27. Deve de-criptografar tráfego Inbound e Outbound em conexões negociadas com TLS 1.2;

- 1.28. Deve de-criptografar sites e aplicações que utilizam certificados ECC, incluindo Elliptical Curve Digital Signature Algorithm (ECDSA);
- 1.29. Controle de inspeção e de-criptografia de SSH por política;
- 1.30. A de-criptografia de SSH deve possibilitar a identificação e bloqueio de tráfego caso o protocolo esteja sendo usado para tunelar aplicações como técnica evasiva para burlar os controles de segurança;
- 1.31. A plataforma de segurança deve implementar espelhamento de tráfego de-criptografado (SSL e TLS) para soluções externas de análise (Forense de rede, DLP, Análise de Ameaças, entre outras);
 - 1.31.1. É permitido uso de appliance externo, específico para a de-criptografia de (SSL e TLS), com espelhamento de cópia do tráfego de-criptografado tanto para o firewall, quanto para as soluções de análise.
- 1.32. Bloqueios dos seguintes tipos de arquivos: bat, cab, dll, exe, pif, e reg
- 1.33. Traffic shaping QoS baseado em Políticas (Prioridade, Garantia e Máximo)
- 1.34. QoS baseado em políticas para marcação de pacotes (diffserv marking), inclusive por aplicações.
- 1.35. Suporte a objetos e regras IPV6.
- 1.36. Suporte a objetos e regras multicast.
- 1.37. Deve suportar no mínimo três tipos de negação de tráfego nas políticas de firewall: Drop sem notificação do bloqueio ao usuário, Drop com opção de envio de ICMP Unreachable para máquina de origem do tráfego, TCP-Reset para o client, TCP-Reset para o server ou para os dois lados da conexão;
- 1.38. Suportar a atribuição de agendamento as políticas com o objetivo de habilitar e desabilitar políticas em horários pré-definidos automaticamente.

CONTROLE DE APLICAÇÕES

- 1.1. Os dispositivos de proteção de rede deverão possuir a capacidade de reconhecer aplicações, independente de porta e protocolo, com as seguintes funcionalidades:
 - 1.1.1. Deve ser possível a liberação e bloqueio somente de aplicações sem a necessidade de liberação de portas e protocolos.
 - 1.1.2. Deve inspecionar o payload do pacote de dados com o objetivo de detectar através de expressões regulares assinaturas de aplicações conhecidas pelo fabricante independente de porta e protocolo. A checagem de assinaturas também deve determinar se uma aplicação está utilizando a porta default ou não, incluindo, mas não limitado a RDP na porta 80 ao invés de 389;
 - 1.1.3. Deve aplicar heurística a fim de detectar aplicações através de análise comportamental do tráfego observado, incluindo, mas não limitado a Encrypted Bittorrent e aplicações VOIP que utilizam criptografia proprietária;
 - 1.1.4. Identificar o uso de táticas evasivas, ou seja, deve ter a capacidade de visualizar e controlar as aplicações e os ataques que utilizam táticas evasivas via comunicações criptografadas, tais como Skype e ataques mediante a porta 443.
 - 1.1.5. Para tráfego criptografado SSL, deve de-criptografar pacotes a fim de possibilitar a leitura de payload para checagem de assinaturas de aplicações conhecidas pelo fabricante;
 - 1.1.6. Deve realizar decodificação de protocolos com o objetivo de detectar aplicações encapsuladas dentro do protocolo e validar se o tráfego corresponde com a especificação do protocolo, incluindo, mas não limitado a Yahoo Instant Messenger usando HTTP. A decodificação de protocolo também deve identificar funcionalidades específicas dentro de uma aplicação, incluindo, mas não limitado a compartilhamento de arquivo dentro do Webex. Além de detectar arquivos e outros conteúdos que devem ser inspecionados de acordo as regras de segurança implementadas;
 - 1.1.7. Identificar o uso de táticas evasivas via comunicações criptografadas;
 - 1.1.8. Atualizar a base de assinaturas de aplicações automaticamente;
 - 1.1.9. Reconhecer aplicações em IPV6;

- 1.1.10. Permitir limitar a banda (download/upload) usada por aplicações (traffic shaping), baseado no IP de origem;
- 1.1.11. Os dispositivos de proteção de rede devem possuir a capacidade de identificar o usuário de rede com integração ao Microsoft Active Directory, sem a necessidade de instalação de agente no Domain Controller, nem nas estações dos usuários;
- 1.1.12. Deve ser possível adicionar controle de aplicações em todas as regras de segurança do dispositivo, ou seja, não se limitando somente a possibilidade de habilitar controle de aplicações em algumas regras;
- 1.1.13. Deve suportar múltiplos métodos de identificação e classificação das aplicações, por pelo menos checagem de assinaturas, decodificação de protocolos e análise heurística;
- 1.1.14. Para manter a segurança da rede eficiente, deve suportar o controle sobre aplicações desconhecidas e não somente sobre aplicações conhecidas;
- 1.1.15. Permitir nativamente a criação de assinaturas personalizadas para reconhecimento de aplicações proprietárias na própria interface gráfica da solução, sem a necessidade de ação do fabricante, mantendo a confidencialidade das aplicações do órgão;
- 1.1.16. A criação de assinaturas personalizadas deve permitir o uso de expressões regulares, contexto (sessões ou transações), usando posição no payload dos pacotes TCP e UDP e usando decoders de pelo menos os seguintes protocolos:
 - 1.1.16.1. HTTP, FTP, SMB, SMTP, Telnet, SSH, MS-SQL, IMAP, IMAP, MS-RPC, RTSP e File body.
- 1.1.17. O fabricante deve permitir a solicitação de inclusão de aplicações na base de assinaturas de aplicações;
- 1.1.18. Deve alertar o usuário quando uma aplicação for bloqueada;
- 1.1.19. Deve possibilitar que o controle de portas seja aplicado para todas as aplicações;
- 1.1.20. Deve permitir criar filtro na tabela de regras de segurança para exibir somente:
 - 1.1.20.1. Regras que permitem passagem de tráfego baseado na porta e não por aplicação, exibindo quais aplicações estão trafegando nas mesmas, o volume em bytes trafegado por cada aplicação por, pelo menos, os últimos 30 dias e o primeiro e último registro de log de cada aplicação trafegada por esta determinada regra;
 - 1.1.20.2. Aplicações permitidas em regras de forma desnecessária, pois não há tráfego da mesma na determinada regra;
 - 1.1.20.3. Regras de segurança onde não houve passagem de tráfego nos últimos 90 dias;
- 1.1.21. Deve possibilitar a diferenciação de tráfegos Peer2Peer (Bittorrent, emule, neonet, etc.) possuindo granularidade de controle/políticas para os mesmos;
- 1.1.22. Deve possibilitar a diferenciação de aplicações Proxies (ghostsurf, freegate, etc.) possuindo granularidade de controle/políticas para os mesmos;
- 1.1.23. Deve ser possível a criação de grupos estáticos de aplicações e grupos dinâmicos de aplicações baseados em características das aplicações como:
 - 1.1.23.1. Tecnologia utilizada na aplicação (Client-Server, Browser Based, Network Protocol, etc).
 - 1.1.23.2. Nível de risco da aplicação.
 - 1.1.23.3. Categoria e subcategoria de aplicações.
 - 1.1.23.4. Aplicações que usem técnicas evasivas, utilizadas por malwares, como transferência de arquivos e/ou uso excessivo de banda, etc.
- 1.2. comum reativo não ser capaz de detectar os mesmos com a mesma velocidade que suas variações são criadas, a solução ofertada deverá possuir funcionalidades para análise de Malwares não conhecidos incluídas na própria ferramenta ou entregue com composição com outro fabricante;
- 1.3. O dispositivo de proteção deve ser capaz de enviar arquivos trafegados de forma automática para análise "In Cloud" ou local, onde o arquivo será executado e simulado em ambiente controlado;
- 1.4. Selecionar através de políticas granulares quais tipos de arquivos sofrerão esta análise incluindo, mas não limitado a: endereço IP de origem/destino, usuário/grupo do AD/LDAP, aplicação, porta, URL/categoria de URL de destino, tipo de arquivo e todas estas opções simultaneamente;
- 1.5. Deve possuir a capacidade de diferenciar arquivos analisados em pelo menos três categorias: malicioso, não malicioso e arquivos não maliciosos, mas com características indesejáveis como softwares que deixam o sistema operacional lento, que alteram parâmetros do sistema, etc.;
- 1.6. Suportar a análise de arquivos maliciosos em ambiente controlado com, no mínimo, sistema operacional Windows XP e Windows 7;

- 1.7. Deve suportar a monitoração de arquivos trafegados na internet (HTTPs, FTP, HTTP, SMTP) como também arquivos trafegados internamente entre servidores de arquivos usando SMB em todos os modos de implementação: sniffer, transparente e L3;
- 1.8. A solução deve possuir a capacidade de analisar em sand-box links (http e https) presentes no corpo de e-mails trafegados em SMTP e POP3. Deve ser gerado um relatório caso a abertura do link pela sandbox o identifique como site hospedeiro de exploits;
- 1.9. A análise de links em sandbox deve ser capaz de classificar sites falsos na categoria de phishing e atualizar a base de filtro de URL da solução;
- 1.10. Para ameaças trafegadas em protocolo SMTP e POP3, a solução deve ter a capacidade de mostrar nos relatórios o remetente, destinatário e assunto dos e-mails permitindo identificação ágil do usuário vítima do ataque;
- 1.11. O sistema de análise "In Cloud" ou local deve prover informações sobre as ações do Malware na máquina infectada, informações sobre quais aplicações são utilizadas para causar/propagar a infecção, detectar aplicações não confiáveis utilizadas pelo Malware, gerar assinaturas de Antivírus e Anti-spyware automaticamente, definir URLs não confiáveis utilizadas pelo novo Malware e prover informações sobre o usuário infectado (seu endereço ip e seu login de rede);
- 1.12. O sistema automático de análise "In Cloud" ou local deve emitir relatório com identificação de quais soluções de antivírus existentes no mercado possuem assinaturas para bloquear o malware;
- 1.13. Deve permitir exportar o resultado das análises de malwares de dia Zero em PDF e CSV a partir da própria interface de gerência;
- 1.14. Deve permitir o download dos malwares identificados a partir da própria interface de gerência;
- 1.15. Deve permitir visualizar os resultados das análises de malwares de dia zero nos diferentes sistemas operacionais suportados;
- 1.16. Deve permitir informar ao fabricante quanto a suspeita de ocorrências de falso-positivo e falso-negativo na análise de malwares de dia Zero a partir da própria interface de gerência.
- 1.17. Caso sejam necessárias licenças de sistemas operacional e softwares para execução de arquivos no ambiente controlado (sandbox), as mesmas devem ser fornecidas em sua totalidade, sem custos adicionais para a contratante;
- 1.18. Suportar a análise de arquivos executáveis, DLLs, ZIP e criptografados em SSL no ambiente controlado;
- 1.19. Suportar a análise de arquivos do pacote office (.doc, .docx, .xls, .xlsx, .ppt, .pptx), arquivos java (.jar e class), Android APKs MacOS (mach-O, DMG e PKG), Linux (ELF), RAR e 7-ZIP no ambiente de sandbox;
- 1.20. Permitir o envio de arquivos e links para análise no ambiente controlado de forma automática via API.
- 1.21. Deve permitir o envio para análise em sandbox de malwares bloqueados pelo antivírus da solução;

FILTRO DE URL

- 1.15. A plataforma de segurança deve possuir as seguintes funcionalidades de filtro de URL:
- 1.15.1. Permite especificar política por tempo, ou seja, a definição de regras para um determinado horário ou período (dia, mês, ano, dia da semana e hora);
- 1.15.2. Deve ser possível a criação de políticas por Usuários, Grupos de Usuários, Ips, Redes e Zonas de segurança.

- 1.15.3. Deverá incluir a capacidade de criação de políticas baseadas na visibilidade e controle de quem está utilizando quais URLs através da integração com serviços de diretório, autenticação via ldap, Active Directory, E-directory e base de dados local.
- 1.15.4. Permite popular todos os logs de URL com as informações dos usuários conforme descrito na integração com serviços de diretório;
- 1.15.5. Suporta a capacidade de criação de políticas baseadas no controle por URL e Categoria de URL;
- 1.15.6. Deve permitir bloquear o acesso a sites de busca (Google, Bing e Yahoo), caso a opção Safe Search esteja desabilitada. Deve ainda exibir pagina de bloqueio fornecendo instruções ao usuário de como habilitar a função;
- 1.15.7. Deve suportar base ou cache de URLs local no appliance, evitando delay de comunicação/validação das URLs;
- 1.15.8. Deve permitir classificar o nível de risco de URLs em, pelo menos, três níveis: baixo, médio e alto;
- 1.15.9. A solução deve ter a capacidade de classificar sites em mais de uma categoria, de acordo com a necessidade;
- 1.15.10. A categorização de URL deve analisar toda a URL e não somente até o nível de diretório;
- 1.15.11. Deve suportar a criação categorias de URLs customizadas;
- 1.15.12. Deve suportar a exclusão de URLs do bloqueio, por categoria;
- 1.15.13. Deve permitir a customização de página de bloqueio;
- 1.15.14. Deve proteger contra o roubo de credenciais, usuários e senhas identificadas através da integração com Active Directory submetidos em sites não corporativos. Deve ainda permitir criação de regra onde usuários do Active Directory só possam enviar informações de login para sites autorizados na solução;
- 1.15.15. Deve permitir bloquear o acesso do usuário caso o mesmo tente fazer o envio de suas credenciais em sites classificados como phishing pelo filtro de URL da solução;
- 1.15.16. Deve permitir o bloqueio e continuação (possibilitando que o usuário acesse um site potencialmente bloqueado informando o mesmo na tela de bloqueio e possibilitando a utilização de um botão "Continuar" para permitir ao usuário continuar acessando o site);
- 1.15.17. Deve suportar a inclusão nos logs do produto de informações das atividades dos usuários;
- 1.15.18. Deve salvar nos logs as informações dos seguintes campos do cabeçalho HTTP nos acessos a URLs: UserAgent, Referer, e X-Forwarded For;

IDENTIFICAÇÃO DE USUÁRIOS

- 1.16. Deve incluir a capacidade de criação de políticas baseadas na visibilidade e controle de quem está utilizando quais aplicações através da integração com serviços de diretório, autenticação via ldap, Active Directory, E-directory e base de dados local;
- 1.17. Deve permitir integração com Microsoft Active Directory para identificação de usuários e grupos permitindo granularidade de controle/políticas baseadas em usuários e grupos de usuários;
- 1.18. Deve permitir integração com Radius para identificação de usuários e grupos permitindo granularidade de controle/políticas baseadas em usuários e grupos de usuários;
- 1.19. Deve implementar a criação de políticas de segurança baseada em atributos específicos do Radius, incluindo mas não limitado a: baseado no sistema operacional do usuário remoto exigir autenticação padrão Windows e on-time password (OTP) para usuários Android;
- 1.20. Deve possuir integração com ldap para identificação de usuários e grupos permitindo granularidade de controle/políticas baseadas em Usuários e Grupos de usuários;
 - 1.20.1.1. Deve suportar o recebimento eventos de autenticação de controladoras wireless, dispositivos 802.1x e soluções NAC via syslog, para a identificação de endereços IP e usuários;
- 1.21. Deve permitir o controle, sem instalação de cliente de software, em equipamentos que solicitem saída a internet para que antes de iniciar a navegação, expanda-se um portal de autenticação residente no firewall (Captive Portal);
- 1.22. Deve suportar a autenticação via Kerberos;
- 1.23. Deve suportar autenticação via Kerberos para administradores da plataforma de segurança, captive Portal e usuário de VPN SSL;
- 1.24. Deve identificar usuários através de leitura do campo x-forwarded-for, populando nos logs do firewall o endereço IP, bem como o usuário de rede responsável pelo acesso;

1.25. Deve permitir a criação de políticas de segurança baseadas em usuários de rede com reconhecimento dos mesmos através de leitura do campo x-forwarded-for;

1.26. O firewall deve operar/suportar Security Assertion Markup Language (SAML) 2.0, com single sign-on e single logout para as funcionalidades de Captive Portal e VPN SSL (client to server), permitindo login único e interativo para fornecer acesso automático a serviços autenticados, internos e externos à organização;

1.27. Deve implementar a criação de grupos customizados de usuários no firewall, baseado em atributos do LDAP/AD;

1.28. Deve possuir suporte a identificação de múltiplos usuários conectados em um mesmo endereço IP em servidores acessados remotamente, mesmo que não sejam servidores Windows.

FILTRO DE URL

1.66. A plataforma de segurança deve possuir as seguintes funcionalidades de filtro de URL:

1.66.1. Permite especificar política por tempo, ou seja, a definição de regras para um determinado horário ou período (dia, mês, ano, dia da semana e hora);

1.66.2. Deve ser possível a criação de políticas por Usuários, Grupos de Usuários, Ips, Redes e Zonas de segurança.

1.66.3. Deverá incluir a capacidade de criação de políticas baseadas na visibilidade e controle de quem está utilizando quais URLs através da integração com serviços de diretório, autenticação via ldap, Active Directory, E-directory e base de dados local.

1.66.4. Permite popular todos os logs de URL com as informações dos usuários conforme descrito na integração com serviços de diretório;

1.66.5. Suporta a capacidade de criação de políticas baseadas no controle por URL e Categoria de URL;

1.66.6. Deve permitir bloquear o acesso a sites de busca (Google, Bing e Yahoo), caso a opção Safe Search esteja desabilitada. Deve ainda exibir pagina de bloqueio fornecendo instruções ao usuário de como habilitar a função;

1.66.7. Deve suportar base ou cache de URLs local no appliance, evitando delay de comunicação/validação das URLs;

1.66.8. Deve permitir classificar o nível de risco de URLs em, pelo menos, três níveis: baixo, médio e alto;

1.66.9. A solução deve ter a capacidade de classificar sites em mais de uma categoria, de acordo com a necessidade;

1.66.10. A categorização de URL deve analisar toda a URL e não somente até o nível de diretório;

1.66.11. Deve suportar a criação categorias de URLs customizadas;

1.66.12. Deve suportar a exclusão de URLs do bloqueio, por categoria;

1.66.13. Deve permitir a customização de página de bloqueio;

1.66.14. Deve proteger contra o roubo de credenciais, usuários e senhas identificadas através da integração com Active Directory submetidos em sites não corporativos. Deve ainda permitir criação de regra onde usuários do Active Directory só possam enviar informações de login para sites autorizados na solução;

1.66.15. Deve permitir bloquear o acesso do usuário caso o mesmo tente fazer o envio de suas credenciais em sites classificados como phishing pelo filtro de URL da solução;

1.66.16. Deve permitir o bloqueio e continuação (possibilitando que o usuário acesse um site potencialmente bloqueado informando o mesmo na tela de bloqueio e possibilitando a utilização de um botão "Continuar" para permitir ao usuário continuar acessando o site);

1.66.17. Deve suportar a inclusão nos logs do produto de informações das atividades dos usuários;

1.66.18. Deve salvar nos logs as informações dos seguintes campos do cabeçalho HTTP nos acessos a URLs: UserAgent, Referer, e X-Forwarded For;

IDENTIFICAÇÃO DE USUÁRIOS

1.67. Deve incluir a capacidade de criação de políticas baseadas na visibilidade e controle de quem está utilizando quais aplicações através da integração com serviços de diretório, autenticação via ldap, Active Directory, E-directory e base de dados local;

- 1.68. Deve permitir integração com Microsoft Active Directory para identificação de usuários e grupos permitindo granularidade de controle/políticas baseadas em usuários e grupos de usuários;
- 1.69. Deve permitir integração com Radius para identificação de usuários e grupos permitindo granularidade de controle/políticas baseadas em usuários e grupos de usuários;
- 1.70. Deve implementar a criação de políticas de segurança baseada em atributos específicos do Radius, incluindo mas não limitado a: baseado no sistema operacional do usuário remoto exigir autenticação padrão Windows e on-time password (OTP) para usuários Android;
- 1.71. Deve possuir integração com Ldap para identificação de usuários e grupos permitindo granularidade de controle/políticas baseadas em Usuários e Grupos de usuários;
- 1.71.1.1. Deve suportar o recebimento eventos de autenticação de controladoras wireless, dispositivos 802.1x e soluções NAC via syslog, para a identificação de endereços IP e usuários;
- 1.72. Deve permitir o controle, sem instalação de cliente de software, em equipamentos que solicitem saída a internet para que antes de iniciar a navegação, expanda-se um portal de autenticação residente no firewall (Captive Portal);
- 1.73. Deve suportar a autenticação via Kerberos;
- 1.74. Deve suportar autenticação via Kerberos para administradores da plataforma de segurança, captive Portal e usuário de VPN SSL;
- 1.75. Deve identificar usuários através de leitura do campo x-forwarded-for, populando nos logs do firewall o endereço IP, bem como o usuário de rede responsável pelo acesso;
- 1.76. Deve permitir a criação de políticas de segurança baseadas em usuários de rede com reconhecimento dos mesmos através de leitura do campo x-forwarded-for;
- 1.77. O firewall deve operar/suportar Security Assertion Markup Language (SAML) 2.0, com single sign-on e single logout para as funcionalidades de Captive Portal e VPN SSL (client to server), permitindo login único e interativo para fornecer acesso automático a serviços autenticados, internos e externos à organização;
- 1.78. Deve implementar a criação de grupos customizados de usuários no firewall, baseado em atributos do LDAP/AD;
- 1.79. Deve possuir suporte a identificação de múltiplos usuários conectados em um mesmo endereço IP em servidores acessados remotamente, mesmo que não sejam servidores Windows.

QOS

- 1.80. Permitir controlar aplicações e tráfego cujo consumo possa ser excessivo e ter um alto consumo de largura de banda.
- 1.81. Suportar a criação de políticas de QoS por:
- 1.81.1. Endereço de origem
- 1.81.2. Endereço de destino
- 1.81.3. Por usuário e grupo do LDAP/AD.
- 1.81.4. Por aplicações;
- 1.81.5. Por porta;
- 1.82. O QoS deve possibilitar a definição de classes por:
- 1.82.1. Banda Garantida
- 1.82.2. Banda Máxima
- 1.82.3. Fila de Prioridade.
- 1.83. Suportar priorização RealTime de protocolos de voz (VOIP) como H.323, SIP, SCCP, MGCP e aplicações como Skype.
- 1.84. Suportar marcação de pacotes Diffserv, inclusive por aplicação;

- 1.85. Deve implementar QOS (traffic-shapping), para pacotes marcados por outros ativos na rede (DSCP). A priorização e limitação do tráfego deve ser efetuada nos dois sentidos da conexão (inbound e outbound);
- 1.86. Disponibilizar estatísticas RealTime para classes de QoS.
- 1.87. Deve suportar QOS (traffic-shapping), em interface agregadas;
- 1.88. Deverá permitir o monitoramento do uso que as aplicações fazem por bytes e sessões.

FILTRO DE DADOS

- 1.89. Permite a criação de filtros para arquivos e dados pré-definidos;
- 1.90. Os arquivos devem ser identificados por extensão e assinaturas;
- 1.91. Permite identificar e opcionalmente prevenir a transferência de vários tipos de arquivos (MS Office, PDF, etc) identificados sobre aplicações (P2P, InstantMessaging, SMB, etc);
- 1.92. Suportar identificação de arquivos compactados e a aplicação de políticas sobre o conteúdo desses tipos de arquivos;
- 1.93. Permitir identificar e opcionalmente prevenir a transferência de informações sensíveis, incluindo, mas não limitado a número de cartão de crédito, possibilitando a criação de novos tipos de dados via expressão regular;
- 1.94. Permitir listar o número de aplicações suportadas para controle de dados;
- 1.95. Permitir listar o número de tipos de arquivos suportados para controle de dados;

VPN

- 1.96. Deve suportar VPN Site-to-Site e Client-To-Site;
- 1.97. Deve suportar IPSec VPN;
- 1.98. Deve suportar SSL VPN;
- 1.99. A VPN IPSEC deve suportar:
 - 1.99.1. 3DES;
 - 1.99.2. Autenticação MD5 e SHA-1;
 - 1.99.3. Diffie-Hellman Group 1, Group 2, Group 5 e Group 14;
 - 1.99.4. Algoritmo Internet Key Exchange (IKEv1 e v2);
 - 1.99.5. AES 128, 192 e 256 (Advanced Encryption Standard)
 - 1.99.6. Autenticação via certificado IKE PKI.
- 1.100. Deve possuir interoperabilidade com os seguintes fabricantes:
 - 1.100.1. Cisco;
 - 1.100.2. Checkpoint;
 - 1.100.3. Juniper;
 - 1.100.4. Palo Alto Networks;
 - 1.100.5. Fortinet;
 - 1.100.6. Sonic Wall;
- 1.101. Deve permitir habilitar, desabilitar, reiniciar e atualizar IKE gateways e túneis de VPN IPSEC a partir da interface gráfica da solução, facilitando o processo de troubleshooting;
- 1.102. A VPN SSL deve suportar:

- 1.102.1. O usuário realizar a conexão por meio de cliente instalado no sistema operacional do equipamento ou por meio de interface WEB;
- 1.102.2. A funcionalidades de VPN SSL devem ser atendidas com ou sem o uso de agente;
- 1.102.3. Atribuição de endereço IP nos clientes remotos de VPN SSL;
- 1.102.4. Deve permitir a atribuição de IPs fixos nos usuários remotos de VPN SSL;
- 1.102.5. Deve permitir a criação de rotas de acesso e faixas de endereços IP atribuídas a clientes remotos de VPN de forma customizada por usuário AD/LDAP e grupo de usuário AD/LDAP;
- 1.102.6. Deve permitir que todo o tráfego dos usuários remotos de VPN seja escoado para dentro do túnel de VPN, impedindo comunicação direta com dispositivos locais como proxies;
- 1.102.7. Atribuição de DNS nos clientes remotos de VPN;
- 1.102.8. Deve permitir que seja definido métodos de autenticação distintos por sistema operacional do dispositivo remoto de VPN (Android, IOS, Mac, Windows e Chrome OS);
- 1.102.9. A solução de VPN deve verificar se o client que está realizando a conexão é o mesmo para o qual o certificado foi emitido inicialmente. O acesso deve ser bloqueado caso o dispositivo não seja o correto;
- 1.102.10. Deve possuir lista de bloqueio para dispositivos que forem reportados com roubado ou perdido pelo usuário;
- 1.102.11. Deve haver a opção de ocultar o agente de VPN instalado no cliente remoto, tornando o mesmo invisível para o usuário;
- 1.102.12. Deve exibir mensagens de notificação customizada toda vez que um usuário remoto se conectar a VPN. Deve permitir que o usuário desabilite a exibição da mensagem nas conexões seguintes;
- 1.102.13. Deve avisar ao usuário remoto de VPN quanto a proximidade da expiração de senha LDAP. Deve permitir também a customização da mensagem com informações relevantes para o usuário;
- 1.102.14. Deve permitir criar políticas de controle de aplicações, IPS, Antivírus, Antispyware e filtro de URL para tráfego dos clientes remotos conectados na VPN SSL;
- 1.102.15. A VPN SSL deve suportar proxy arp e uso de interfaces PPPOE;
- 1.102.16. Suportar autenticação via Radius, AD/LDAP, OTP (One Time Password), certificado e base de usuários local;
- 1.102.17. Deve permitir a distribuição de certificado para o usuário de remoto através do portal de VPN de forma automatizada;
- 1.102.18. Deve possuir lista de bloqueio para dispositivos em casos quando, por exemplo, o usuário reportar que o dispositivo foi perdido ou roubado;
- 1.102.19. Permite estabelecer um túnel VPN client-to-site do cliente a plataforma de segurança, fornecendo uma solução de single-sign-on aos usuários, integrando-se com as ferramentas de Windows-logon;
- 1.102.20. Suporta leitura e verificação de CRL (certificate revocation list);
- 1.102.21. Permite a aplicação de políticas de segurança e visibilidade para as aplicações que circulam dentro dos túneis SSL;
- 1.102.22. O agente de VPN a ser instalado nos equipamentos desktop e laptops, deve ser capaz de ser distribuído de maneira automática via Microsoft SMS, Active Directory e ser descarregado diretamente desde o seu próprio portal, o qual residirá no centralizador de VPN;
- 1.102.23. O agente deverá comunicar-se com o portal para determinar as políticas de segurança do usuário,
- 1.102.24. Deve permitir que a conexão com a VPN SSL seja estabelecida das seguintes formas:
- 1.102.24.1. Antes do usuário autenticar na estação;
- 1.102.24.2. Após autenticação do usuário na estação;
- 1.102.24.3. Sob demanda do usuário;
- 1.102.25. Deve Manter uma conexão segura com o portal durante a sessão.
- 1.102.26. O agente de VPN SSL client-to-site deve ser compatível com pelo menos: Windows XP, Vista Windows 7, Windows 8, Mac OS e Chrome OS;
- 1.102.27. O portal de VPN deve enviar ao cliente remoto, a lista de gateways de VPN ativos para estabelecimento da conexão, os quais devem poder ser administrados centralmente;
- 1.102.28. Deve haver a opção de o cliente remoto escolher manualmente o gateway de VPN e de forma automática através da melhor rota entre os gateways disponíveis com base no tempo de resposta mais rápido;
- 1.102.29. Deve possuir a capacidade de identificar se a origem da conexão de VPN é externa ou interna;

GRUPO	ITE M	DESCRIÇÃO	QTD
1	1	FIREWALL TIPO 1 COM SUPORTE, GARANTIA E LICENÇAS DE	2

	<p>PROTEÇÃO COM VIGÊNCIA DE 36 MESES</p> <p>Características técnicas mínimas:</p> <p>23. Throughput de 16 Gbps com a funcionalidade de controle de aplicação habilitada para todas as assinaturas que o fabricante possuir;</p> <p>24. Throughput de 8 Gbps com as seguintes funcionalidades habilitadas simultaneamente para todas as assinaturas que a plataforma de segurança possuir devidamente ativadas e atuantes: controle de aplicação IPS, Antivírus e Antispyware. Caso o fabricante divulgue múltiplos números de desempenho para qualquer uma destas funcionalidades, somente o de menor valor será aceito;</p> <p>24.1. Os throughputs devem ser comprovados por documento de domínio público do fabricante. A ausência de tais documentos comprobatórios reservará ao órgão o direito de aferir a performance dos equipamentos em bancada, assim como atendimento de todas as funcionalidades especificadas neste edital. Caso seja comprovado o não atendimento das especificações mínimas nos testes de bancada, serão considerados inabilitados e sujeitos às sanções previstas em lei;</p> <p>24.2. Os documentos públicos devem comprovar os throughputs aferidos com tráfego HTTP ou blend de protocolos definidos pelo fabricante como tráfego real (real-world traffic blend);</p> <p>24.3. Não será aceito aceleração de pacotes na placa de rede limitando a análise somente até camada 4.</p> <p>25. Suporte a, no mínimo, 3.500.000 de conexões simultâneas;</p> <p>26. Suporte a, no mínimo, 100.000 novas conexões HTTP por segundo;</p> <p>27. Possuir fonte 120/240 AC ou DC, redundante e hot-swappable;</p> <p>28. Possuir cooler hot-swappable;</p> <p>29. Possuir disco Solid State Drive (SSD) redundante de, no mínimo, 240 GB.</p> <p>30. Possuir discos de, no mínimo, 2 TB em RAID 1 para armazenamento de logs interno ou externo a solução de firewall;</p> <p>31. No mínimo, 04 (quatro) interfaces de rede 1 Gbps em portas cobre;</p> <p>32. No mínimo, 08 (oito) interfaces de rede 1 Gbps SFP;</p> <p>33. No mínimo, 08 (oito) interfaces de rede 10 Gbps SFP+;</p> <p>34. No mínimo, 04 (quatro) interfaces de rede 40 Gbps QSFP+;</p> <p>35. 2 (duas) Gbps interfaces dedicadas para alta disponibilidade sendo pelo menos uma do tipo 40 Gbps QSFP+;</p> <p>36. 1 (uma) interface de rede 1 Gbps dedicada para gerenciamento;</p> <p>37. 1 (uma) interface do tipo console ou similar;</p> <p>38. Suporte a, no mínimo, 60 (sessenta) zonas de segurança;</p> <p>39. Estar licenciada para ou suportar sem o uso de licença, 10.000 (dez mil) clientes de VPN SSL simultâneos;</p> <p>40. Estar licenciada para ou suportar sem o uso de licença, 3.000 (três mil) túneis de VPN IPSEC simultâneos;</p> <p>41. Deve suportar, no mínimo, 10 sistemas virtuais lógicos (Contextos) no firewall Físico;</p> <p>42. Os contextos virtuais devem suportar as funcionalidades nativas do gateway de proteção incluindo: Firewall, IPS, Antivírus, Anti-Spyware, Filtro de URL, Filtro de Dados VPN, Controle de Aplicações, QOS, NAT e Identificação de usuários;</p> <p>43. Na data da proposta, nenhum dos modelos ofertados poderão estar listados no site do fabricante em listas de end-of-life e end-of-sale.</p>	
--	--	--

		<p>44. Conforme disposto no item I do artigo 15 da lei 8.666, de 21 de junho de 1993 (I - Atender ao princípio de padronização, que imponha compatibilidade técnica e de desempenho, observadas, quando for o caso, as condições de manutenção, assistência técnica e garantia oferecidas), estes equipamentos, por questões de compatibilidade, gerência, suporte e garantia, devem ser do mesmo fabricante dos equipamentos deste grupo/lote;</p>	
2		<p>FIREWALL TIPO 2 COM SUPORTE, GARANTIA E LICENÇAS DE PROTEÇÃO COM VIGÊNCIA DE 36 MESES</p> <p>Características técnicas mínimas:</p> <p>22. Throughput de 8 Gbps com a funcionalidade de controle de aplicação habilitada para todas as assinaturas que o fabricante possuir;</p> <p>23. Throughput de 4 Gbps com as seguintes funcionalidades habilitadas simultaneamente para todas as assinaturas que a plataforma de segurança possuir devidamente ativadas e atuantes: controle de aplicação IPS, Antivírus e Antispyware. Caso o fabricante divulgue múltiplos números de desempenho para qualquer uma destas funcionalidades, somente o de menor valor será aceito;</p> <p>23.1. Os throughputs devem ser comprovados por documento de domínio público do fabricante. A ausência de tais documentos comprobatórios reservará ao órgão o direito de aferir a performance dos equipamentos em bancada, assim como atendimento de todas as funcionalidades especificadas neste edital. Caso seja comprovado o não atendimento das especificações mínimas nos testes de bancada, serão considerados inabilitados e sujeitos as sanções previstas em lei;</p> <p>23.2. Os documentos públicos devem comprovar os throughputs aferidos com tráfego HTTP ou blend de protocolos definidos pelo fabricante como tráfego real (real-word traffic blend ou similar);</p> <p>23.3. Não será aceito aceleração de pacotes na placa de rede limitando a análise somente até camada 4.</p> <p>24. Suporte a, no mínimo, 2.000.000 conexões simultâneas;</p> <p>25. Suporte a, no mínimo, 50.000 novas conexões por segundo;</p> <p>26. Possuir fonte 120/240 AC ou DC, redundante e hot-swappable;</p> <p>27. Possuir cooler hot-swappable;</p> <p>28. Possuir disco Solid State Drive (SSD) de, no mínimo, 240 GB;</p> <p>29. 12 (doze) interfaces de rede 1 Gbps 10/100/1000 base-TX ou SFP;</p> <p>30. 8 (oito) interfaces de rede 10 Gbps SFP+;</p> <p>31. 4 (quatro) interfaces de rede 40 Gbps QSFP+;</p> <p>32. 2 (duas) Gbps interfaces dedicadas para alta disponibilidade sem pelo menos uma do tipo 10Gbps SFP+;</p> <p>33. 1 (uma) interface de rede 1 Gbps dedicada para gerenciamento;</p> <p>34. 1 (uma) interface do tipo console ou similar;</p> <p>35. Suporte a, no mínimo, 30 (trinta) zonas de segurança;</p> <p>36. Estar licenciada para ou suportar sem o uso de licença, 2.000 (dois mil) clientes de VPN SSL simultâneos;</p> <p>37. Estar licenciada para ou suportar sem o uso de licença, 2.000 túneis de VPN IPSEC simultâneos;</p> <p>38. Deve suportar, no mínimo, 1 sistema virtual lógico (Contexto) no firewall Físico;</p> <p>39. Deve permitir expansão com aquisição futura de licenças a até 6 sistemas virtuais lógicos (Contextos) no firewall Físico;</p> <p>40. Os contextos virtuais devem suportar as funcionalidades nativas do gateway de proteção incluindo: Firewall, IPS, Antivírus, Anti-Spyware, Filtro de</p>	2

		<p>URL, Filtro de Dados, VPN, Controle de Aplicações, QOS, NAT e Identificação de usuários;</p> <p>41. Na data da proposta, nenhum dos modelos ofertados poderão estar listados no site do fabricante em listas de end-of-life e end-of-sale.</p> <p>42. Conforme disposto no item I do artigo 15 da lei 8.666, de 21 de junho de 1993 (I - Atender ao princípio de padronização, que imponha compatibilidade técnica e de desempenho, observadas, quando for o caso, as condições de manutenção, assistência técnica e garantia oferecidas), estes equipamentos, por questões de compatibilidade, gerência, suporte e garantia, devem ser do mesmo fabricante dos equipamentos deste grupo/lote;</p>	
3		<p>SERVIÇOS DE INSTALAÇÃO DE FIREWALL</p> <p>A contratada deverá prestar serviços de instalação e configuração da solução, que compreendem, entre outros, os seguintes procedimentos:</p> <p>13) Reunião de alinhamento para criação do escopo do projeto previamente a instalação;</p> <p>14) Instalação física de todos os equipamentos (hardware) e licenças (softwares) adquiridos no local determinado pela equipe responsável pelo projeto por parte da contratante (DTI). Quando aplicável, considerar instalação em modo Alta Disponibilidade (ativo/passivo);</p> <p>15) Análise da topologia e arquitetura da rede, considerando todos equipamentos já existentes e instalados;</p> <p>16) Análise do acesso à Internet, sites remotos, serviços de rede oferecidos aos funcionários e aos usuários externos;</p> <p>17) Migração das regras de firewall existentes e aplicáveis à solução ofertada, considerando a adequação às políticas de aplicações em camada 7;</p> <p>18) Análise do posicionamento de qualquer outro equipamento ou sistema relevante na segurança de qualquer perímetro protegido pela solução;</p> <p>19) Configuração do sistema de firewall, VPN, IPS, Filtro URL, Anti-vírus e Anti-malware de acordo com as exigências levantadas;</p> <p>20) Toda configuração de sistema (políticas gerais, objetos, itens de administração) deverá ser realizada de acordo com as melhores práticas recomendadas pelo fabricante da solução ofertada, além de compreender as principais disciplinas de funcionamento seguro dos frameworks CIS e NIST Framework. O fabricante da solução ofertada deverá disponibilizar ferramenta gratuita (ou incluir nos custos de serviço) para acompanhamento da evolução da parametrização de proteção dos firewalls a fim de garantir a melhor eficiência da solução durante o período de vigência das licenças;</p> <p>21) Configuração do sistema de gerenciamento centralizado considerando adição dos novos appliances;</p> <p>22) Repasse de informação das configurações realizadas no formato hands-on de 4 horas para o DTI após validação da migração;</p> <p>23) Deve haver geração de relatório com as configurações efetuadas e as decisões tomadas em formato legível e tecnicamente fundamentado;</p> <p>24) Os serviços de instalação e configuração deverá ser realizado por técnico certificado oficialmente pelo fabricante da solução ofertada ou pelo próprio fabricante;</p>	4
4		<p>TREINAMENTO OFICIAL DE FIREWALL DE PRÓXIMA GERAÇÃO</p> <p>4.8. A contratada deverá disponibilizar vouchers para treinamento oficial do fabricante;</p> <p>4.9. O treinamento deve ser ministrado abrangendo teoria e prática de implantação, configuração, administração e solução de problemas no ambiente deste órgão, bem como assuntos teóricos relacionados;</p>	4

		<p>4.10. Deve conter no mínimo a seguinte ementa:</p> <ul style="list-style-type: none"> • Arquitetura e Plataforma; • Configuração Inicial; • Configuração de Interface; • Políticas de Segurança e NAT; • Identificação de Aplicações; • Identificação de Conteúdo Básico; • Filtro URL; • De-criptografia; • Sandboxing de ameaças avançadas; • Identificação de Usuário; • VPN; • Monitoramento e Relatórios; • Alta Disponibilidade (redundância); • Demais assuntos pertinentes a solução; <p>4.11. Deve ser emitido um único certificado de conclusão cobrindo todo o curso, sendo um para cada participante;</p> <p>4.12. O treinamento deverá ser ministrado pelo próprio fabricante ou por um parceiro nacional, capacitado, certificado e autorizado pelo fabricante a ministrar treinamentos oficiais.</p> <p>4.13. O treinamento deve estar disponível preferencialmente na modalidade presencial na sede da Contratante;</p> <p>4.14. O fabricante ou autorizada fornecerá os materiais didáticos para ministrar o curso.</p>	
--	--	---	--

7.1. Requisitos de Negócio

- Aquisição de solução de firewall de próxima geração, provendo visibilidade detalhada e controle do tráfego e proteção da rede;
- Adequação às legislações vigentes, tais como LGPD – Lei Geral de Proteção de Dados (Lei nº 13.709/2018) e Marco Civil da Internet Lei nº 12.965/2014);
- Manter a integridade dos dados e das informações sensíveis dos sistemas da universidade;
- Melhorar o nível de qualidade de serviço das aplicações internas da universidade;
- Melhorar substancialmente o nível de segurança da informação da universidade;
- Permitir ao time de segurança da informação ter visibilidade das aplicações e os riscos que elas trazem para o ambiente.

7.2. Requisitos de Capacitação

Os técnicos da envolvidos por parte da Contratante deverão realizar treinamento oficial do fabricante conforme especificado no item 4 deste termo de referência.

7.3. Requisitos Legais

Atender, quando aplicável, as diretrizes da Portaria nº 170 de abril de 2012 do Instituto Nacional de Metrologia, Qualidade e Tecnologia - INMETRO.

7.4. Requisitos de Manutenção

- 1-Todos os itens deste processo devem possuir garantia do fabricante ou autorizada no Brasil com validade mínima de 36 (trinta e seis) meses;
- 2-Durante o prazo de garantia, deve ser possível realizar a atualização de sistema operacional dos equipamentos para obter novas funcionalidades e correção de bugs;
- 3-Durante o prazo de garantia, deve ser possível realizar a atualização das assinaturas de proteção da solução;
- 4-Em caso de defeitos de fabricação, a garantia deve incluir envio de peças ou equipamentos de reposição nos locais especificados neste edital, obedecendo a modalidade NBD (Next Business Day);
- 5-Os chamados poderão ser abertos diretamente com a contratada ou autorizada oficial do fabricante no Brasil através de ligação telefônica gratuita (0800) no idioma português, website e e-mail durante a vigência da garantia. O suporte deverá ser na modalidade de 24x7 (24 horas por dia, 7 dias por semana);

6-O suporte deverá ter no mínimo o seguinte tempo de resposta para os níveis de severidade abaixo:

a-Crítico: significa que o produto ficou inoperante ou ocorreu falha de grande impacto e o sistema está parado. Para este nível de severidade o atendimento deve ser imediato e com tempo de resposta de até 1 (uma) hora para resolução total ou encontro de solução temporária de contorno. Neste caso o chamado deverá ser aberto via telefone (0800);

b-Alta: impacto moderado no sistema, travamento, ou parada de ambiente parcial. Para este nível de severidade o tempo de resposta deve ser de até 2 (duas) horas, em horário comercial, para resolução total ou encontro de solução temporária de contorno;

c-Média: Redução de performance do equipamento ou aplicação de solução temporária de contorno bem-sucedida. Para este nível de severidade o tempo de resposta deve ser de até 4 (quatro) horas, em horário comercial, para resolução total ou encontro de solução temporária de contorno;

d-Baixa: dúvidas de configuração ou anomalia de baixo impacto. Para este nível de severidade o tempo de resposta deve ser de até 8 (oito) horas, em horário comercial.

7.5. Requisitos Temporais

O prazo de entrega de produtos deverá ocorrer em até no máximo 90 (noventa) dias corridos a partir da data de assinatura do contrato.

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

A implantação completa da solução deve ser concluída em até 30 (trinta) dias corridos após a entrega do objeto.

7.6. Requisitos de Segurança

A Contratada deverá submeter-se aos procedimentos de segurança existentes ou que possam ser criados durante a vigência do contrato. Os procedimentos deverão ser observados sempre que for necessária a presença nas dependências da Contratante.

7.7. Requisitos Sociais, Ambientais e Culturais

A documentação e os manuais da solução deverão ser apresentados no idioma Português (Brasil), eventualmente poderão ser apresentados em inglês.

Todos os contatos para gerenciamento de chamados e suporte técnico deverão ser realizados em Português (Brasil).

7.8. Requisitos de Arquitetura Tecnológica

Conforme disposto no item I do artigo 15 da lei 8.666, de 21 de junho de 1993 (I - Atender ao princípio de padronização, que imponha compatibilidade técnica e de desempenho, observadas, quando for o caso, as condições de manutenção, assistência técnica e garantia oferecidas), os equipamentos e softwares, por questões de compatibilidade, gerência, suporte e garantia, devem ser do mesmo fabricante.

7.9. Requisitos de Projeto e de Implementação

Antes de iniciar a implantação da solução a Contratada deve apresentar um projeto e cronograma para instalação da solução. O projeto e o cronograma devem ser aprovados pela Contratante.

7.10. Requisitos de Implantação

A implantação deverá ser realizada por profissionais especializados da contratada, que possuam certificação do fabricante da solução adquirida que lhes confira as competências necessárias para a realização dos respectivos serviços de implantação, ou pelo próprio fabricante.

Deverá abranger a configuração de quaisquer funcionalidades suportadas pelos equipamentos. Estas informações serão documentadas no termo de abertura do projeto a ser elaborado pela CONTRATADA após alinhamento do escopo de trabalho definido entre CONTRATADA e CONTRATANTE.

7.11. Requisitos de Garantia

Toda solução deste termo de referência deverá considerar período de garantia por um prazo de até 36 meses, para hardware e licenças de software.

Os serviços de garantia deverão ser prestados pelo próprio fabricante da solução ofertada ou por empresa autorizada oficialmente pelo fabricante a prestar este tipo de serviço no Brasil.

Como comprovação de autorização, deverá ser apresentado documento com informações da empresa prestadora da assistência técnica com sua identificação, endereço, CNPJ, responsável técnico e região de atuação.

7.12. Requisitos de Experiência Profissional

Os serviços de instalação e configuração dos itens relacionados neste termo de referência deverão ser executados por técnicos capacitados com certificação oficial do fabricante.

A contratada deverá possuir, pelo menos, dois técnicos certificados oficialmente pelo fabricante da solução.

7.14. Requisitos de Metodologia de Trabalho

A metodologia de trabalho relacionado aos serviços prestados deverá observar os preceitos do ITIL V4.

7.15. Requisitos de Segurança da Informação

1-A solução contratada deverá respeitar a adequação à legislação vigente, tais como LGPD – Lei Geral de Proteção de Dados (Lei nº 13.709/2018) e Marco Civil da Internet Lei nº 12.965/2014).

2-A solução contratada deverá observar a Norma Brasileira ABNT NBR ISO/IEC 27002.

3-A Contratada deverá manter a integridade da rede de dados e das informações da universidade.

4-A Contratada deverá respeitar a Política de Segurança da Informação e Comunicações (POSIC) da Universidade Federal de Santa Maria bem como demais políticas e normas que poderão ser instituídas durante a vigência do contrato.

5-A Contratada deverá guardar sigilo de todos os dados e informações a que tiver acesso, não podendo cedê-los a terceiros ou divulgá-los de qualquer forma.

6-Qualquer unidade de armazenamento, tais como SSDs, HDDs e memórias, utilizadas deverão permanecer em posse de Contratante mesmo após o uso, após dano ou após o término do contrato. Caso seja necessária a remoção de alguma unidade de armazenamento, esta ação deve ser realizada no prédio do CPD/UFSM e imediatamente entregue a Contratante.

8 – RESPONSABILIDADES

8.1. Deveres e responsabilidades da CONTRATANTE

a-Nomear Gestor e Fiscais Técnico, Administrativo e Requisitante do contrato para acompanhar e fiscalizar a execução dos contratos;

b-Encaminhar formalmente a demanda por meio de Ordem de Serviço ou de Fornecimento de Bens, de acordo com os critérios estabelecidos no Termo de Referência ou Projeto Básico;

c-Receber o objeto fornecido pela contratada que esteja em conformidade com a proposta aceita, conforme inspeções realizadas;

d-Aplicar à contratada as sanções administrativas regulamentares e contratuais cabíveis, comunicando ao órgão gerenciador da Ata de Registro de Preços, quando aplicável;

e-Liquidar o empenho e efetuar o pagamento à contratada, dentro dos prazos preestabelecidos em contrato;

f-Comunicar à contratada todas e quaisquer ocorrências relacionadas com o fornecimento da solução de TIC;

g-Definir produtividade ou capacidade mínima de fornecimento da solução de TIC por parte da contratada, com base em pesquisas de mercado, quando aplicável; e

h-Prever que os direitos de propriedade intelectual e direitos autorais da solução de TIC sobre os diversos artefatos e produtos produzidos em decorrência da relação contratual, incluindo a documentação, o código-fonte de aplicações, os modelos de dados e as bases de dados, pertençam à Administração.

8.2. Deveres e responsabilidades da CONTRATADA

a-Indicar formalmente preposto apto a representá-lo junto à contratante, que deverá responder pela fiel

execução do contrato;

b-Atender prontamente quaisquer orientações e exigências da Equipe de Fiscalização do Contrato, inerentes à execução do objeto contratual;

c-Efetuar a entrega do objeto em perfeitas condições, conforme especificações, prazo e local constantes no Edital e seus anexos, acompanhado da respectiva nota fiscal, na qual constarão as indicações referentes a: marca, fabricante, modelo, procedência e prazo de garantia ou validade;

d-Fornecer equipamentos novos e realizar os serviços de instalação com a qualidade adequada;

e-Reparar quaisquer danos diretamente causados à contratante ou a terceiros por culpa ou dolo de seus representantes legais, prepostos ou empregados, em decorrência da relação contratual, não excluindo ou reduzindo a responsabilidade da fiscalização ou o acompanhamento da execução dos serviços pela contratante;

f-Propiciar todos os meios necessários à fiscalização do contrato pela contratante, cujo representante terá poderes para sustar o fornecimento, total ou parcial, em qualquer tempo, sempre que considerar a medida necessária;

g-Manter, durante toda a execução do contrato, as mesmas condições da habilitação;

h-Quando especificada, manter, durante a execução do contrato, equipe técnica composta por profissionais devidamente habilitados, treinados e qualificados para fornecimento da solução de TIC;

i-Quando especificado, manter a produtividade ou a capacidade mínima de fornecimento da solução de TIC durante a execução do contrato; e

j-Ceder os direitos de propriedade intelectual e direitos autorais da solução de TIC sobre os diversos artefatos e produtos produzidos em decorrência da relação contratual, incluindo a documentação, os modelos de dados e as bases de dados à Administração.

9 – MODELO DE EXECUÇÃO DO CONTRATO

9.1. Rotinas de Execução

a-Realização de reunião inicial,

b-Apresentação de projeto e cronograma de instalação pela Contratada;

c-Aprovação do projeto e cronograma de instalação pela Contratante;

d-Entrega do(s) equipamento(s) respeitando o disposto no item 4.5 deste Termo de Referência;

e-Verificação do(s) equipamento(s) recebidos com base nos requisitos deste Termo de Referência;

f-Configuração e instalação do(s) equipamento(s) conforme o projeto;

g-Ativação das licenças cuja duração deverá ser contada a partir do momento de ativação;

h-Teste em ambiente de produção da UFSM dos requisitos e funcionalidades contidos neste Termo de Referência.

i-Validação e aceite da UFSM.

A reunião inicial poderá ser realizada de forma remota ou presencial.

O(s) equipamento(s) deverão ser entregues e instalados no Centro de Processamento de Dados da Universidade de Santa Maria (Avenida Roraima, 1000, Prédio 48 - Camobi, RS, 97105-900).

O teste em ambiente de produção deve levar em conta um período normal de tráfego da UFSM, não podendo ser realizado durante férias ou outro período de baixa demanda. Se necessário, poderá ser realizado um teste de validação da capacidade máxima de tráfego utilizando uma ferramenta própria para este fim. Após 30 dias úteis de pleno funcionamento da solução será dado o aceite da UFSM para o serviço de instalação e configuração do(s) equipamento(s).

9.2. Quantidade mínima de bens ou serviços para comparação e controle

Não se aplica.

9.3. Mecanismos formais de comunicação

As questões administrativas formais ocorridas durante a execução do contrato serão tratadas através de ofício. Questões administrativas ou operacionais cotidianas durante a execução do contrato poderão ser tratadas através de mensagem eletrônica (e-mail), telefone ou aplicativo de mensagens.

9.4. Manutenção de Sigilo e Normas de Segurança

A Contratada deverá manter sigilo absoluto sobre quaisquer dados e informações contidos em quaisquer documentos e mídias, incluindo os equipamentos e seus meios de armazenamento, de que venha a ter conhecimento durante a execução dos serviços, não podendo, sob qualquer pretexto, divulgar, reproduzir ou utilizar, sob pena de lei, independentemente da classificação de sigilo conferida pelo Contratante a tais documentos.

O **Termo de Compromisso**, contendo declaração de manutenção de sigilo e respeito às normas de segurança vigentes na entidade, a ser assinado pelo representante legal da Contratada, encontra-se no ANEXO II.

10 – MODELO DE GESTÃO DO CONTRATO

10.1. Critérios de Aceitação

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

O aceite do bem somente será dado após comprovação da entrega e o efetivo cumprimento de todas as exigências presentes nas especificações técnicas deste termo de referência.

Será consultado diretamente no site do fabricante do equipamento manuais e toda documentação pública disponível para comprovação do pleno atendimento aos requisitos deste edital. Em caso de dúvidas ou divergência na comprovação da especificação técnica, este órgão poderá solicitar amostra do equipamento ofertado, sem ônus ao processo, para comprovação técnica de funcionalidades. Esta amostra deverá ocorrer em até 15 (quinze) dias úteis após a solicitação deste órgão. Para a amostra, a empresa deverá apresentar o mesmo modelo do equipamento ofertado no certame, com técnicos certificados na solução para configuração e comprovação dos itens pendentes, nas dependências deste órgão.

10.2. Procedimentos de Teste e Inspeção

Na fase de aprovação da proposta técnica comercial durante a fase licitatória:

1- Será utilizado um método comparativo entre os requisitos da solução e os prospectos do fabricante.

Na fase de implantação da solução:

2- Após instalação e configuração da solução os itens constantes no Termo de Referência serão testados na solução a fim de verificar se as especificações são atendidas.

3. O aceite do bem somente será dado após comprovação da entrega e o efetivo cumprimento de todas as exigências da presente nas especificações técnicas deste termo de referência.

10.3. Níveis Mínimos de Serviço Exigidos

Os chamados poderão ser abertos diretamente com a contratada ou autorizada oficial do fabricante no Brasil através de ligação telefônica gratuita (0800) no idioma Português (Brasil), website e e-mail durante a vigência da garantia. O suporte deverá ser na modalidade de 24x7 (24 horas por dia, 7 dias por semana).

O suporte deverá ter no mínimo o seguinte tempo de resposta para os níveis de severidade abaixo:

Crítico: significa que o produto ficou inoperante ou ocorreu falha de grande impacto e o sistema está parado. Para este nível de severidade o atendimento deve ser imediato e com tempo de resposta de até 1 (uma) hora para resolução total ou encontro de solução temporária de contorno. Neste caso o chamado deverá ser aberto via telefone (0800);

Alta: impacto moderado no sistema, travamento, ou parada de ambiente parcial. Para este nível de severidade o tempo de resposta deve ser de até 2 (duas) horas, em horário comercial, para resolução total ou encontro de solução temporária de contorno;

Média: Redução de performance do equipamento ou aplicação de solução temporária de contorno bem-

sucedida. Para este nível de severidade o tempo de resposta deve ser de até 4 (quatro) horas, em horário comercial, para resolução total ou encontro de solução temporária de contorno;

Baixa: dúvidas de configuração ou anomalia de baixo impacto. Para este nível de severidade o tempo de resposta deve ser de até 8 (oito) horas, em horário comercial.

