PREGÃO ELETRÔNICO Nº 007/2020 – IRP **nº 003/2020**

O presente certame será regido pela Lei nº. 10.520, de 17 de julho de 2002, Decreto 10.024 de 20 de setembro de 2019, Decreto 7.892 de 23 de janeiro de 2013, Lei Complementar 123/06 e subsidiariamente pela Lei nº. 8.666/93, de 21 de junho de 1993.

Tipo:	**Menor Preço (01 ITEM)**
Objeto:	**Registro de preço para eventual aquisição de material de material permanente (fornecimento de solução de proteção de rede de dados com características de Firewall de próxima geração (Next Generation Firewall – NGFW), com suporte de 60 meses, solução de gerenciamento centralizado, serviços de instalação, configuração e treinamento de pessoal), conforme condições, quantidades, exigências e estimativas encaminhadas pelo Centro de Tecnologia da Informação e Comunicação-CTIC da Universidade Federal do Amazonas, e estabelecidas neste Edital e seus anexos.**
Processo:	**23105.009252/2020-83**
Órgão Gerenciador:	154039-UFAM
Órgão Participante:	**-**
Sessão pública para recebimento das propostas de preços e dos documentos de habilitação:	
Data:	**09/07/2020**
Hora:	**10h (horário de Brasília)**
Local:	WWW.COMPRASNET.GOV.BR
Edital disponível a partir de:	**29/06/2020**
Dias, horários e local para leitura ou obtenção deste Edital:	
Dias:	Segunda a Sexta-feira (dias úteis e de expediente)
Horários:	De 08:00h às 17h00min
Local:	**Sala de Licitações / UFAM -** Av. Rodrigo Otávio n.º 6.200, Campus Universitário Senador Arthur Virgílio Filho, Setor Sul, Bloco "J", Setor de Licitações, Coroado – Manaus-AM, **CEP 69.077-000.** **Telefone: (92) 3305-1181 ramal 4041 e (92) 99318-2191.**
Aviso de licitação divulgado no site: www.comprasnet.gov.br Edital disponível (gratuitamente) no site: www.comprasnet.gov.br	

Angélica Aguiar Costa Lima
PREGOEIRO (A)

PREGÃO ELETRÔNICO

FUNDAÇÃO UNIVERSIDADE DO AMAZONAS

PREGÃO ELETRÔNICO Nº 007/2020

(Processo Administrativo n° **23105.009252/2020-83**)

Torna-se público, para conhecimento dos interessados, que a FUNDAÇÃO UNIVERSIDADE DO AMAZONAS, C.N.P.J. n.º 04.378.626/0001-97, com sede na Av. Rodrigo Otávio n.º 6.200, Campus Universitário Senador Arthur Virgílio Filho, Coroado – Manaus-AM, por meio deste pregoeiro, designado pela **Portaria – PROADM nº 114/2019 de 19/09/2019**, publicado no DOU em **20/09/2019**, realizará licitação, para **registro de preços**, na modalidade **PREGÃO**, na forma **ELETRÔNICA**, com **critério de julgamento menor preço por item**, nos termos da Lei nº 10.520, de 17 de julho de 2002, do Decreto nº 10.024, de 20 de setembro de 2019, do Decreto nº 7.746, de 05 de junho de 2012, do Decreto nº 7892, de 23 de janeiro e 2013, da Instrução Normativa SLTI/MP nº 01, de 19 de janeiro de 2010, da Instrução Normativa SEGES/MP nº 03, de 26 de abril, de 2018, da Lei Complementar n° 123, de 14 de dezembro de 2006, da Lei nº 11.488, de 15 de junho de 2007, do Decreto n° 8.538, de 06 de outubro de 2015, aplicando-se, subsidiariamente, a Lei nº 8.666, de 21 de junho de 1993, e as exigências estabelecidas neste Edital.

Data da sessão: **09/07/2020**
Horário: **10h (horário de Brasília)**
Local: Portal de Compras do Governo Federal – www.comprasgovernamentais.gov.br

1. DO OBJETO

1.1. O objeto da presente licitação é a escolha da proposta mais vantajosa para a aquisição de **aquisição de material de material permanente (fornecimento de solução de proteção de rede de dados com características de Firewall de próxima geração (Next Generation Firewall – NGFW), com suporte de 60 meses, solução de gerenciamento centralizado, serviços de instalação, configuração e treinamento de pessoal), conforme condições, quantidades, exigências e estimativas encaminhadas pelo Centro de Tecnologia da Informação e Comunicação-CTIC da Universidade Federal do Amazonas,** conforme condições, quantidades e exigências estabelecidas neste Edital e seus anexos.

1.2. A licitação será realizada em único item.

1.3. O critério de julgamento adotado será o menor preço do item, observadas as exigências contidas neste Edital e seus Anexos quanto às especificações do objeto.

2. DO REGISTRO DE PREÇOS

2.1. As regras referentes aos órgãos gerenciador e participantes, bem como a eventuais adesões são as que constam da minuta de Ata de Registro de Preços

3. DO CREDENCIAMENTO

3.1. O Credenciamento é o nível básico do registro cadastral no SICAF, que permite a participação dos interessados na modalidade licitatória Pregão, em sua forma eletrônica.

3.2. O cadastro no SICAF deverá ser feito no Portal de Compras do Governo Federal, no sítio www.comprasgovernamentais.gov.br, por meio de certificado digital conferido pela Infraestrutura de Chaves Públicas Brasileira – ICP - Brasil.

3.3. O credenciamento junto ao provedor do sistema implica a responsabilidade do licitante ou de seu representante legal e a presunção de sua capacidade técnica para realização das transações inerentes a este Pregão.

3.4. O licitante responsabiliza-se exclusiva e formalmente pelas transações efetuadas em seu nome, assume como firmes e verdadeiras suas propostas e seus lances, inclusive os atos praticados diretamente ou por seu representante, excluída a responsabilidade do provedor do sistema ou do órgão ou entidade promotora da licitação por eventuais danos decorrentes de uso indevido das credenciais de acesso, ainda que por terceiros.

3.5. É de responsabilidade do cadastrado conferir a exatidão dos seus dados cadastrais no SICAF e mantê-los atualizados junto aos órgãos responsáveis pela informação, devendo proceder, imediatamente, à correção ou à alteração dos registros tão logo identifique incorreção ou aqueles se tornem desatualizados.

3.5.1. A não observância do disposto no subitem anterior poderá ensejar desclassificação no momento da habilitação

4. DA PARTICIPAÇÃO NO PREGÃO.

4.1. Poderão participar deste Pregão interessados cujo ramo de atividade seja compatível com o objeto desta licitação, e que estejam com Credenciamento regular no Sistema de Cadastramento Unificado de Fornecedores – SICAF, conforme disposto no art. 9º da IN SEGES/MP nº 3, de 2018.

4.1.1. Os licitantes deverão utilizar o certificado digital para acesso ao Sistema.

4.2. Será concedido tratamento favorecido para as microempresas e empresas de pequeno porte, para as sociedades cooperativas mencionadas no artigo 34 da Lei nº 11.488, de 2007, para o agricultor familiar, o produtor rural pessoa física e para o microempreendedor individual - MEI, nos limites previstos da Lei Complementar nº 123, de 2006.

4.3. Não poderão participar desta licitação os interessados:

4.3.1. proibidos de participar de licitações e celebrar contratos administrativos, na forma da legislação vigente;

4.3.2. que não atendam às condições deste Edital e seu(s) anexo(s);

4.3.3. estrangeiros que não tenham representação legal no Brasil com poderes expressos para receber citação e responder administrativa ou judicialmente;

4.3.4. que se enquadrem nas vedações previstas no artigo 9º da Lei nº 8.666, de 1993;

4.3.5. que estejam sob falência, concurso de credores, concordata ou em processo de dissolução ou liquidação;

4.3.6. pessoas jurídicas que possuam em seus quadros societários servidores da FUA ou administradores que mantenham vínculo familiar com detentor de cargo em comissão ou função de confiança, atuante na área responsável pela demanda ou contratação, ou de autoridade a ele hierarquicamente superior;

4.3.7. entidades empresariais que estejam reunidas em consórcio, uma vez que a aquisição não se configura de grande vulto e/ou de alta complexidade técnica;

4.3.8. Organizações da Sociedade Civil de Interesse Público - OSCIP, atuando nessa condição (Acórdão nº 746/2014-TCU-Plenário).

4.4. Como condição para participação no Pregão, a licitante assinalará “sim” ou “não” em campo próprio do sistema eletrônico, relativo às seguintes declarações:

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

4.4.1.1. nos itens exclusivos para participação de microempresas e empresas de pequeno porte, a assinalação do campo “não” impedirá o prosseguimento no certame;

4.4.1.2. nos itens em que a participação não for exclusiva para microempresas e empresas de pequeno porte, a assinalação do campo “não” apenas produzirá o efeito de o licitante não ter direito ao tratamento favorecido previsto na Lei Complementar nº 123, de 2006, mesmo que microempresa, empresa de pequeno porte.

4.4.2. que está ciente e concorda com as condições contidas no Edital e seus anexos;

4.4.3. que cumpre os requisitos para a habilitação definidos no Edital e que a proposta apresentada está em conformidade com as exigências editalícias;

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

4.4.5. 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 7°, XXXIII, da Constituição;

4.4.6. que a proposta foi elaborada de forma independente, nos termos da Instrução Normativa SLTI/MP nº 2, de 16 de setembro de 2009.

4.4.7. 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;

4.4.8. 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.

4.4.9. que cumpre os requisitos do Decreto n. 7.174, de 2010, estando apto a usufruir dos critérios de preferência.

4.5. Ainda como condição de participação, para fins de comprovação do subitem **4.3.6**, o licitante deverá enviar a declaração de que não possuem em seus quadros societários servidores da FUA ou administradores que mantenham vínculo familiar com detentor de cargo em comissão ou função de confiança, atuante na área responsável pela demanda ou contratação, ou de autoridade a ele hierarquicamente superior, em cumprimento ao Acórdão Nº 409/2015 – TCU – Plenário, em conformidade com o modelo disponível Anexo II deste Edital.

4.6. A declaração falsa relativa ao cumprimento de qualquer condição sujeitará o licitante às sanções previstas em lei e neste Edital.

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 **e a declaração que trata o subitem 4.5,** 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.

6. DO PREENCHIMENTO DA PROPOSTA

6.1. O licitante deverá enviar sua proposta mediante o preenchimento, no sistema eletrônico, dos seguintes campos:

6.1.1. Valor unitário e total do item;

6.1.2. Marca;

6.1.3. Fabricante;

6.1.4. Descrição detalhada do objeto, contendo as informações similares à especificação do Termo de Referência: indicando, no que for aplicável, o modelo, prazo de validade ou de garantia, número do registro ou inscrição do bem no órgão competente, quando for o caso;

6.2. Todas as especificações do objeto contidas na proposta vinculam a Contratada.

6.3. Nos valores propostos estarão inclusos todos os custos operacionais, encargos previdenciários, trabalhistas, tributários, comerciais e quaisquer outros que incidam direta ou indiretamente no fornecimento dos bens.

6.4. Os preços ofertados, tanto na proposta inicial, quanto na etapa de lances, serão de exclusiva responsabilidade do licitante, não lhe assistindo o direito de pleitear qualquer alteração, sob alegação de erro, omissão ou qualquer outro pretexto.

6.5. O prazo de validade da proposta não será inferior a 60 (sessenta) dias**,** a contar da data de sua apresentação.

6.6. Os licitantes devem respeitar os preços máximos estabelecidos nas normas de regência de contratações públicas federais, quando participarem de licitações públicas;

6.6.1. O descumprimento das regras supramencionadas pela Administração por parte dos contratados 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 empresa contratada ao pagamento dos prejuízos ao erário, caso verificada a ocorrência de superfaturamento por sobrepreço na execução do contrato.

7. DA ABERTURA DA SESSÃO, CLASSIFICAÇÃO DAS PROPOSTAS E FORMULAÇÃO DE LANCES

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

7.2. O Pregoeiro verificará as propostas apresentadas, desclassificando desde logo aquelas que não estejam em conformidade com os requisitos estabelecidos neste Edital, contenham vícios insanáveis ou não apresentem as especificações técnicas exigidas no Termo de Referência.

7.2.1. Também será desclassificada a proposta que identifique o licitante.

7.2.2. A desclassificação será sempre fundamentada e registrada no sistema, com acompanhamento em tempo real por todos os participantes.

7.2.3. A não desclassificação da proposta não impede o seu julgamento definitivo em sentido contrário, levado a efeito na fase de aceitação.

7.3. O sistema ordenará automaticamente as propostas classificadas, sendo que somente estas participarão da fase de lances.

7.4. O sistema disponibilizará campo próprio para troca de mensagens entre o Pregoeiro e os licitantes.

7.5. Iniciada a etapa competitiva, os licitantes deverão encaminhar lances exclusivamente por meio do sistema eletrônico, sendo imediatamente informados do seu recebimento e do valor consignado no registro.

7.5.1. O lance deverá ser ofertado pelo valor unitário do item.

7.6. Os licitantes poderão oferecer lances sucessivos, observando o horário fixado para abertura da sessão e as regras estabelecidas no Edital.

7.7. O licitante somente poderá oferecer lance de valor inferior ou percentual de desconto superior ao último por ele ofertado e registrado pelo sistema.

7.8. O intervalo mínimo de diferença de valores ou percentuais entre os lances, que incidirá tanto em relação aos lances intermediários quanto em relação à proposta que cobrir a melhor oferta deverá ser 0,01% (um centésimo por cento).

7.9 Será adotado para o envio de lances no pregão eletrônico o modo de disputa "**aberto**", em que os licitantes apresentarão lances públicos e sucessivos, com prorrogações.

7.10 A etapa de lances da sessão pública terá duração de dez minutos e, após isso, será prorrogada automaticamente pelo sistema quando houver lance ofertado nos últimos dois minutos do período de duração da sessão pública.

7.11 A prorrogação automática da etapa de lances, de que trata o item anterior, será de dois minutos e ocorrerá sucessivamente sempre que houver lances enviados nesse período de prorrogação, inclusive no caso de lances intermediários.

7.12 Não havendo novos lances na forma estabelecida nos itens anteriores, a sessão pública encerrar-se-á automaticamente.

7.13 Encerrada a fase competitiva sem que haja a prorrogação automática pelo sistema, poderá o pregoeiro, assessorado pela equipe de apoio, justificadamente, admitir o reinício da sessão pública de lances, em prol da consecução do melhor preço.

7.14. Não serão aceitos dois ou mais lances de mesmo valor, prevalecendo aquele que for recebido e registrado em primeiro lugar.

7.15. Durante o transcurso da sessão pública, os licitantes serão informados, em tempo real, do valor do menor lance registrado, vedada a identificação do licitante.

7.16. No caso de desconexão com o Pregoeiro, no decorrer da etapa competitiva do Pregão, o sistema eletrônico poderá permanecer acessível aos licitantes para a recepção dos lances.

7.17. Quando a desconexão do sistema eletrônico para o pregoeiro persistir por tempo superior a dez minutos, a sessão pública será suspensa e reiniciada somente após decorridas vinte e quatro horas da comunicação do fato pelo Pregoeiro aos participantes, no sítio eletrônico utilizado para divulgação.

7.18. O Critério de julgamento adotado será o ***menor preço***, conforme definido neste Edital e seus anexos.

7.19. Caso o licitante não apresente lances, concorrerá com o valor de sua proposta.

7.20. Em relação a itens não exclusivos para participação de microempresas e empresas de pequeno porte, uma vez encerrada a etapa de lances, será efetivada a verificação automática, junto à Receita Federal, do porte da entidade empresarial. O sistema identificará em coluna própria as microempresas e empresas de pequeno porte participantes, procedendo à comparação com os valores da primeira colocada, se esta for empresa de maior porte, assim como das demais classificadas, para o fim de aplicar-se o disposto nos arts. 44 e 45 da LC nº 123, de 2006, regulamentada pelo Decreto nº 8.538, de 2015.

7.21. Nessas condições, as propostas de microempresas e empresas de pequeno porte que se encontrarem na faixa de até 5% (cinco por cento) acima da melhor proposta ou melhor lance serão consideradas empatadas com a primeira colocada.

7.22. A melhor classificada nos termos do item anterior terá o direito de encaminhar uma última oferta para desempate, obrigatoriamente em valor inferior ao da primeira colocada, no prazo de 5 (cinco) minutos controlados pelo sistema, contados após a comunicação automática para tanto.

7.23. Caso a microempresa ou a empresa de pequeno porte melhor classificada desista ou não se manifeste no prazo estabelecido, serão convocadas as demais licitantes microempresa e empresa de pequeno porte que se encontrem naquele intervalo de 5% (cinco por cento), na ordem de classificação, para o exercício do mesmo direito, no prazo estabelecido no subitem anterior.

7.24. No caso de equivalência dos valores apresentados pelas microempresas e empresas de pequeno porte que se encontrem nos intervalos estabelecidos nos subitens anteriores, será realizado sorteio entre elas para que se identifique aquela que primeiro poderá apresentar melhor oferta.

7.25. Só poderá haver empate entre propostas iguais (não seguidas de lances), ou entre lances finais da fase fechada do modo de disputa aberto e fechado.

7.26. Havendo eventual empate entre propostas ou lances, o critério de desempate será aquele previsto no art. 3º, § 2º, da Lei nº 8.666, de 1993, assegurando-se a preferência, sucessivamente, aos bens produzidos:

7.26.1. no pais;

7.26.2. por empresas brasileiras;

7.26.3. por empresas que invistam em pesquisa e no desenvolvimento de tecnologia no País;

7.26.4. 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.

7.27. Persistindo o empate, a proposta vencedora será sorteada pelo sistema eletrônico dentre as propostas ou os lances empatados.

7.28. Encerrada a etapa de envio de lances da sessão pública, o pregoeiro deverá encaminhar, pelo sistema eletrônico, contraproposta ao licitante que tenha apresentado o melhor preço, para que seja obtida melhor proposta, vedada a negociação em condições diferentes das previstas neste Edital.

7.28.1. A negociação será realizada por meio do sistema, podendo ser acompanhada pelos demais licitantes.

7.28.2. O pregoeiro solicitará ao licitante melhor classificado que, no prazo de **02 (duas) horas**, envie a proposta adequada ao último lance ofertado após a negociação realizada, acompanhada, se for o caso, dos documentos complementares, quando necessários à confirmação daqueles exigidos neste Edital e já apresentados.

7.29. Após a negociação do preço, o Pregoeiro iniciará a fase de aceitação e julgamento da proposta.

7.30. *Para a aquisição de bens comuns de informática e automação, definidos no art. 16-A da Lei n° 8.248, de 1991, será assegurado o direito de preferência previsto no seu artigo 3º, conforme procedimento estabelecido nos artigos 5° e 8° do Decreto n° 7.174, de 2010.*

7.30.1. *Nas contratações de bens e serviços de informática e automação, nos termos da Lei nº 8.248, de 1991, as licitantes qualificadas como microempresas ou empresas de pequeno porte que fizerem jus ao direito de preferência previsto no Decreto nº 7.174, de 2010, terão prioridade no exercício desse benefício em relação às médias e às grandes empresas na mesma situação.*

8. DA ACEITABILIDADE DA PROPOSTA VENCEDORA.

8.1. Encerrada a etapa de negociação, o pregoeiro examinará a proposta classificada em primeiro lugar quanto à adequação ao objeto e à compatibilidade do preço em relação ao máximo estipulado para contratação neste Edital e em seus anexos, observado o disposto no parágrafo único do art. 7º e no § 9º do art. 26 do Decreto n.º 10.024/2019.

8.2. O licitante qualificado como produtor rural pessoa física deverá incluir, na sua proposta, os percentuais das contribuições previstas no art. 176 da Instrução Normativa RFB n. 971, de 2009, em razão do disposto no art. 184, inciso V, sob pena de desclassificação.

8.3. Será desclassificada a proposta ou o lance vencedor, apresentar preço final superior ao preço máximo fixado (Acórdão nº 1455/2018 -TCU - Plenário), desconto menor do que o mínimo exigido ou que apresentar preço manifestamente inexequível.

8.3.1. Considera-se inexequível a proposta que apresente preços global ou unitários simbólicos, irrisórios ou de valor zero, incompatíveis com os preços dos insumos e salários de mercado, acrescidos dos respectivos encargos, ainda que o ato convocatório da licitação não tenha estabelecido limites mínimos, exceto quando se referirem a materiais e instalações de propriedade do próprio licitante, para os quais ele renuncie a parcela ou à totalidade da remuneração.

8.4. Qualquer interessado poderá requerer que se realizem diligências para aferir a exequibilidade e a legalidade das propostas, devendo apresentar as provas ou os indícios que fundamentam a suspeita;

8.5. Na hipótese de necessidade de suspensão da sessão pública para a realização de diligências, com vistas ao saneamento das propostas, a sessão pública somente poderá ser reiniciada mediante aviso prévio no sistema com, no mínimo, vinte e quatro horas de antecedência, e a ocorrência será registrada em ata;

8.6. O Pregoeiro poderá convocar o licitante para enviar documento digital complementar, por meio de funcionalidade disponível no sistema, no prazo de **02 (duas) horas,** sob pena de não aceitação da proposta.

8.6.1. É facultado ao pregoeiro prorrogar o prazo estabelecido, a partir de solicitação fundamentada feita no chat pelo licitante, antes de findo o prazo.

8.6.2. Dentre os documentos passíveis de solicitação pelo Pregoeiro, destacam-se os que contenham as características do material ofertado, tais como marca, modelo, tipo, fabricante e procedência, além de outras informações pertinentes, a exemplo de catálogos, folhetos ou propostas, encaminhados por meio eletrônico, ou, se for o caso, por outro meio e prazo indicados pelo Pregoeiro, sem prejuízo do seu ulterior envio pelo sistema eletrônico, sob pena de não aceitação da proposta.

8.7. Se a proposta ou lance vencedor for desclassificado, o Pregoeiro examinará a proposta ou lance subsequente, e, assim sucessivamente, na ordem de classificação.

8.8. Havendo necessidade, o Pregoeiro suspenderá a sessão, informando no "*chat*" a nova data e horário para a sua continuidade.

8.9. O Pregoeiro poderá encaminhar, por meio do sistema eletrônico, contraproposta ao licitante que apresentou o lance mais vantajoso, com o fim de negociar a obtenção de melhor preço, vedada a negociação em condições diversas das previstas neste Edital.

8.9.1. Também nas hipóteses em que o Pregoeiro não aceitar a proposta e passar à subsequente, poderá negociar com o licitante para que seja obtido preço melhor.

8.9.2. A negociação será realizada por meio do sistema, podendo ser acompanhada pelos demais licitantes.

8.10. Nos itens não exclusivos para a participação de microempresas e empresas de pequeno porte, sempre que a proposta não for aceita, e antes de o Pregoeiro passar à subsequente, haverá nova verificação, pelo sistema, da eventual ocorrência do empate ficto, previsto nos artigos 44 e 45 da LC nº 123, de 2006, seguindo-se a disciplina antes estabelecida, se for o caso.

8.11. Encerrada a análise quanto à aceitação da proposta, o pregoeiro verificará a habilitação do licitante, observado o disposto neste Edital.

9. DA HABILITAÇÃO

9.1. Como condição prévia ao exame da documentação de habilitação do licitante detentor da proposta classificada em primeiro lugar, o Pregoeiro verificará o eventual descumprimento das condições de participação, especialmente quanto à existência de sanção que impeça a participação no certame ou a futura contratação, mediante a consulta aos seguintes cadastros:

a) SICAF;

b) Cadastro Nacional de Empresas Inidôneas e Suspensas - CEIS, mantido pela Controladoria-Geral da União (www.portaldatransparencia.gov.br/ceis);

c) Cadastro Nacional de Condenações Cíveis por Atos de Improbidade Administrativa, mantido pelo Conselho Nacional de Justiça (www.cnj.jus.br/improbidade_adm/consultar_requerido.php).
d) Lista de Inidôneos e o Cadastro Integrado de Condenações por Ilícitos Administrativos - CADICON, mantidos pelo Tribunal de Contas da União - TCU;

9.1.1. Para a consulta de licitantes pessoa jurídica poderá haver a substituição das consultas das alíneas “b”, “c” e “d” acima pela Consulta Consolidada de Pessoa Jurídica do TCU (https://certidoesapf.apps.tcu.gov.br/)

9.1.2. A consulta aos cadastros será realizada em nome da empresa licitante e também de seu sócio majoritário, por força do artigo 12 da Lei n° 8.429, de 1992, que prevê, dentre as sanções impostas ao responsável pela prática de ato de improbidade administrativa, a proibição de contratar com o Poder Público, inclusive por intermédio de pessoa jurídica da qual seja sócio majoritário.

9.1.2.1. Caso conste na Consulta de Situação do Fornecedor a existência de Ocorrências Impeditivas Indiretas, o gestor diligenciará para verificar se houve fraude por parte das empresas apontadas no Relatório de Ocorrências Impeditivas Indiretas.

9.1.2.2. A tentativa de burla será verificada por meio dos vínculos societários, linhas de fornecimento similares, dentre outros.

9.1.2.3. O licitante será convocado para manifestação previamente à sua desclassificação.

9.1.3. Constatada a existência de sanção, o Pregoeiro reputará o licitante inabilitado, por falta de condição de participação.

9.1.4. No caso de inabilitação, haverá nova verificação, pelo sistema, da eventual ocorrência do empate ficto, previsto nos arts. 44 e 45 da Lei Complementar nº 123, de 2006, seguindo-se a disciplina antes estabelecida para aceitação da proposta subsequente.

9.2. Caso atendidas as condições de participação, a habilitação do licitantes será verificada por meio do SICAF, nos documentos por ele abrangidos em relação à habilitação jurídica, à regularidade fiscal e trabalhista, à qualificação econômica financeira e habilitação técnica, conforme o disposto na Instrução Normativa SEGES/MP nº 03, de 2018.

9.2.1. O interessado, para efeitos de habilitação prevista na Instrução Normativa SEGES/MP nº 03, de 2018 mediante utilização do sistema, deverá atender às condições exigidas no cadastramento no SICAF até o terceiro dia útil anterior à data prevista para recebimento das propostas;

9.2.2. É dever do licitante atualizar previamente as comprovações constantes do SICAF para que estejam vigentes na data da abertura da sessão pública, ou encaminhar, em conjunto com a apresentação da proposta, a respectiva documentação atualizada.

9.2.3. O descumprimento do subitem acima implicará a inabilitação do licitante, exceto se a consulta aos sítios eletrônicos oficiais emissores de certidões feita pelo Pregoeiro lograr êxito em encontrar a(s) certidão(ões) válida(s), conforme art. 43, §3º, do Decreto 10.024, de 2019.

9.3. Havendo a necessidade de envio de documentos de habilitação complementares, necessários à confirmação daqueles exigidos neste Edital e já apresentados, o licitante será convocado a encaminhá-los, em formato digital, via sistema, no prazo de **02 (duas) horas, sob pena de inabilitação.**

9.4. Somente haverá a necessidade de comprovação do preenchimento de requisitos mediante apresentação dos documentos originais não-digitais quando houver dúvida em relação à integridade do documento digital.

9.5. Não serão aceitos documentos de habilitação com indicação de CNPJ/CPF diferentes, salvo aqueles legalmente permitidos.

9.6. Se o licitante for a matriz, todos os documentos deverão estar em nome da matriz, e se o licitante for a filial, todos os documentos deverão estar em nome da filial, exceto aqueles documentos que, pela própria natureza, comprovadamente, forem emitidos somente em nome da matriz.

9.6.1. Serão aceitos registros de CNPJ de licitante matriz e filial com diferenças de números de documentos pertinentes ao CND e ao CRF/FGTS, quando for comprovada a centralização do recolhimento dessas contribuições.

9.7. Ressalvado o disposto no item 5.3, os licitantes deverão encaminhar, nos termos deste Edital, a documentação relacionada nos itens a seguir, para fins de habilitação:

9.8. **Habilitação jurídica:**

9.8.1. No caso de empresário individual: inscrição no Registro Público de Empresas Mercantis, a cargo da Junta Comercial da respectiva sede;

9.8.2. Em se tratando de microempreendedor individual – MEI: Certificado da Condição de Microempreendedor Individual - CCMEI, cuja aceitação ficará condicionada à verificação da autenticidade no sítio www.portaldoempreendedor.gov.br;

9.8.3. No caso de sociedade empresária ou empresa individual de responsabilidade limitada - EIRELI: ato constitutivo, estatuto ou contrato social em vigor, devidamente registrado na Junta Comercial da respectiva sede, acompanhado de documento comprobatório de seus administradores;

9.8.4. inscrição no Registro Público de Empresas Mercantis onde opera, com averbação no Registro onde tem sede a matriz, no caso de ser o participante sucursal, filial ou agência;

9.8.5. No caso de sociedade simples: inscrição do ato constitutivo no Registro Civil das Pessoas Jurídicas do local de sua sede, acompanhada de prova da indicação dos seus administradores;

9.8.6. No caso de cooperativa: ata de fundação e estatuto social em vigor, com a ata da assembleia que o aprovou, devidamente arquivado na Junta Comercial ou inscrito no Registro Civil das Pessoas Jurídicas da respectiva sede, bem como o registro de que trata o art. 107 da Lei nº 5.764, de 1971;

9.8.7. No caso de empresa ou sociedade estrangeira em funcionamento no País: decreto de autorização;

9.8.8. Os documentos acima deverão estar acompanhados de todas as alterações ou da consolidação respectiva;

9.9. **Regularidade fiscal e trabalhista:**

9.9.1. prova de inscrição no Cadastro Nacional de Pessoas Jurídicas ou no Cadastro de Pessoas Físicas, conforme o caso;

9.9.2. prova de regularidade fiscal perante a Fazenda Nacional, mediante apresentação de certidão expedida conjuntamente pela Secretaria da Receita Federal do Brasil (RFB) e pela Procuradoria-Geral da Fazenda Nacional (PGFN), referente a todos os créditos tributários federais e à Dívida Ativa da União (DAU) por elas administrados, inclusive aqueles relativos à Seguridade Social, nos termos da Portaria Conjunta nº

1.751, de 02/10/2014, do Secretário da Receita Federal do Brasil e da Procuradora-Geral da Fazenda Nacional.

9.9.3. prova de regularidade com o Fundo de Garantia do Tempo de Serviço (FGTS);

9.9.4. prova de inexistência de débitos inadimplidos perante a justiça do trabalho, mediante a apresentação de certidão negativa ou positiva com efeito de negativa, nos termos do Título VII-A da Consolidação das Leis do Trabalho, aprovada pelo Decreto-Lei nº 5.452, de 1º de maio de 1943;

9.9.5. prova de inscrição no cadastro de contribuintes estadual, relativo ao domicílio ou sede do licitante, pertinente ao seu ramo de atividade e compatível com o objeto contratual;

9.9.6. prova de regularidade com a Fazenda Estadual do domicílio ou sede do licitante, relativa à atividade em cujo exercício contrata ou concorre;

9.9.7. caso o licitante seja considerado isento dos tributos estaduais relacionados ao objeto licitatório, deverá comprovar tal condição mediante declaração da Fazenda Estadual do seu domicílio ou sede, ou outra equivalente, na forma da lei;

9.9.8. caso o licitante detentor do menor preço seja qualificado como microempresa ou empresa de pequeno porte deverá apresentar toda a documentação exigida para efeito de comprovação de regularidade fiscal, mesmo que esta apresente alguma restrição, sob pena de inabilitação.

9.10. **Qualificação Econômico-Financeira**.

9.10.1. certidão negativa de falência expedida pelo distribuidor da sede da pessoa jurídica;

9.10.2. balanço patrimonial e demonstrações contábeis do último exercício social, já exigíveis e apresentados na forma da lei, que comprovem a boa situação financeira da empresa, vedada a sua substituição por balancetes ou balanços provisórios, podendo ser atualizados por índices oficiais quando encerrado há mais de 3 (três) meses da data de apresentação da proposta;

9.10.2.1. No caso de fornecimento de bens para pronta entrega, não será exigido da licitante qualificada como microempresa ou empresa de pequeno porte, a apresentação de balanço patrimonial do último exercício financeiro. (Art. 3º do Decreto nº 8.538, de 2015);

9.10.2.2. no caso de empresa constituída no exercício social vigente, admite-se a apresentação de balanço patrimonial e demonstrações contábeis referentes ao período de existência da sociedade;

9.10.2.3. é admissível o balanço intermediário, se decorrer de lei ou contrato social/estatuto social.

9.10.2.4. Caso o licitante seja cooperativa, tais documentos deverão ser acompanhados da última auditoria contábil-financeira, conforme dispõe o artigo 112 da Lei nº 5.764, de 1971, ou de uma declaração, sob as penas da lei, de que tal auditoria não foi exigida pelo órgão fiscalizador;

9.10.3. A comprovação da situação financeira da empresa será constatada mediante obtenção de índices de Liquidez Geral (LG), Solvência Geral (SG) e Liquidez Corrente (LC), superiores a 1 (um) resultantes da aplicação das fórmulas:

$$LG = \frac{\text{Ativo Circulante + Realizável a Longo Prazo}}{\text{Passivo Circulante + Passivo Não Circulante}}$$

$$SG = \frac{\text{Ativo Total}}{\text{Passivo Circulante + Passivo Não Circulante}}$$

$$LC = \frac{\text{Ativo Circulante}}{\text{Passivo Circulante}}$$

9.10.4. As empresas que apresentarem resultado inferior ou igual a 1(um) em qualquer dos índices de Liquidez Geral (LG), Solvência Geral (SG) e Liquidez Corrente (LC), deverão comprovar, considerados os riscos para a Administração, e, a critério da autoridade competente, o capital mínimo ou o patrimônio líquido mínimo de 10% (dez por cento) do valor estimado da contratação ou do item pertinente.

9.11. **Qualificação Técnica**

9.11.1. Comprovação de aptidão para o fornecimento de bens em características, quantidades e prazos compatíveis com o objeto desta licitação, ou com o item pertinente, por meio da apresentação de atestados fornecidos por pessoas jurídicas de direito público ou privado, **comprovando que a licitante forneceu, instalou, configurou, realizou treinamento e prestou suporte técnico de solução.**

9.11.1.1. Para fins da comprovação de que trata este subitem, os atestados deverão dizer respeito a contratos executados com as seguintes características mínimas:

9.11.1.1.1. Solução de segurança composta por Firewall de Próxima Geração em alta disponibilidade de modelo igual ou superior ofertado.

9.12. O licitante enquadrado como microempreendedor individual que pretenda auferir os benefícios do tratamento diferenciado previstos na Lei Complementar n. 123, de 2006, estará dispensado (a) da prova de inscrição nos cadastros de contribuintes estadual e municipal e (b) da apresentação do balanço patrimonial e das demonstrações contábeis do último exercício.

9.13. A existência de restrição relativamente à regularidade fiscal e trabalhista não impede que a licitante qualificada como microempresa ou empresa de pequeno porte seja declarada vencedora, uma vez que atenda a todas as demais exigências do edital.

9.13.1. A declaração do vencedor acontecerá no momento imediatamente posterior à fase de habilitação.

9.14. Caso a proposta mais vantajosa seja ofertada por licitante qualificada como microempresa ou empresa de pequeno porte, e uma vez constatada a existência de alguma restrição no que tange à regularidade fiscal e trabalhista, a mesma será convocada para, no prazo de 5 (cinco) dias úteis, após a declaração do vencedor, comprovar a regularização. O prazo poderá ser prorrogado por igual período, a critério da administração pública, quando requerida pelo licitante, mediante apresentação de justificativa.

9.15. A não-regularização fiscal e trabalhista no prazo previsto no subitem anterior acarretará a inabilitação do licitante, sem prejuízo das sanções previstas neste Edital, sendo facultada a convocação dos licitantes remanescentes, na ordem de classificação. Se, na ordem de classificação, seguir-se outra microempresa, empresa de pequeno porte ou sociedade cooperativa com alguma restrição na documentação fiscal e trabalhista, será concedido o mesmo prazo para regularização.

9.16. Havendo necessidade de analisar minuciosamente os documentos exigidos, o Pregoeiro suspenderá a sessão, informando no “chat” a nova data e horário para a continuidade da mesma.

9.17. Será inabilitado o licitante que não comprovar sua habilitação, seja por não apresentar quaisquer dos documentos exigidos, ou apresentá-los em desacordo com o estabelecido neste Edital.

9.18. Nos itens não exclusivos a microempresas e empresas de pequeno porte, em havendo inabilitação, haverá nova verificação, pelo sistema, da eventual ocorrência do empate ficto, previsto nos artigos 44 e 45 da LC nº 123, de 2006, seguindo-se a disciplina antes estabelecida para aceitação da proposta subsequente.

9.19. O licitante provisoriamente vencedor em um item, que estiver concorrendo em outro item, ficará obrigado a comprovar os requisitos de habilitação cumulativamente, isto é, somando as exigências do item em que venceu às do item em que estiver concorrendo, e assim sucessivamente, sob pena de inabilitação, além da aplicação das sanções cabíveis.

9.19.1. Não havendo a comprovação cumulativa dos requisitos de habilitação, a inabilitação recairá sobre o(s) item(ns) de menor(es) valor(es) cuja retirada(s) seja(m) suficiente(s) para a habilitação do licitante nos remanescentes.

Constatado o atendimento às exigências de habilitação fixadas no Edital, o licitante será declarado vencedor.

10. DO ENCAMINHAMENTO DA PROPOSTA VENCEDORA

10.1. A proposta final do licitante declarado vencedor deverá ser encaminhada no prazo de **02 (duas) horas,** a contar da solicitação do Pregoeiro no sistema eletrônico e deverá:

10.1.1. ser redigida em língua portuguesa, datilografada ou digitada, em uma via, sem emendas, rasuras, entrelinhas ou ressalvas, devendo a última folha ser assinada e as demais rubricadas pelo licitante ou seu representante legal.

10.1.2. conter a indicação do banco, número da conta e agência do licitante vencedor, para fins de pagamento.

10.2. A proposta final deverá ser documentada nos autos e será levada em consideração no decorrer da execução do contrato e aplicação de eventual sanção à Contratada, se for o caso.

10.2.1. Todas as especificações do objeto contidas na proposta, tais como marca, modelo, tipo, fabricante e procedência, vinculam a Contratada.

10.3. Os preços deverão ser expressos em moeda corrente nacional, o valor unitário em algarismos e o valor global em algarismos e por extenso (art. 5º da Lei nº 8.666/93).

10.3.1. Ocorrendo divergência entre os preços unitários e o preço global, prevalecerão os primeiros; no caso de divergência entre os valores numéricos e os valores expressos por extenso, prevalecerão estes últimos.

10.4. A oferta deverá ser firme e precisa, limitada, rigorosamente, ao objeto deste Edital, sem conter alternativas de preço ou de qualquer outra condição que induza o julgamento a mais de um resultado, sob pena de desclassificação.

10.5. A proposta deverá obedecer aos termos deste Edital e seus Anexos, não sendo considerada aquela que não corresponda às especificações ali contidas ou que estabeleça vínculo à proposta de outro licitante.

10.6. As propostas que contenham a descrição do objeto, o valor e os documentos complementares estarão disponíveis na internet, após a homologação.

11. DOS RECURSOS

11.1. Declarado o vencedor e decorrida a fase de regularização fiscal e trabalhista da licitante qualificada como microempresa ou empresa de pequeno porte, se for o caso, será concedido o prazo de no mínimo trinta minutos, para que qualquer licitante manifeste a intenção de recorrer, de forma motivada, isto é, indicando contra qual(is) decisão(ões) pretende recorrer e por quais motivos, em campo próprio do sistema.

11.2. Havendo quem se manifeste, caberá ao Pregoeiro verificar a tempestividade e a existência de motivação da intenção de recorrer, para decidir se admite ou não o recurso, fundamentadamente.

11.2.1. Nesse momento o Pregoeiro não adentrará no mérito recursal, mas apenas verificará as condições de admissibilidade do recurso.

11.2.2. A falta de manifestação motivada do licitante quanto à intenção de recorrer importará a decadência desse direito.

11.2.3. Uma vez admitido o recurso, o recorrente terá, a partir de então, o prazo de três dias para apresentar as razões, pelo sistema eletrônico, ficando os demais licitantes, desde logo, intimados para, querendo, apresentarem contrarrazões também pelo sistema eletrônico, em outros três dias, que começarão a contar do término do prazo do recorrente, sendo-lhes assegurada vista imediata dos elementos indispensáveis à defesa de seus interesses.

11.3. O acolhimento do recurso invalida tão somente os atos insuscetíveis de aproveitamento.

11.4. Os autos do processo permanecerão com vista franqueada aos interessados, no endereço constante neste Edital.

12. DA REABERTURA DA SESSÃO PÚBLICA

12.1. A sessão pública poderá ser reaberta:

12.1.1. Nas hipóteses de provimento de recurso que leve à anulação de atos anteriores à realização da sessão pública precedente ou em que seja anulada a própria sessão pública, situação em que serão repetidos os atos anulados e os que dele dependam.

12.1.2. Quando houver erro na aceitação do preço melhor classificado ou quando o licitante declarado vencedor não assinar o contrato, não retirar o instrumento equivalente ou não comprovar a regularização fiscal e trabalhista, nos termos do art. 43, §1º da LC nº 123/2006. Nessas hipóteses, serão adotados os procedimentos imediatamente posteriores ao encerramento da etapa de lances.

12.2. Todos os licitantes remanescentes deverão ser convocados para acompanhar a sessão reaberta.

12.2.1. A convocação se dará por meio do sistema eletrônico (“chat”), e-mail, de acordo com a fase do procedimento licitatório.

12.2.2. A convocação feita por e-mail dar-se-á de acordo com os dados contidos no SICAF, sendo responsabilidade do licitante manter seus dados cadastrais atualizados.

13. DA ADJUDICAÇÃO E HOMOLOGAÇÃO

13.1. O objeto da licitação será adjudicado ao licitante declarado vencedor, por ato do Pregoeiro, caso não haja interposição de recurso, ou pela autoridade competente, após a regular decisão dos recursos apresentados.

13.2. Após a fase recursal, constatada a regularidade dos atos praticados, a autoridade competente homologará o procedimento licitatório.

14. DA GARANTIA DE EXECUÇÃO

13.1 Não haverá exigência de garantia de execução para a presente contratação, conforme regras constantes **do item 12 do Anexo I – Termo de Referência deste Edital.**

15. DA GARANTIA CONTRATUAL DOS BENS

15.1. Será exigida garantia contratual dos bens fornecidos na presente contratação, complementar à legal, conforme prazos mínimos e demais regras constantes no **item 13 do Anexo I – Termo de Referência deste Edital.**

16. DA ATA DE REGISTRO DE PREÇOS

16.1. Homologado o resultado da licitação, terá o adjudicatário o prazo de de 05 (cinco) dias, contados a partir da data de sua convocação, para assinar a Ata de Registro de Preços, cujo prazo de validade encontra-se nela fixado, sob pena de decair do direito à contratação, sem prejuízo das sanções previstas neste Edital.

16.2. Alternativamente à convocação para comparecer perante o órgão ou entidade para a assinatura da Ata de Registro de Preços, a Administração poderá encaminhá-la para assinatura, mediante correspondência postal com aviso de recebimento (AR) ou meio eletrônico, para que seja assinada e devolvida no prazo de de 05 (cinco) dias, a contar da data de seu recebimento.

16.3. O prazo estabelecido no subitem anterior para assinatura da Ata de Registro de Preços poderá ser prorrogado uma única vez, por igual período, quando solicitado pelo(s) licitante(s) vencedor(s), durante o seu transcurso, e desde que devidamente aceito.

16.4. Serão formalizadas tantas Atas de Registro de Preços quanto necessárias para o registro de todos os itens constantes no Termo de Referência, com a indicação do licitante vencedor, a descrição do(s) item(ns), as respectivas quantidades, preços registrados e demais condições.

16.4.1. Será incluído na ata, sob a forma de anexo, o registro dos licitantes que aceitarem cotar os bens ou serviços com preços iguais aos do licitante vencedor na sequência da classificação do certame, excluído o percentual referente à margem de preferência, quando o objeto não atender aos requisitos previstos no art. 3º da Lei nº 8.666, de 1993;

17. DO TERMO DE CONTRATO OU INSTRUMENTO EQUIVALENTE

17.1. Após a homologação da licitação, em sendo realizada a contratação, será firmado Termo de Contrato ou emitido instrumento equivalente.

17.2. O adjudicatário terá o prazo de 05 (cinco) dias úteis, contados a partir da data de sua convocação, para assinar o Termo de Contrato ou aceitar instrumento equivalente, conforme o caso (Nota de Empenho/Carta Contrato/Autorização), sob pena de decair do direito à contratação, sem prejuízo das sanções previstas neste Edital.

17.2.1. Alternativamente à convocação para comparecer perante o órgão ou entidade para a assinatura do Termo de Contrato ou aceite do instrumento equivalente, a Administração poderá encaminhá-lo para assinatura ou aceite da Adjudicatária, mediante correspondência postal com aviso de recebimento (AR) ou meio eletrônico, para que seja assinado ou aceito no prazo de 05 (cinco) dias, a contar da data de seu recebimento.

17.2.2. O prazo previsto no subitem anterior poderá ser prorrogado, por igual período, por solicitação justificada do adjudicatário e aceita pela Administração.

17.3. O Aceite da Nota de Empenho ou do instrumento equivalente, emitida à empresa adjudicada, implica no reconhecimento de que:

17.3.1. referida Nota está substituindo o contrato, aplicando-se à relação de negócios ali estabelecida as disposições da Lei nº 8.666, de 1993;

17.3.2. a contratada se vincula à sua proposta e às previsões contidas no edital e seus anexos;

17.3.3. a contratada reconhece que as hipóteses de rescisão são aquelas previstas nos artigos 77 e 78 da Lei nº 8.666/93 e reconhece os direitos da Administração previstos nos artigos 79 e 80 da mesma Lei.

17.4. O prazo de vigência da contratação é de **12 (dose) meses** prorrogável conforme previsão no instrumento contratual ou no termo de referência.

17.5. Previamente à contratação a Administração realizará consulta ao SICAF para identificar possível suspensão temporária de participação em licitação, no âmbito do órgão ou entidade, proibição de contratar com o Poder Público, bem como ocorrências impeditivas indiretas, observado o disposto no art. 29, da Instrução Normativa nº 3, de 26 de abril de 2018, e nos termos do art. 6º, III, da Lei nº 10.522, de 19 de julho de 2002, consulta prévia ao CADIN.

17.5.1. Nos casos em que houver necessidade de assinatura do instrumento de contrato, e o fornecedor não estiver inscrito no SICAF, este deverá proceder ao seu cadastramento, sem ônus, antes da contratação.

17.5.2. Na hipótese de irregularidade do registro no SICAF, o contratado deverá regularizar a sua situação perante o cadastro no prazo de até 05 (cinco) dias úteis, sob pena de aplicação das penalidades previstas no edital e anexos.

17.6. Na assinatura do contrato ou da ata de registro de preços, será exigida a comprovação das condições de habilitação consignadas no edital, que deverão ser mantidas pelo licitante durante a vigência do contrato ou da ata de registro de preços.

17.7. Na hipótese de o vencedor da licitação não comprovar as condições de habilitação consignadas no edital ou se recusar a assinar o contrato ou a ata de registro de preços, a Administração, sem prejuízo da aplicação das sanções das demais cominações legais cabíveis a esse licitante, poderá convocar outro licitante, respeitada a ordem de classificação, para, após a comprovação dos requisitos para habilitação, analisada a proposta e eventuais documentos complementares e, feita a negociação, assinar o contrato ou a ata de registro de preços.

18. DO REAJUSTAMENTO EM SENTIDO GERAL

18.1. As regras acerca do reajustamento em sentido geral do valor contratual são as estabelecidas no Termo de Referência, anexo a este Edital.

19. DO RECEBIMENTO DO OBJETO E DA FISCALIZAÇÃO

19.1. Os critérios de recebimento e aceitação do objeto e de fiscalização estão previstos no Termo de Referência.

20. DAS OBRIGAÇÕES DA CONTRATANTE E DA CONTRATADA

20.1. As obrigações da Contratante e da Contratada são as estabelecidas no Termo de Referência.

21. DAS SANÇÕES ADMINISTRATIVAS.

21.1. Comete infração administrativa, nos termos da Lei nº 10.520, de 2002, o licitante/adjudicatário que:

21.1.1. não assinar o termo de contrato ou aceitar/retirar o instrumento equivalente, quando convocado dentro do prazo de validade da proposta;

21.1.2. não assinar a ata de registro de preços, quando cabível;

21.1.3. apresentar documentação falsa;

21.1.4. deixar de entregar os documentos exigidos no certame;

21.1.5. ensejar o retardamento da execução do objeto;

21.1.6. não mantiver a proposta;

21.1.7. cometer fraude fiscal;

21.1.8. comportar-se de modo inidôneo;

21.2. As sanções do item acima também se aplicam aos integrantes do cadastro de reserva, em pregão para registro de preços que, convocados, não honrarem o compromisso assumido injustificadamente.

21.3. Considera-se comportamento inidôneo, entre outros, a declaração falsa quanto às condições de participação, quanto ao enquadramento como ME/EPP ou o conluio entre os licitantes, em qualquer momento da licitação, mesmo após o encerramento da fase de lances.

21.4. O licitante/adjudicatário que cometer qualquer das infrações discriminadas nos subitens anteriores ficará sujeito, sem prejuízo da responsabilidade civil e criminal, às seguintes sanções:

21.4.1. Advertência por faltas leves, assim entendidas como aquelas que não acarretarem prejuízos significativos ao objeto da contratação;

21.4.2. Multa de 20% (vinte por cento) sobre o valor estimado do(s) item(s) prejudicado(s) pela conduta do licitante;

21.4.3. Suspensão de licitar e impedimento de contratar com o órgão, entidade ou unidade administrativa pela qual a Administração Pública opera e atua concretamente, pelo prazo de até dois anos;

21.4.4. Impedimento de licitar e de contratar com a União e descredenciamento no SICAF, pelo prazo de até cinco anos;

21.5. Declaração de inidoneidade para licitar ou contratar com a Administração Pública, enquanto perdurarem os motivos determinantes da punição ou até que seja promovida a

reabilitação perante a própria autoridade que aplicou a penalidade, que será concedida sempre que a Contratada ressarcir a Contratante pelos prejuízos causados;

21.6. A penalidade de multa pode ser aplicada cumulativamente com as demais sanções.

21.7. Se, durante o processo de aplicação de penalidade, se houver indícios de prática de infração administrativa tipificada pela Lei nº 12.846, de 1º de agosto de 2013, como ato lesivo à administração pública nacional ou estrangeira, cópias do processo administrativo necessárias à apuração da responsabilidade da empresa deverão ser remetidas à autoridade competente, com despacho fundamentado, para ciência e decisão sobre a eventual instauração de investigação preliminar ou Processo Administrativo de Responsabilização – PAR.

21.8. A apuração e o julgamento das demais infrações administrativas não consideradas como ato lesivo à Administração Pública nacional ou estrangeira nos termos da Lei nº 12.846, de 1º de agosto de 2013, seguirão seu rito normal na unidade administrativa.

21.9. O processamento do PAR não interfere no seguimento regular dos processos administrativos específicos para apuração da ocorrência de danos e prejuízos à Administração Pública Federal resultantes de ato lesivo cometido por pessoa jurídica, com ou sem a participação de agente público.

21.10. Caso o valor da multa não seja suficiente para cobrir os prejuízos causados pela conduta do licitante, a União ou Entidade poderá cobrar o valor remanescente judicialmente, conforme artigo 419 do Código Civil.

21.11. A aplicação de qualquer das penalidades previstas realizar-se-á em processo administrativo que assegurará o contraditório e a ampla defesa ao licitante/adjudicatário, observando-se o procedimento previsto na Lei nº 8.666, de 1993, e subsidiariamente na Lei nº 9.784, de 1999.

21.12. A autoridade competente, na aplicação das sanções, levará em consideração a gravidade da conduta do infrator, o caráter educativo da pena, bem como o dano causado à Administração, observado o princípio da proporcionalidade.

21.13. As penalidades serão obrigatoriamente registradas no SICAF.

21.14. As sanções por atos praticados no decorrer da contratação estão previstas no Termo de Referência.

22. DA FORMAÇÃO DO CADASTRO DE RESERVA

22.1. Após o encerramento da etapa competitiva, os licitantes poderão reduzir seus preços ao valor da proposta do licitante mais bem classificado.

22.2. A apresentação de novas propostas na forma deste item não prejudicará o resultado do certame em relação ao licitante melhor classificado.

22.3. Havendo um ou mais licitantes que aceitem cotar suas propostas em valor igual ao do licitante vencedor, estes serão classificados segundo a ordem da última proposta individual apresentada durante a fase competitiva.

22.4. Esta ordem de classificação dos licitantes registrados deverá ser respeitada nas contratações e somente será utilizada acaso o melhor colocado no certame não assine a ata ou tenha seu registro cancelado nas hipóteses previstas nos artigos 20 e 21 do Decreto n° 7.892/213.

23. DA IMPUGNAÇÃO AO EDITAL E DO PEDIDO DE ESCLARECIMENTO

23.1. **Até 03 (três) dias úteis antes da data designada para a abertura da sessão pública**, qualquer pessoa poderá impugnar este Edital.

23.2. A impugnação poderá ser realizada por forma eletrônica, pelo e-mail pelo e-mail **cpl@ufam.edu.br,** ou por petição dirigida ou protocolada no endereço Sala de Licitações /

UFAM - Av. Rodrigo Otávio n.º 6.200, Campus Universitário Senador Arthur Virgílio Filho, Setor Sul, Bloco “J”, Setor de Licitações, Coroado – Manaus-AM, CEP 69.077-000.

23.3. Caberá ao Pregoeiro, auxiliado pelos responsáveis pela elaboração deste Edital e seus anexos, **decidir sobre a impugnação no prazo de até dois dias úteis contados da data de recebimento da impugnação.**

23.4. Acolhida a impugnação, será definida e publicada nova data para a realização do certame.

23.5. Os pedidos de esclarecimentos referentes a este processo licitatório deverão ser enviados ao Pregoeiro, **até 03 (três) dias úteis anteriores à data designada para abertura da sessão pública**, exclusivamente por meio eletrônico via internet, no endereço indicado no Edital.

23.6. **O pregoeiro responderá aos pedidos de esclarecimentos no prazo de dois dias úteis, contado da data de recebimento do pedido**, e poderá requisitar subsídios formais aos responsáveis pela elaboração do edital e dos anexos.

23.7. As impugnações e pedidos de esclarecimentos não suspendem os prazos previstos no certame.

23.7.1. A concessão de efeito suspensivo à impugnação é medida excepcional e deverá ser motivada pelo pregoeiro, nos autos do processo de licitação.

23.8. As respostas aos pedidos de esclarecimentos serão divulgadas pelo sistema e vincularão os participantes e a administração.

24. DAS DISPOSIÇÕES GERAIS

24.1. Da sessão pública do Pregão divulgar-se-á Ata no sistema eletrônico.

24.2. Não havendo expediente ou ocorrendo qualquer fato superveniente que impeça a realização do certame na data marcada, a sessão será automaticamente transferida para o primeiro dia útil subsequente, no mesmo horário anteriormente estabelecido, desde que não haja comunicação em contrário, pelo Pregoeiro.

24.3. Todas as referências de tempo no Edital, no aviso e durante a sessão pública observarão o horário de Brasília – DF.

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

24.5. A homologação do resultado desta licitação não implicará direito à contratação.

24.6. As normas disciplinadoras da licitação serão sempre interpretadas em favor da ampliação da disputa entre os interessados, desde que não comprometam o interesse da Administração, o princípio da isonomia, a finalidade e a segurança da contratação.

24.7. Os licitantes assumem todos os custos de preparação e apresentação de suas propostas e a Administração não será, em nenhum caso, responsável por esses custos, independentemente da condução ou do resultado do processo licitatório.

24.8. Na contagem dos prazos estabelecidos neste Edital e seus Anexos, excluir-se-á o dia do início e incluir-se-á o do vencimento. Só se iniciam e vencem os prazos em dias de expediente na Administração.

24.9. O desatendimento de exigências formais não essenciais não importará o afastamento do licitante, desde que seja possível o aproveitamento do ato, observados os princípios da isonomia e do interesse público.

24.10. Em caso de divergência entre disposições deste Edital e de seus anexos ou demais peças que compõem o processo, prevalecerá as deste Edital.

24.11. O Edital está disponibilizado, na íntegra, no endereço eletrônico https://proadm.ufam.edu.br/menu06item01.html, e também poderão ser lidos e/ou obtidos no endereço **Sala de Licitações / UFAM -** Av. Rodrigo Otávio n.º 6.200, Campus Universitário Senador Arthur Virgílio Filho, Setor Sul, Bloco "J", Setor de Licitações, Coroado – Manaus-AM, **CEP 69.077-000,** nos dias úteis, no horário das 08h horas às 17h horas, mesmo endereço e período no qual os autos do processo administrativo permanecerão com vista franqueada aos interessados.

24.12. Integram este Edital, para todos os fins e efeitos, os seguintes anexos:

24.12.1. ANEXO I - Termo de Referência;

24.12.2. ANEXO II – Modelo de Declaração de Inexistência de Vinculo Familiar;

24.12.3. ANEXO II – Minuta de Ata de Registro de Preços.

Manaus, 25 de junho de 2020.

TIAGO LUZ DE OLIVEIRA
Coordenador Geral de Licitações
Universidade Federal do Amazonas

ANEXO I

TERMO DE REFERÊNCIA 11/2020
IRP 16/2020

1 DO OBJETO

1.1 Aquisição de material permanente (fornecimento de solução de proteção de rede de dados com características de *Firewall* de próxima geração (*Next Generation Firewall* – NGFW), com suporte de 60 meses, solução de gerenciamento centralizado, serviços de instalação, configuração e treinamento de pessoal), conforme condições, quantidades, exigências e estimativas encaminhadas pelo Centro de Tecnologia da Informação e Comunicação-CTIC, estabelecidas neste instrumento:

ITEM	CATMAT E MATERIAL ESPECIFICADO	TIPO DE BENEFÍCIO	UNIDADE	QUANTIDADE	VALOR MÁXIMO ACEITÁVEL	VALOR TOTAL DO ITEM
01	150100 - FIREWALL DE PRÓXIMA GERAÇÃO. INCLUSO LICENCIAMENTO DE THREAT PREVENTION, URL FILTERING E SUPORTE POR 60 MESES, SOLUÇÃO DE GERENCIAMENTO CENTRALIZADO E SERVIÇOS DE INSTALAÇÃO, CONFIGURAÇÃO E TREINAMENTO DE PESSOAL	SEM BENEFÍCIO	UNIDADE	02	R$ 1.182.941,94	R$ 2.365.883,88

1.2 Este Termo de Referência segue as orientações da Secretaria de Logística e Tecnologia da Informação, do Ministério do Planejamento, Orçamento e Gestão, para atendimento do Decreto n. 8.538/2015, sendo que a licitação será destinada à ampla concorrência (Tipo Sem Benefício).

1.2.1 A solução constituída dos itens relacionados neste Termo de Referência, deverá ser do mesmo fabricante, a fim de garantir a entrega e execução dos serviços por uma única empresa e a total compatibilidade entre eles. Tal condição visa a plena qualificação da empresa fornecedora que prestará os serviços de fornecimento, bem como prestará os serviços de suporte durante a vigência do contrato de garantia dos equipamentos, a total compatibilidade entre os equipamentos solicitados, a redução de custos operacionais e de infraestrutura física, a capacidade técnica de manter a solução em operação, os recursos humanos disponíveis para prestarem o devido apoio, treinamento e curva de aprendizagem e o custo total de propriedade.

1.3 A pesquisa de mercado segue as determinações da Instrução Normativa n. 05/2014, emitida pela Secretária de Logística e Tecnologia da Informação do Ministério do Planejamento, Orçamento e Gestão, sendo utilizada como metodologia para obtenção do preço de referência para a contratação à média dos valores obtidos na pesquisa de preços. Declaramos para todos os fins de direito, que realizamos a pesquisa de preços para futura aquisição dos materiais, objetos deste processo licitatório. A pesquisa foi feita junto ao Banco de Preços, refletindo a similaridade dos serviços e preços. Os valores obtidos na pesquisa foram avaliados criticamente, no sentido de que suas médias não apresentam grandes variações, não comprometendo a estimativa do preço de referência, representando de forma satisfatória os preços praticados no mercado.

1.3.1 O Banco de Preços é um avançado banco de dados desenvolvido para auxiliar em todas as fases da contratação pública: preparação, licitação e execução do contrato. Possui a maior base de consulta disponível no mercado, com mais de 12 milhões de preços, o que amplia o resultado da pesquisa, afere a realidade dos preços e atende aos princípios constitucionais da economicidade e da moralidade. Possui funcionalidades exclusivas que o caracterizam como uma solução integrada e completa. Além da pesquisa global, sem distinção de fonte, o recurso possibilita a realização de pesquisas específicas e individualizadas nos Portais Compras Governamentais, Licitações-e e Bolsa Eletrônica de Compras – BEC, nos sítios eletrônicos especializados e de domínio amplo e, ainda, junto aos fornecedores, possibilitando maior transparência quanto aos parâmetros utilizados e garantindo a amplitude da pesquisa (art. 37, caput da CF/88 e Acórdão n. 1445/2015-TCU/Plenário). Para os órgãos e entidades integrantes do SISG, operacionaliza a utilização de todos os parâmetros indicados no art. 2º,

da IN n. 05/2014, de forma conjunta ou individualizada, conforme a conveniência e oportunidade administrativa.

1.4 Caso seja necessário, o pregoeiro poderá encaminhar os esclarecimentos, questionamentos e pedidos de impugnações à Centro de Tecnologia da Informação e Comunicação, responsável Jorge Carlos Magno Silva de Lima (Diretor do CTIC), por meio do *e-mail* secretariactic@ufam.edu.br. O pregoeiro também poderá solicitar análise dos materiais ofertados, bem com emissão de Parecer Técnico, junto à unidade solicitante.

1.5 Em conformidade com a IN SLTI/MPOG n. 01/2010, a Contratada deverá cumprir com os seguintes requisitos de sustentabilidade ambiental:

1.5.1 Que os bens sejam constituídos, no todo ou em parte, por material reciclado, atóxico, biodegradável, conforme ABNT NBR – 15448-1 e 15448-2.

1.5.2 Que sejam observados os requisitos ambientais para a obtenção de certificação do Instituto Nacional de Metrologia, Normalização e Qualidade Industrial – INMETRO como produtos sustentáveis ou de menor impacto ambiental em relação aos seus similares.

1.5.3 Que os bens devam ser, preferencialmente, acondicionados em embalagem individual adequada, com o menor volume possível, que utilize materiais recicláveis, de forma a garantir a máxima proteção durante o transporte e o armazenamento.

1.5.4 Que os bens não contenham substâncias perigosas em concentração acima da recomendada na diretiva RoHS (Restriction of Certain Hazardous Substances), tais como mercúrio (Hg), chumbo (Pb), cromo hexavalente (Cr(VI)), cádmio (Cd), bifenil-polibromados (PBBs), éteres difenil-polibromados (PBDEs).

1.6 Quando da participação na licitação, o licitante vencedor deverá cumprir com as obrigações estabelecidas no Decreto n. 7.174/2010, que regulamenta a contratação de bens e serviços de informática e automação pela Administração Federal.

1.7 O prazo de vigência da contratação é de 12 (doze) meses contados da homologação, não prorrogável.

2 DA JUSTIFICATIVA PARA AQUISIÇÃO DOS MATERIAIS

2.1 O ganho alcançado pela instituição com a informatização de seus processos administrativos e de negócio está calcada na capacidade da TI em assegurar a disponibilidade e o desempenho da sua infraestrutura tecnológica, que é suporte aos sistemas de informação e serviços de TI. Assim, a indisponibilidade ou a grave degradação dessa infraestrutura coloca em risco o funcionamento da instituição e impacta sobremaneira a prestação dos serviços públicos e institucionais.

2.2 Os pilares da segurança da informação sofreram diversas alterações na era da informação. Segurança é um processo continuo, que não se conclui. Novos tipos de ataques cibernéticos sãos descobertos quase que diariamente. Vulnerabilidades de soGwares são divulgadas todos os dias. Os processos referentes à segurança da informação precisam ser revistos constantemente através de relatórios e acompanham netos e, obviamente, as soluções de TIC envolvidas com a segurança da rede de dados precisam ser atualizados na mesma velocidade.

2.3 Firewall é um dispositivo composto de soGware e/ou hardware, que limita o acesso a rede de dados. Seu objetivo é permitir somente a transmissão e recepção de dados autorizados. Pode ser usado para ajudar a impedir que a rede ou um servidor seja acessado sem autorização. Assim, é possível evitar que informações sejam capturadas ou que sistemas tenham seu funcionamento prejudicado pela ação de “pragas digitais”, além de possibilitar o bloqueio de acesso a programas e sites não autorizados.

2.4 A contratação mostra-se imprescindível em razão da necessidade de manutenção dos sistemas e serviços de TIC, sendo de suma importância a adoção de solução de segurança de informações. Um ataque bem sucedido, no mundo digital, à rede de dados pode ter consequências graves difíceis de estimar, tanto técnica como para a imagem da UFAM.

2.5 Atualmente o CTIC mantêm em seus servidores muitos serviços e sistema informatizados, como E-Campus, SEI, Concursos e outros. Nesse cenário é cada vez maior a necessidade de implementação de uma solução de segurança para o ambiente de TIC. Focado na missão e visão da UFAM e garantindo a perfeita operacionalização dos serviços e sistemas de informação e comunicação, este projeto tem como objetivo o atendimento das melhores práticas de gestão de TIC, focado em garantir a disponibilidade, acessibilidade, segurança e performance das nossas soluções tecnológicas.

2.6 As soluções de TIC de alta complexidade atendidos neste projeto, são considerados de extrema necessidade, a fim de garantir a integridade da redes da dados da instituição, assim como a segurança das informações que trafegam interna e externamente, possibilitando o atendimento das demandas da comunidade da Universidade Federal do Amazonas e assim cumprir com a visão do Centro de Centro de Tecnologia da Informação e Comunicação da UFAM (CTIC/UFAM) que é "Promover soluções de TIC com eficiência e qualidade, alinhadas às estratégias da Universidade Federal do Amazonas".

2.7 PDI e PDTIC: A demanda objeto deste Termo de Referência está incluída no PDI da UFAM no item 8.3.2. Garantir a qualidade na prestação dos serviços de TIC com eficiência e eficácia, no item 8.3.3. Garantir a segurança da informação e comunicação e no item 8.4.1. Assegurar o funcionamento dos serviços da instituição; e no PDTIC no item #13447. Assegurar continuidade e disponibilidade dos serviços de TIC e no item 13449. Garantir infraestrutura de TIC adequada ao pleno funcionamento dos serviços da instituição.

3 DA CLASSIFICAÇÃO DOS BENS COMUNS

3.1 Os materiais são considerados bens comuns, para fins do disposto no art. 3º, inciso II, do Decreto n. 10.024/2019, devendo a licitação ser realizada na modalidade Pregão Eletrônico SRP, Tipo Menor Preço.

3.2 Em conformidade com o art. 3º, do Decreto n. 7.892/2013, a escolha pelo SRP se dá em razão do seguinte fator:

3.2.1 Quando for conveniente a aquisição de bens com previsão de entregas parceladas.

3.3 Será vedado efetuar acréscimos nos quantitativos, quando da assinatura da Ata de Registro de Preços, inclusive o acréscimo de que trata o § 1º do art. 65, da Lei n. 8.666/1993, conforme estabelecido no Decreto n. 7.892/2013.

4 DA ENTREGA DOS MATERIAIS E DA ACEITAÇÃO DOS OBJETOS

4.1 O prazo de entrega dos materiais é de 90 (noventa) dias, contados a partir do recebimento da Nota de Empenho, enviada pela Coordenação de Compras através do *e-mail* compras_ufam@hotmail.com, em remessa única.

4.1.2 Os materiais permanentes deverão ser entregues à Coordenação de Patrimônio, localizada na Avenida Rodrigo Octávio Jordão Ramos, nº 6.200, Prédio do Patrimônio, Estrada do Aviário, Setor Sul, Campus Universitário Senador Arthur Virgílio Filho, Bairro Coroado, CEP 69077-000, em Manaus/AM.

4.1.2.1 A empresa fornecedora deverá comunicar a Coordenação de Patrimônio sobre a entrega dos materiais com, no mínimo, 02 (dois) dias de antecedência, através do telefone (92) 3305-1187 ou pelo *e-mail* patrimonio@ufam.edu.br, possibilitando ao setor liberar e organizar o espaço destinado ao recebimento dos materiais no estoque.

4.2 Os bens serão recebidos provisoriamente no prazo de 07 (sete) dias pela Coordenação, responsável pelo acompanhamento e fiscalização do contrato, para efeito de posterior verificação de sua conformidade com as especificações constantes neste Termo de Referência e na proposta.

4.3 Os bens poderão ser rejeitados, no todo ou em parte, quando em desacordo com as especificações constantes neste Termo de Referência e na proposta, devendo ser substituídos no

prazo de 15 (quinze) dias, a contar da notificação da Contratada, às suas custas, sem prejuízo da aplicação das penalidades.

4.4 Os bens serão recebidos definitivamente no prazo de 15 (quinze) dias, contados do recebimento provisório, após a verificação da qualidade e quantidade do material e consequente aceitação mediante termo circunstanciado.

4.4.1 Na hipótese de a verificação a que se refere o subitem anterior não ser procedida dentro do prazo fixado, reputar-se-á como realizada, consumando-se o recebimento definitivo no dia do esgotamento do prazo.

4.5 O recebimento provisório ou definitivo do objeto não exclui a responsabilidade da contratada pelos prejuízos resultantes da incorreta execução do contrato.

4.6 Requisitos de Negócio:

4.6.1 Garantir a continuidade e disponibilidade dos serviços de segurança de comunicação;

4.6.2 Garantir a disponibilidade de suporte dos equipamentos e software incorporados na solução implantada;

4.6.3 Adquirir licenças para uso de hardware e software;

4.6.4 Garantir a correta instalação e funcionamento da solução a ser implantada.

4.7 Requisitos de Capacitação:

4.7.1 A CONTRATADA deverá ministrar treinamento nas dependências da CONTRATANTE com no mínimo de 40 (quarenta) horas;

4.7.2 O treinamento deverá ser ministrado por profissional certificado na solução implementada;

4.7.3 Deverá ser providenciado pela CONTRATADA material didático e certificado;

4.7.4 Todas as despesas de deslocamento serão por conta da CONTRATADA, ficando por conta da CONTRATANTE providenciar o ambiente de treinamento como sala, projetor, acesso à internet entre outros recursos necessários para a execução do treinamento;

4.7.5 Deverá ser ministrado conteúdo teórico e prático com laboratórios virtuais *hands-on*, como no mínimo 01 (um) laboratório virtual por participante;

4.7.6 Deverá ser considerado treinamento para até 10 (dez) participantes;

4.7.7 Deverá ser abordado, no mínimo, os seguintes tópicos:

4.7.7.1 Configurações iniciais;

4.7.7.2 Configurações de VLANs, LACP, DHCP e tipos NAT;

4.7.7.3 Políticas de segurança;

4.7.7.4 Prevenção de ameaças, anti-malware e filtro URL;

4.7.7.5 Identificação de usuários, qualidade de serviço e regras por aplicação;

4.7.7.6 Filtro de dados;

4.7.7.8 VPN *Site-to-Site* e *Client-To-Site*;

4.7.7.9 Alta disponibilidade;

4.7.7.10 Gerenciamento e relatórios.

4.8 Para itens de software, estes devem ser fornecidos com ou sem mídia de instalação. No caso de não fornecimento de mídia, deve ser indicado local para download do arquivo de instalação.

4.9 Requisitos de Segurança:

4.9.1 A CONTRATADA deverá fornecer garantia da solução adquirida, bem como, garantia de nível de acordo de serviço (SLA), observando os parâmetros de desempenho mínimo que devem ser garantidos pela CONTRATADA e conforme legislação em vigor.

4.10 Requisitos Sociais, Ambientais e Culturais

4.10.1 A aquisição da solução estará contribuindo para a melhoria da rede de comunicação e de dados da Instituição, que viabiliza aos acadêmicos, pesquisadores e professores melhores condições para realizar suas atividades.

4.11 Requisitos de Arquitetura Tecnológica:

4.11.1 Conforme disposto no item I do artigo 15 da Lei N°. 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.

4.12 Requisitos de Implantação:

4.12.1 Os equipamentos deverão ser novos e sem uso. Não serão aceitos equipamentos usados, remanufaturados ou de demonstração; Os equipamentos deverão ser entregues nas caixas lacradas pelo fabricante, não sendo aceitos equipamentos com caixas violadas;

4.12.2 A CONTRATANTE poderá efetuar consulta do número de série do equipamento, junto ao fabricante, informando data de compra e empresa adquirente, confirmando a procedência legal dos equipamentos;

4.12.3 A CONTRATANTE também poderá efetuar consulta junto aos órgãos competentes para certificar a legalidade do processo de importação;

4.12.4 O aceite do bem somente será dado após comprovação da entrega e o efetivo cumprimento de todas as exigências da presente especificação técnica.

4.13 Requisitos de Experiência Profissional:

4.13.1 A empresa deverá possuir, após a assinatura do contrato, pelo menos 2 (dois) profissionais com certificação técnica oficial do fabricante, compatível com o(s) objeto(s) deste processo, capaz de prestar o suporte em garantia e escalar o chamado ao fabricante conforme necessidade; No momento da habilitação deve ser indicado o nome e detalhes da certificação do profissional, incluindo comprovação; O técnico deverá ser contratado da empresa ou esta deverá emitir declaração com assinatura de ambos com promessa de contratação;

4.13.1.1 A empresa deverá possuir, após a assinatura do contrato pelo menos:

4.13.1.2 01 (um) profissional com conhecimentos na biblioteca ITIL (*Information Technology Infrastructure Library*) comprovados por certificação ITIL Foundation versão 3 ou superior;

4.13.1.3 01 (um) profissional PMP (*Project Management Professional*), certificados pelo PMI (*Project Management Institute*) ou versão superior;

4.13.1.4 As certificações requisitadas deverão estar válidas no momento da assinatura do contrato e durante todo o período de vigência do mesmo; Em caso de expiração de uma ou mais certificações durante o período vigente do contrato, a contratante poderá requerer que a CONTRATADA apresente os novos certificados atualizados no prazo máximo de 03 (três) meses após o vencimento.

4.14 Descrição Detalhada do Objeto: Firewall de Próxima Geração (NGFW)

4.14.1. Descrição Geral

4.14.1.1. 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 a internet compondo uma plataforma de segurança integrada e robusta;

4.14.1.2. Por plataforma de segurança entende-se hardware e software integrados do tipo *appliances*.

4.14.2. Capacidade e Quantidades

4.14.2.1. *Throughput* de 20 Gbps com a funcionalidade de controle de aplicação habilitada para todas as assinaturas que o fabricante possuir;

4.14.2.2. *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, Antispyware e Antimalware;

4.14.2.3. Os documentos públicos devem comprovar os throughputs aferidos com tráfego HTTP ou blend de protocolos definidos pelo fabricante como misto de aplicações. Não sendo aceitos números baseados em tráfego total do tipo UDP (User Datagram Protocol);

4.14.2.4. 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;

4.14.2.5. Não será aceito aceleração de pacotes na placa de rede limitando a análise somente até camada 4;

4.14.2.6. Suporte a, no mínimo, 3.800.000 de conexões simultâneas;

4.14.2.7. Suporte a, no mínimo, 110.000 novas conexões HTTP por segundo;

4.14.2.8. Fonte 120/240 AC, redundante e *hot-swappble*;

4.14.2.9. Disco *Solid State Drive* (SSD) redundante de, no mínimo, 240 GB;

4.14.2.10. Discos de, no mínimo, 2 TB em RAID 1 para armazenamento de logs interno ou externo a solução de *firewall*;

4.14.2.11. No mínimo, 04 (quatro) interfaces de rede 1 Gbps em portas cobre;

4.14.2.12. No mínimo, 16 (dezesseis) interfaces de rede 10 Gbps SFP+;

4.14.2.13. No mínimo, 04 (quatro) interfaces de rede 40 Gbps QSFP+;

4.14.2.14. 2 (duas) interfaces dedicadas para alta disponibilidade;

4.14.2.15. 1 (uma) interface de rede 1 Gbps dedicada para gerenciamento;

4.14.2.16. 1 (uma) interface do tipo console ou similar;

4.14.2.17. Suporte a, no mínimo, 60(sessenta) zonas de segurança;

4.14.2.18. Estar licenciada para ou suportar sem o uso de licença, 10.000 (dez mil) clientes de VPN SSL simultâneos;

4.14.2.19. Estar licenciada para ou suportar sem o uso de licença, 3.000 (três mil) túneis de VPN IPSEC simultâneos;

4.14.2.20. Deve suportar, no mínimo, 10 (dez) sistemas virtuais lógicos (Contextos) no *firewall* Físico;

4.14.2.21. Deve permitir expansão futura de, no mínimo, mais 10 (dez) sistemas virtuais lógicos (Contextos) no *firewall* Físico;

4.14.2.22. 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;

4.14.2.23. Por cada equipamento que compõe a plataforma de segurança, entende-se o hardware e as licenças de softwares necessárias para o seu funcionamento;

4.14.2.24. Por console de gerência e monitoração, entende-se as licenças de software necessárias para as duas funcionalidades, bem como hardware dedicado para o funcionamento das mesmas;

4.14.2.25. A console de gerência e monitoração podem residir no mesmo *appliance* de proteção de rede, desde que possuam recurso de CPU, memória, interface de rede e sistema operacional dedicados para esta função;

4.14.2.26. 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*.

4.14.3. Características Gerais

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

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

4.14.3.3. 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;

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

4.14.3.5. 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;

4.14.3.6. Todos os equipamentos fornecidos devem ser próprios para montagem em rack 19", incluindo kit tipo trilho para adaptação se necessário e cabos de alimentação. Deverá ser entregue junto de cada um dos appliances os seguintes módulos:

- 2 (dois) Módulos QSFP 40 Gigabit Ethernet padrão 40GBASE-LR4 para fibra monomodo até 10km;
- 2 (dois) Módulos SFP+ 10 Gigabit Ethernet padrão 10GBASE-LR para fibra monomodo até 10km;
- 4 (quatro) Cabos ópticos ativo do tipo AOC 10 Gigabit Ethernet SFP+ com no mínimo 10 metros compatível com a solução ofertada e com switches Extreme modelos BackDaimond-8810 e X460. A conectividade e fornecimento destes serão de responsabilidade da CONTRATADA.

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

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

4.14.3.8.1. Suporte a 4094 VLAN Tags 802.1q;

4.14.3.8.2. Agregação de links 802.3ad e LACP;

4.14.3.8.3. *Policy based routing* ou *policy based forwarding*;

4.14.3.8.4. Roteamento *multicast* (PIM-SM);

4.14.3.8.5. DHCP Relay;

4.14.3.8.6. DHCP Server;

4.14.3.8.7. Jumbo Frames;

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

4.14.3.9. Suportar sub-interfaces ethernet lógicas;

4.14.3.9.1. Suporte a, no mínimo, 15 (quinze) roteadores virtuais na mesma instância de *firewall*;

4.14.3.10. 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;

4.14.3.11. Deve suportar os seguintes tipos de NAT:

4.14.3.11.1. Nat dinâmico (Many-to-1);

4.14.3.11.2. Nat dinâmico (Many-to-Many);

4.14.3.11.3. Nat estático (1-to-1);

4.14.3.11.4. NAT estático (Many-to-Many);

4.14.3.11.5. Nat estático bidirecional 1-to-1;

4.14.3.11.6. Tradução de porta (PAT);

4.14.3.11.7. NAT de Origem;

4.14.3.11.8. NAT de Destino;

4.14.3.11.9. Suportar NAT de Origem e NAT de Destino simultaneamente;

4.14.3.11.10. Deve implementar *Network Prefix Translation* (NPTv6), prevenindo problemas de roteamento assimétrico;

4.14.3.12. Deve implementar o protocolo ECMP;

4.14.3.12.1. Deve implementar balanceamento de link por *hash* do IP de origem;

4.14.3.12.2. Deve implementar balanceamento de link por *hash* do IP de origem e destino;

4.14.3.12.3. Deve implementar balanceamento de link através do método *round-robin*;

4.14.3.12.4. Deve implementar balanceamento de link por peso. Nesta opção deve ser possível definir o percentual de tráfego que será escoado por cada um dos links. Deve suportar o balanceamento de, no mínimo, quarto links;

4.14.3.12.5. Deve implementar balanceamento de link através de políticas por usuário e grupos de usuários do LDAP/AD;

4.14.3.12.6. Deve implementar balanceamento de link através de políticas por aplicação e porta de destino;

4.14.3.12.7. Deve implementar o protocolo *Link Layer Dicovery* (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;

4.14.3.12.8. Enviar log para sistemas de monitoração externos, simultaneamente;

4.14.3.12.9. Deve haver a opção de enviar logs para os sistemas de monitoração externos via protocolo TCP e SSL;

4.14.3.12.10. Deve permitir configurar certificado caso necessário para autenticação no sistema de monitoração externo de logs;

4.14.3.12.11. Proteção contra anti-spoofing;

4.14.3.12.12. Deve permitir bloquear sessões TCP que usarem variações do 3-way hand-shake, como 4 way e 5 way split hand-shake, prevenindo desta forma possíveis tráfegos maliciosos;

4.14.3.12.13. Deve permitir bloquear conexões que contenham dados no payload de pacotes TCP-SYN e SYN-ACK durante o three-way handshake;

4.14.3.12.14. 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;

4.14.3.12.15. Para IPv4, deve suportar roteamento estático e dinâmico (RIPv2, BGP e OSPFv2);

4.14.3.12.16. Para IPv6, deve suportar roteamento estático e dinâmico (OSPFv3);

4.14.3.12.17. Suportar a OSPF *graceful restart*;

4.14.3.12.18. Deve suportar o protocolo MP-BGP (Multiprotocol BGP) permitindo que o *firewall* possa anunciar rotas *multicast* para IPv4 e rotas *unicast* para IPv6;

4.14.3.12.19. 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 (RDNSS), DNS Search List (DNSSL) e controle de aplicação;

4.14.3.12.20. 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);

4.14.3.12.20.1. Modo *Sniffer*, para inspeção via porta espelhada do tráfego de dados da rede;

4.14.3.12.20.2. Modo Camada – 2 (L2), para inspeção de dados em linha e ter visibilidade e controle do tráfego em nível de aplicação;

4.14.3.12.20.3. 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;

4.14.3.12.21. Modo misto de trabalho Sniffer, L2 e L3 em diferentes interfaces físicas;

4.14.3.13. Suporte a configuração de alta disponibilidade Ativo/Passivo e Ativo/Ativo:

4.14.3.13.1. Em modo transparente;

4.14.3.13.2. Em layer 3;

4.14.3.14. A configuração em alta disponibilidade deve sincronizar:

4.14.3.14.1. Sessões;

4.14.3.14.2. Configurações, incluindo, mas não limitado a políticas de Firewall, NAT, QOS e objetos de rede;

4.14.3.14.3. Certificados descriptografados;

4.14.3.14.4. Associações de Segurança das VPNs;

4.14.3.14.5. Tabelas FIB;

4.14.3.14.6. O HA (modo de Alta-Disponibilidade) deve possibilitar monitoração de falha de link;

4.14.3.15. 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.

4.14.4. Controle Por Política de *Firewall*

4.14.4.1. Deverá suportar controles por zona de segurança;

4.14.4.2. Controles de políticas por porta e protocolo;

4.14.4.3. Controle de políticas por aplicações grupos estáticos de aplicações, grupos dinâmicos de aplicações (baseados em características e comportamento das aplicações) e categorias de aplicações;

4.14.4.4. Controle de políticas por usuários, grupos de usuários, IPs, redes e zonas de segurança;

4.14.4.5. 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;

4.14.4.5.1. Deve permitir autenticação segura através de certificado nas fontes externas de endereços IP, domínios e URLs;

4.14.4.5.2. Deve permitir consultar e criar exceção para objetos das listas externas a partir da interface de gerência do próprio *firewall*;

4.14.4.6. Controle de políticas por código de País (Por exemplo: BR, USA, UK, RUS);

4.14.4.7. Controle, inspeção e decriptografia de SSL por política para tráfego de entrada (*Inbound*) e Saída (*Outbound*);

4.14.4.8. Deve suportar *offload* de certificado em inspeção de conexões SSL de entrada (*Inbound*);

4.14.4.9. Deve descriptografar tráfego *Inbound* e *Outbound* em conexões negociadas com TLS 1;2;

4.14.4.10. Deve decriptografar sites e aplicações que utilizam certificados ECC, incluindo *Elliptical Curve Digital Signature Algorithm* (ECDSA);

4.14.4.11. Controle de inspeção e decriptografia de SSH por política;

4.14.4.12. A decriptografia 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;

4.14.4.13. A plataforma de segurança deve implementar espelhamento de tráfego descriptografado (SSL e TLS) para soluções externas de análise (Forense de rede, DLP, Análise de Ameaças, entre outras);

4.14.4.13.1. É permitido uso de *appliance* externo, específico para a decriptografia de (SSL e TLS), com espelhamento de cópia do tráfego descriptografado tanto para o *firewall*, quanto para as soluções de análise;

4.14.4.14. Bloqueios dos seguintes tipos de arquivos: bat, cab, dll, exe, pif e reg;

4.14.4.15. Traffic shaping QoS baseado em Políticas (Prioridade, Garantia e Máximo)

4.14.4.16. QoS baseado em políticas para marcação de pacotes (diffserv marking), inclusive por aplicações;

4.14.4.17. Suporte a objetos e regras IPV6;

4.14.4.18. Suporte a objetos e regras *multicast*;

4.14.4.19. 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;

4.14.4.20. Suportar a atribuição de agendamento as políticas com o objetivo de habilitar e desabilitar políticas em horários pré-definidos automaticamente.

4.14.5. Controle de Aplicações

4.14.5.1. Os dispositivos de proteção de rede deverão possuir a capacidade de reconhecer aplicações, independente de porta e protocolo, com as seguintes funcionalidades:

4.14.5.1.1. Deve ser possível a liberação e bloqueio somente de aplicações sem a necessidade de liberação de portas e protocolos;

4.14.5.1.2. Reconhecer pelo menos 1700 aplicações diferentes, incluindo, mas não limitado: a tráfego relacionado a peer-to-peer, redes sociais, acesso remoto, *update* de software, protocolos de rede, voip, áudio, vídeo, proxy, mensageiros instantâneos, compartilhamento de arquivos, e-mail;

4.14.5.1.3. Reconhecer pelo menos as seguintes aplicações: bittorrent, gnutella, skype, facebook, linked-in, twitter, citrix, logmein, teamviewer, ms-rdp, vnc, gmail, youtube, http-proxy, http-tunnel, facebook chat, gmail chat, whatsapp, 4shared, dropbox, google drive, skydrive, db2, mysql, oracle, active directory, kerberos, ldap, radius, itunes, dhcp, ftp, dns, wins, msrpc, ntp, snmp, rpc over http, gotomeeting, webex, evernote, google-docs, etc;

4.14.5.1.4. 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;

4.14.5.1.5. 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;

4.14.5.1.6. 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;

4.14.5.1.7. 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;

4.14.5.1.8. 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;

4.14.5.1.9. Deve permitir a utilização de aplicativos para um determinado grupo de usuário e bloquear para o restante, incluindo, mas não limitado a Skype. Deve permitir também a criação de políticas de exceção concedendo o acesso a aplicativos como Skype apenas para alguns usuários;

4.14.5.1.10. Deve permitir habilitar aplicações SAAS apenas no modo corporativo e bloqueá-las quando usadas no modo pessoal, tais como: Office 365, Skype, aplicativos google, gmail, etc;

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

4.14.5.1.12. Atualizar a base de assinaturas de aplicações automaticamente;

4.14.5.1.13. Reconhecer aplicações em IPv6;

4.14.5.1.14. Limitar a banda (download/upload) usada por aplicações (traffic shaping), baseado no IP de origem, usuários e grupos do LDAP/AD;

4.14.5.1.15. 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;

4.14.5.1.16. 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;

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

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

4.14.5.1.19. 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;

4.14.5.1.20. 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:

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

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

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

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

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

4.14.5.1.24.1. 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 a aplicação por, pelo menos, os últimos 30 dias e o primeiro e último registro de log de cada aplicação trafegada por esta determinada regra;

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

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

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

4.14.5.1.26. Deve possibilitar a diferenciação de tráfegos de Instant Messaging (AIM, Gtalk, Facebook Chat, etc;) possuindo granularidade de controle/políticas para os mesmos;

4.14.5.1.27. Deve possibilitar a diferenciação e controle de partes das aplicações como por exemplo permitir o Gtalk chat e bloquear a transferência de arquivos;

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

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

4.14.5.1.29.1. Tecnologia utilizada nas aplicações (Client-Server, Browser Based, Network Protocol, etc);

4.14.5.1.29.2. Nível de risco da aplicação;

4.14.5.1.29.3. Categoria e subcategoria de aplicações;

4.14.5.1.29.4. Aplicações que usem técnicas evasivas, utilizadas por *malwares*, como transferência de arquivos e/ou uso excessivo de banda, etc.

4.14.6. Prevenção de Ameaças

4.14.6.1. Para proteção do ambiente contra ataques, os dispositivos de proteção devem possuir módulo de IPS, Antivírus e Anti-Spyware integrados no próprio *appliance* de Firewall ou entregue através de composição com outro equipamento ou fabricante;

4.14.6.2. Deve incluir assinaturas de prevenção de intrusão (IPS) e bloqueio de arquivos maliciosos (Antivírus e Anti-Spyware);

4.14.6.3. As funcionalidades de IPS, Antivírus e Anti-Spyware devem operar em caráter permanente, podendo ser utilizadas por tempo indeterminado, mesmo que não subsista o direito de receber atualizações ou que não haja contrato de garantia de software com o fabricante;

4.14.6.4. Deve sincronizar as assinaturas de IPS, Antivírus, Anti-Spyware quando implementado em alta disponibilidade ativo/ativo e ativo/passivo;

4.14.6.5. Deve implementar os seguintes tipos de ações para ameaças detectadas pelo IPS e Antispyware: permitir, permitir e gerar log, bloquear, bloquear IP do atacante por um intervalo de tempo e enviar *tcp-reset*;

4.14.6.6. Deve possuir a capacidade de detectar e prevenir contra ameaças em tráfegos HTTP/2;

4.14.6.7. As assinaturas devem poder ser ativadas ou desativadas, ou ainda habilitadas apenas em modo de monitoração;

4.14.6.8. Exceções por IP de origem ou de destino devem ser possíveis nas regras, de forma geral e assinatura a assinatura;

4.14.6.9. Deve suportar granularidade nas políticas de IPS Antivírus e Anti-Spyware, possibilitando a criação de diferentes políticas por zona de segurança, endereço de origem, endereço de destino, serviço e a combinação de todos esses itens;

4.14.6.10. Deve permitir o bloqueio de vulnerabilidades;

4.14.6.11. Deve permitir o bloqueio de *exploits* conhecidos;

4.14.6.12. Deve incluir proteção contra ataques de negação de serviços;

4.14.6.13. Deve suportar a inspeção e criação de regras de proteção de DOS e QOS para o conteúdo de tráfego tunelado pelo protocolo GRE;

4.14.6.14. Deverá possuir os seguintes mecanismos de inspeção de IPS:

4.14.6.14.1. Análise de padrões de estado de conexões;

4.14.6.14.2. Análise de decodificação de protocolo;

4.14.6.14.3. Análise para detecção de anomalias de protocolo;

4.14.6.14.4. Análise heurística;

4.14.6.14.5. IP Defragmentation;

4.14.6.14.6. Remontagem de pacotes de TCP;

4.14.6.14.7. Bloqueio de pacotes malformados;

4.14.6.15. Ser imune e capaz de impedir ataques básicos como: Synflood, ICMPflood, UDPfloof, etc;

4.14.6.16. Detectar e bloquear a origem de *portscans* com possibilidade de criar exceções para endereços IPs de ferramentas de monitoramento da organização;

4.14.6.17. Bloquear ataques efetuados por *worms* conhecidos, permitindo ao administrador acrescentar novos padrões;

4.14.6.18. Suportar os seguintes mecanismos de inspeção contra ameaças de rede: análise de padrões de estado de conexões, análise de decodificação de protocolo, análise para detecção de anomalias de protocolo, análise heurística, IP Defragmentation, remontagem de pacotes de TCP e bloqueio de pacotes malformados;

4.14.6.19. Possuir assinaturas específicas para a mitigação de ataques DoS e DDoS;

4.14.6.20. Possuir assinaturas para bloqueio de ataques de *buffer overflow*;

4.14.6.21. Deverá possibilitar a criação de assinaturas customizadas pela interface gráfica do produto;

4.14.6.22. Deve permitir usar operadores de negação na criação de assinaturas customizadas de IPS e *anti-spyware*, permitindo a criação de exceções com granularidade nas configurações;

4.14.6.23. Permitir o bloqueio de vírus e *spywares* em, pelo menos, os seguintes protocolos: HTTP, FTP, SMB, SMTP e POP3;

4.14.6.23.1. É permitido uso de *appliance* externo (antivírus de rede), para o bloqueio de vírus e *spywares* em protocolo SMB de forma a conter *malwares* se espalhando horizontalmente pela rede;

4.14.6.24. Suportar bloqueio de arquivos por tipo;

4.14.6.25. Identificar e bloquear comunicação com *botnets*;

4.14.6.26. Deve suportar várias técnicas de prevenção, incluindo Drop e tcp-rst (Cliente, Servidor e ambos);

4.14.6.27. Deve suportar referência cruzada com CVE;

4.14.6.28. Registrar na console de monitoração as seguintes informações sobre ameaças identificadas:

4.14.6.28.1. O nome da assinatura ou do ataque, aplicação, usuário, origem e o destino da comunicação, além da ação tomada pelo dispositivo;

4.14.6.29. Deve suportar a captura de pacotes (PCAP), por assinatura de IPS e *Antispyware*;

4.14.6.30. Deve permitir que na captura de pacotes por assinaturas de IPS e *Antispyware* seja definido o número de pacotes a serem capturados. Esta captura deve permitir selecionar, no mínimo, 50 pacotes;

4.14.6.31. Deve possuir a função resolução de endereços via DNS, para que conexões com destino a domínios maliciosos sejam resolvidas pelo Firewall com endereços (IPv4 e IPv6), previamente definidos;

4.14.6.32. Permitir o bloqueio de vírus, pelo menos, nos seguintes protocolos: HTTP, FTP, SMB, SMTP e POP3;

4.14.6.33. Os eventos devem identificar o país de onde partiu a ameaça;

4.14.6.34. Deve incluir proteção contra vírus em conteúdo HTML e Java script, software espião (spyware) e worms;

4.14.6.35. Proteção contra downloads involuntários usando HTTP de arquivos executáveis; maliciosos;

4.14.6.36. Rastreamento de vírus em pdf;

4.14.6.37. Deve permitir a inspeção em arquivos comprimidos que utilizam o algoritmo deflate (zip, gzip, etc;)

4.14.6.38. Deve ser possível a configuração de diferentes políticas de controle de ameaças e ataques baseado em políticas do *firewall* considerando Usuários, Grupos de usuários, origem, destino, zonas de segurança, etc, ou seja, cada regra de *firewall* poderá ter uma configuração diferentes de IPS, sendo essas políticas por Usuários, Grupos de usuário, origem, destino, zonas de segurança.

4.14.7. Análise de *Malwares* Modernos

4.14.7.1. Devido aos *Malwares* hoje em dia serem muito dinâmicos e um antivírus 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;

4.14.7.2. 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;

4.14.7.3. 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;

4.14.7.4. 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 deixa o sistema operacional lento, que alteram parâmetros do sistema, etc;

4.14.7.5. Suportar a análise com pelo menos 100 (cem) tipos de comportamentos maliciosos para a análise da ameaça não conhecida;

4.14.7.6. Suportar a análise de arquivos maliciosos em ambiente controlado com, no mínimo, sistema operacional Windows XP e Windows 7;

4.14.7.7. 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;

4.14.7.8. 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 *sand-box* o identifique como site hospedeiro de *exploits*;

4.14.7.9. A análise de links em *sand-box* deve ser capaz de classificar sites falsos na categoria de *phishing* e atualizar a base de filtro de URL da solução;

4.14.7.10. 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;

4.14.7.11. 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);

4.14.7.12. 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*;

4.14.7.13. Deve permitir exportar o resultado das análises de *malwares* de dia Zero em PDF e CSV a partir da própria interface de gerência;

4.14.7.14. Deve permitir o download dos *malwares* identificados a partir da própria interface de gerência;

4.14.7.15. Deve permitir visualizar os resultados das análises de *malwares* de dia zero nos diferentes sistemas operacionais suportados;

4.14.7.16. 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;

4.14.7.17. Caso a solução seja fornecida em *appliance* local, deve possuir, no mínimo, 28 ambientes controlados (*sand-box*) independentes para execução simultânea de arquivos suspeitos;

4.14.7.18. Caso sejam necessárias licenças de sistemas operacional e softwares para execução de arquivos no ambiente controlado (*sand-box*), as mesmas devem ser fornecidas em sua totalidade, sem custos adicionais para a contratante;

4.14.7.19. Suportar a análise de arquivos executáveis, DLLs, ZIP e criptografados em SSL no ambiente controlado;

4.14.8. Filtro de URL

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

4.14.8.1.1. 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);

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

4.14.8.1.3. 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;

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

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

4.14.8.1.6. Deve 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;

4.14.8.1.7. Suporte base ou cache de URLs local no *appliance*, evitando *delay* de comunicação/validação das URLs;

4.14.8.1.8. Possui pelo menos 60 categorias de URLs;

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

4.14.8.1.10. Deve possuir categoria específica para classificar domínios recém registrados (com menos de 32 dias);

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

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

4.14.8.1.13. Suporta a criação categorias de URLs customizadas;

4.14.8.1.14. Suporta a exclusão de URLs do bloqueio, por categoria;

4.14.8.1.15. Permite a customização de página de bloqueio;

4.14.8.1.16. 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;

4.14.8.1.17. 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;

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

4.14.8.1.19. Suporta a inclusão nos logs do produto de informações das atividades dos usuários;

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

4.14.9. Identificação de Usuários

4.14.9.1. 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;

4.14.9.2. Deve possuir integração com Microsoft Active Directory para identificação de usuários e grupos permitindo granularidade de controle/políticas baseadas em usuários e grupos de usuários;

4.14.9.3. Deve possuir integração com Radius para identificação de usuários e grupos permitindo granularidade de controle/políticas baseadas em usuários e grupos de usuários;

4.14.9.4. 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;

4.14.9.5. Deve possuir integração com LDAP para identificação de usuários e grupos permitindo granularidade de controle/políticas baseadas em Usuários e Grupos de usuários;

4.14.9.5.1. 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;

4.14.9.6. 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);

4.14.9.7. Suporte a autenticação Kerberos;

4.14.9.8. Deve suportar autenticação via Kerberos para administradores da plataforma de segurança, captive Portal e usuário de VPN SSL;

4.14.9.9. Deve possuir suporte a identificação de múltiplos usuários conectados em um mesmo endereço IP em ambientes Citrix e Microsoft Terminal Server, permitindo visibilidade e controle granular por usuário sobre o uso das aplicações que estão nestes serviços;

4.14.9.10. Deve identificar usuários através de leitura do campo x-fowarded-for, populando nos logs do *firewall* o endereço IP, bem como o usuário de rede responsável pelo acesso;

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

4.14.9.12. 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 a organização;

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

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

4.14.10. QoS

4.14.10.1. Com a finalidade de controlar aplicações e tráfego cujo consumo possa ser excessivo, (como youtube, ustream, etc) e ter um alto consumo de largura de banda, se requer que a solução, além de poder permitir ou negar esse tipo de aplicações, deve ter a capacidade de controlá-las por políticas de máximo de largura de banda quando forem solicitadas por diferentes usuários ou aplicações, tanto de áudio como de vídeo *streaming*;

4.14.10.2. Suportar a criação de políticas de QoS por:

4.14.10.2.1. Endereço de origem

4.14.10.2.2. Endereço de destino

4.14.10.2.3. Por usuário e grupo do LDAP/AD;

4.14.10.2.4. Por aplicações, incluindo, mas não limitado a Skype, Bittorrent, YouTube e Azureus;

4.14.10.2.5. Por porta;

4.14.10.3. O QoS deve possibilitar a definição de classes por:

4.14.10.3.1. Banda Garantida

4.14.10.3.2. Banda Máxima

4.14.10.3.3. Fila de Prioridade;

4.14.10.4. Suportar priorização RealTime de protocolos de voz (VoIP) como H;323, SIP, SCCP, MGCP e aplicações como Skype;

4.14.10.5. Suportar marcação de pacotes Diffserv, inclusive por aplicação;

4.14.10.6. 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 (*inboud* e *outbound*);

4.14.10.7. Disponibilizar estatísticas Real Time para classes de QoS;

4.14.10.8. Deve suportar QoS (*traffic-shapping*), em interface agregadas;

4.14.10.9. Deverá permitir o monitoramento do uso que as aplicações fazem por bytes, sessões e por usuário.

4.14.11. Filtro de Dados

4.14.11.1. Permite a criação de filtros para arquivos e dados pré-definidos;

4.14.11.2. Os arquivos devem ser identificados por extensão e assinaturas;

4.14.11.3. Permite identificar e opcionalmente prevenir a transferência de vários tipos de arquivos (MS Office, PDF, etc) identificados sobre aplicações (P2P, InstantMessaging, SMB, etc);

4.14.11.4. Suportar identificação de arquivos compactados e a aplicação de políticas sobre o conteúdo desses tipos de arquivos;

4.14.11.5. 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;

4.14.11.6. Permitir listar o número de aplicações suportadas para controle de dados;

4.14.11.7. Permitir listar o número de tipos de arquivos suportados para controle de dados.

4.14.12. Geolocalização

4.14.12.1. Suportar a criação de políticas por Geolocalização, permitindo o tráfego de determinado País/Países sejam bloqueados;

4.14.12.2. Deve possibilitar a visualização dos países de origem e destino nos logs dos acessos;

4.14.12.3. Deve permitir visualizar nos logs e criar políticas para liberar e bloquear tráfego de países por: tipo de arquivo, aplicação e categoria de URL;

4.14.12.4. Deve possibilitar a criação de regiões geográficas pela interface gráfica e criar políticas utilizando as mesmas.

4.14.13. VPN

4.14.13.1. Suportar VPN Site-to-Site e Client-To-Site;

4.14.13.2. Suportar IPSec VPN;

4.14.13.3. Suportar SSL VPN;

4.14.13.4. A VPN IPSEc deve suportar:

4.14.13.4.1. 3DES;

4.14.13.4.2. Autenticação MD5 e SHA-1;

4.14.13.4.3. Diffie-Hellman Group 1, Group 2, Group 5 e Group 14;

4.14.13.4.4. Algoritmo Internet Key Exchange (IKEv1 e v2);

4.14.13.4.5. AES 128, 192 e 256 (Advanced Encryption Standard)

4.14.13.4.6. Autenticação via certificado IKE PKI;

4.14.13.5. Deve possuir interoperabilidade com os seguintes fabricantes:

4.14.13.5.1. Cisco;

4.14.13.5.2. Checkpoint;

4.14.13.5.3. Juniper;

4.14.13.5.4. Palo Alto Networks;

4.14.13.5.5. Fortinet;

4.14.13.5.6. Sonic Wall;

4.14.13.6. 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;

4.14.13.7. A VPN SSL deve suportar:

4.14.13.7.1. O usuário realizar a conexão por meio de cliente instalado no sistema operacional do equipamento ou por meio de interface WEB;

4.14.13.7.2. A funcionalidades de VPN SSL devem ser atendidas com ou sem o uso de agente;

4.14.13.7.3. Atribuição de endereço IP nos clientes remotos de VPN SSL;

4.14.13.7.4. Deve permitir a atribuição de IPs fixos nos usuários remotos de VPN SSL;

4.14.13.7.5. 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;

4.14.13.7.6. 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*;

4.14.13.7.7. Atribuição de DNS nos clientes remotos de VPN;

4.14.13.7.8. Deve permitir que seja definido métodos de autenticação distintos por sistema operacional do dispositivo remoto de VPN (Android, IOS, Mac, Windows e Chrome OS);

4.14.13.7.9. A solução de VPN deve verificar se o cliente que está conectado é o mesmo para o qual o certificado foi emitido inicialmente; O acesso deve ser bloqueado caso o dispositivo não seja o correto;

4.14.13.7.10. Deve possuir lista de bloqueio para dispositivos que forem reportados com roubado ou perdido pelo usuário;

4.14.13.7.11. Deve haver a opção de ocultar o agente de VPN instalado no cliente remoto, tornando o mesmo invisível para o usuário;

4.14.13.7.12. 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;

4.14.13.7.13. 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;

4.14.13.7.14. Deve permitir criar políticas de controle de aplicações, IPS, Antivírus, Antipyware e filtro de URL para tráfego dos clientes remotos conectados na VPN SSL;

4.14.13.7.15. A VPN SSL deve suportar proxy arp e uso de interfaces PPPOE;

4.14.13.7.16. Suportar autenticação via AD/LDAP, OTP (One Time Password), certificado e base de usuários local;

4.14.13.7.17. Deve permitir a distribuição de certificado para o usuário de remoto através do portal de VPN de forma automatizada;

4.14.13.7.18. Deve possuir lista de bloqueio para dispositivos em casos quando, por exemplo, o usuário reportar que o dispositivo foi perdido ou roubado;

4.14.13.7.19. 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;

4.14.13.7.20. Suporta leitura e verificação de CRL (certificate revocation list);

4.14.13.7.21. Permite a aplicação de políticas de segurança e visibilidade para as aplicações que circulam dentro dos túneis SSL;

4.14.13.7.22. 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;

4.14.13.7.23. O agente deverá comunicar-se com o portal para determinar as políticas de segurança do usuário,

4.14.13.7.24. Deve permitir que a conexão com a VPN SSL seja estabelecida das seguintes formas:

4.14.13.7.24.1. Antes do usuário autenticar na estação;

4.14.13.7.24.2. Após autenticação do usuário na estação;

4.14.13.7.24.3. Sob demanda do usuário;

4.14.13.7.25. Deve manter uma conexão segura com o portal durante a sessão;

4.14.13.7.26. O agente de VPN SSL *client-to-site* deve ser compatível com pelo menos: Windows XP, Vista Windows 7, Windows 8, Mac OSx e Chrome OS;

4.14.13.7.27. 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;

4.14.13.7.28. Deve haver a opção do 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;

4.14.13.7.29. Deve possuir a capacidade de identificar se a origem da conexão de VPN é externa ou interna.

4.15. Solução de Gerenciamento Centralizado

4.15.1. Descrição Geral

4.15.1.1. Solução de Gerenciamento Centralizado para plataforma de segurança;

4.15.1.2. Deve ser fornecido solução de gerenciamento centralizado, possibilitando o gerenciamento de pelo menos 2 (dois) equipamentos de *firewall*;

4.15.1.3. A fim de garantir total compatibilidade entre os sistemas a Solução de Gerenciamento Centralizado deverá ser compatível com a Soluções de Next Generation Firewall (NGFW);

4.15.1.4. O gerenciamento centralizado poderá ser entregue com appliance físico ou virtual;

4.15.1.5. No caso de fornecimento de *appliance* físico o mesmo deverá possuir:

4.15.1.5.1. Acessórios para montagem em rack 19 polegadas;

4.15.1.5.2. No mínimo, 2 interfaces 1000Base-T com conectores RJ-45;

4.15.1.5.3. Discos redundantes com espaço de armazenamento para logs de pelo menos 2TB;

4.15.1.5.4. Possuir fonte de energia AC redundante com ajuste automático de tensão para operação nas tensões de 100 a 240-VAC/60 Hz;

4.15.1.5.5. Ser fornecido com todos acessórios necessários para sua instalação;

4.15.1.6. Caso seja entregue em *appliance* virtual deve ser compatível com VMware ESXi;

4.15.1.7. O gerenciamento da solução deve possibilitar a coleta de estatísticas de todo o tráfego que passar pelos equipamentos da plataforma de segurança;

4.15.1.8. Controle sobre todos os equipamentos da plataforma de segurança em uma única console, com administração de privilégios e funções;

4.15.1.9. Deve permitir controle global de políticas para todos os equipamentos que compõe a plataforma de segurança;

4.15.1.10. Deve suportar organizar os dispositivos administrados em grupos: os sistemas virtuais devem ser administrados como dispositivos individuais, os grupos podem ser geográficos, por funcionalidade (por exemplo, IPS), e distribuição;

4.15.1.11. Deve implementar sistema de hierarquia entre os *firewalls* gerenciados, onde seja possível aplicar configurações de forma granular em grupos de *firewalls*;

4.15.1.12. Deve implementar a criação de perfis de usuários com acesso a plataforma de gerenciamento com definição exata de quais informações e de quais *firewalls* e grupos de *firewalls* o usuário terá acesso referente a logs e relatórios;

4.15.1.13. Deve permitir a criação de objetos e políticas compartilhadas;

4.15.1.14. Deve consolidar logs e relatórios de todos os dispositivos administrados;

4.15.1.15. Deve permitir que exportar backup de configuração automaticamente via agendamento;

4.15.1.16. Deve permitir que a configuração dos *firewalls* seja importada de forma automática na plataforma de gerenciamento centralizado e que possa ser usada em outros *firewalls* e grupos de *firewalls*;

4.15.1.17. Deve mostrar os status dos *firewalls* em alta disponibilidade a partir da plataforma de gerenciamento centralizado;

4.15.1.18. Centralizar a administração de regras e políticas do cluster, usando uma única interface de gerenciamento;

4.15.1.19. O gerenciamento da solução deve suportar acesso via SSH, cliente ou WEB (HTTPS) e API aberta;

4.15.1.20. Deve permitir substituir o certificado de fábrica no acesso HTTPS a gerência do *firewall* como possibilidade de uso de certificado criado localmente na própria solução ou importado de fonte externa;

4.15.1.21. Caso haja a necessidade de instalação de cliente para administração da solução o mesmo deve ser compatível com sistemas operacionais Windows e Linux;

4.15.1.22. O gerenciamento deve permitir/possuir:

4.15.1.22.1. Criação e administração de políticas de *firewall* e controle de aplicação;

4.15.1.22.2. Criação e administração de políticas de IPS, Antivírus e Anti-Spyware;

4.15.1.22.3. Criação e administração de políticas de Filtro de URL;

4.15.1.22.4. Monitoração de logs;

4.15.1.22.5. Ferramentas de investigação de logs;

4.15.1.22.6. Debugging;

4.15.1.22.7. Captura de pacotes;

4.15.1.23. Acesso concorrente de administradores;

4.15.1.24. Deve permitir que administradores concorrentes façam modificações, valide configurações e reverta configurações do *firewall* simultaneamente e que cada administrador consiga aplicar apenas as suas alterações de forma independente das realizadas por outro administrador;

4.15.1.25. Deve mostrar ao administrador do *firewall* a hora e data do último login e tentativas de login com falha para acessos a partir da interface gráfica e CLI;

4.15.1.26. Deve possuir mecanismo busca global na solução onde possa se consultar por uma string tais como: nome de objetos, ID ou nome de ameaças, nome de aplicações, nome de políticas, endereços IPs, permitindo a localização e uso dos mesmo na configuração do dispositivo;

4.15.1.27. Deve possuir um mecanismo de busca por comandos no gerenciamento via SSH, facilitando a localização de comandos;

4.15.1.28. Deve permitir usar palavras chaves e cores para facilitar identificação de regras;

4.15.1.29. Deve permitir monitorar via SNMP falhas de hardware, inserção ou remoção de fontes, discos e *coolers*, uso de recursos por número elevado de sessões, número de túneis estabelecidos na VPN client-to-site, porcentagem de utilização em referência ao número total suportado/licenciado e número de sessões estabelecidas, estatísticas/taxa de logs, uso de disco, período de retenção dos logs e status do envio de logs para soluções externas;

4.15.1.30. Deve suportar também o monitoramento dos seguintes recursos via SNMP: IP *fragmentation*, TCP *state* e *dropped packets*;

4.15.1.31. Bloqueio de alterações, no caso acesso simultâneo de dois ou mais administradores;

4.15.1.32. Definição de perfis de acesso à console com permissões granulares como: acesso de escrita, acesso de leitura, criação de usuários, alteração de configurações;

4.15.1.33. Autenticação integrada ao Microsoft Active Directory e servidor Radius;

4.15.1.34. Localização de em quais regras um endereço IP, IP Range, *subnet* ou objetos estão sendo utilizados;

4.15.1.35. Deve atribuir sequencialmente um número a cada regra de *firewall*, NAT, QoS e regras de DOS;

4.15.1.36. Criação de regras que fiquem ativas em horário definido;

4.15.1.37. Criação de regras com data de expiração;

4.15.1.38. Backup das configurações e *rollback* de configuração para a última configuração salva;

4.15.1.39. Suportar *Rollback* de Sistema Operacional para a última versão local;

4.15.1.40. Habilidade de upgrade via SCP, TFTP e interface de gerenciamento;

4.15.1.41. Deve possuir mecanismo de análise de impacto na política de segurança antes de atualizar a base com novas aplicações disponibilizadas pelo fabricante;

4.15.1.42. Validação de regras antes da aplicação;

4.15.1.43. Deve implementar mecanismo de validação de configurações antes da aplicação das mesmas permitindo identificar erros, tais como: rota de destino inválida, regras em *shadowing* etc;

4.15.1.43.1. É permitido o uso de *appliance* externo para permitir a validação de regras antes da aplicação;

4.15.1.44. Validação das políticas, avisando quando houver regras que, ofusquem ou conflitem com outras (*shadowing*);

4.15.1.44.1. É permitido o uso de *appliance* externo para permitir a validação de políticas, avisando quando houver regras que, ofusquem ou conflitem com outras (*shadowing*);

4.15.1.45. Deve possibilitar a visualização e comparação de configurações Atuais, configuração anterior e configurações antigas;

4.15.1.46. Deve permitir auditar regras de segurança exibindo quadro comparativo das alterações de uma regra em relação a versão anterior;

4.15.1.47. Deve possibilitar a integração com outras soluções de SIEM de mercado (third-party SIEM vendors)

4.15.1.48. Geração de logs de auditoria detalhados, informando a configuração realizada, o administrador que a realizou e o horário da alteração;

4.15.1.49. Deverá ter a capacidade de gerar um relatório gráfico que permita visualizar as mudanças na utilização de aplicações na rede no que se refere a um período de tempo anterior, para permitir comparar os diferentes consumos realizados pelas aplicações no tempo presente com relação ao passado;

4.15.1.50. Geração de relatórios com mapas geográficos gerados em tempo real para a visualização de origens e destinos do tráfego gerado na instituição;

4.15.1.51. Deve prover relatórios com visão correlacionada de aplicações, ameaças (IPS, Antivírus e Anti-Spware), URLs e filtro de arquivos, para melhor diagnóstico e resposta a incidentes;

4.15.1.52. Deve permitir a criação de *Dash Boards* customizados para visibilidades do tráfego de aplicativos, usuários, categorias de URL, ameaças identificadas pelo IPS, antivírus, anti-spyware, *malwares* "Zero Day" detectados em *sand-box* e tráfego bloqueado;

4.15.1.53. O gerenciamento da solução deve possibilitar a coleta de estatísticas de todo o tráfego que passar pelos dispositivos de segurança;

4.15.1.54. Dever permitir a visualização dos logs de *malwares* modernos, tráfego (IP de origem, destino, usuário e porta), aplicação, IPS, antivírus, anti-spyware, Filtro de URL e filtro de arquivos em uma única tela;

4.15.1.55. Deve possuir relatórios de utilização dos recursos por aplicações, URL, ameaças (IPS, Antivírus e Anti-Spware), etc;

4.15.1.56. Prover uma visualização sumarizada de todas as aplicações, ameaças (IPS, Antivírus e Anti-Spware), e URLs que passaram pela solução;

4.15.1.57. Deve possuir mecanismo "*Drill-Down*" para navegação nos relatórios em *Real Time*;

4.15.1.58. Nas opções de "*Drill-Down*", ser possível identificar o usuário que fez determinado acesso;

4.15.1.59. Deve possuir relatório de visibilidade e uso sobre aplicativos (SaaS); O relatório também deve mostrar os riscos para a segurança do ambiente, tais como a entrega de *malwares* através de aplicativos SaaS com a informação do usuário responsável pelo acesso;

4.15.1.60. Os relatórios de visibilidade e uso sobre aplicativos (SaaS) devem poder ser extraídos por grupo de usuários apresentando o uso e consumo de aplicações por grupo de usuário;

4.15.1.61. Deve ser possível exportar os logs em CSV;

4.15.1.62. Deverá ser possível acessar o equipamento a aplicar configurações durante momentos onde o trafego é muito alto e a CPU e memória do equipamento estiver totalmente utilizada;

4.15.1.63. Rotação do log;

4.15.1.64. Deve permitir que os logs e relatórios sejam rotacionados automaticamente baseado no tempo em que estão armazenados na solução, assim como no espaço em disco usado;

4.15.1.65. Deve permitir fazer o envio de logs para soluções externas de forma granular podendo selecionar quais campos dos logs serão enviados incluindo, mas não limitado a: tipo de ameaça, usuário, aplicação, etc;

4.15.1.66. Exibição das seguintes informações, de forma histórica e em tempo real (atualizado de forma automática e contínua a cada 1 minuto):

4.15.1.66.1. Situação do dispositivo e do *cluster*;

4.15.1.66.2. Principais aplicações;

4.15.1.66.3. Principais aplicações por risco;

4.15.1.66.4. Administradores autenticados na gerência da plataforma de segurança;

4.15.1.66.5. Número de sessões simultâneas;

4.15.1.66.6. Status das interfaces;

4.15.1.66.7. Uso de CPU;

4.15.1.67. Geração de relatórios. No mínimo os seguintes relatórios devem ser gerados:

4.15.1.67.1. Resumo gráfico de aplicações utilizadas;

4.15.1.67.2. Principais aplicações por utilização de largura de banda de entrada e saída;

4.15.1.67.3. Principais aplicações por taxa de transferência de bytes;

4.15.1.67.4. Principais *hosts* por número de ameaças identificadas;

4.15.1.67.5. Atividades de um usuário específico e grupo de usuários do AD/LDAP, incluindo aplicações acessadas, categorias de URL, URL/tempo de utilização e ameaças (IPS, Antivírus e Anti-Spware), de rede vinculadas a este tráfego;

4.15.1.67.6. Deve permitir a criação de relatórios personalizados;

4.15.1.68. Em cada critério de pesquisa do log deve ser possível incluir múltiplas entradas (ex: 10 redes e IP's distintos; serviços HTTP, HTTPS e SMTP), exceto no campo horário, onde deve ser possível definir um faixa de tempo como critério de pesquisa;

4.15.1.69. Gerar alertas automáticos via:

4.15.1.69.1. Email;

4.15.1.69.2. SNMP;

4.15.1.69.3. *Syslog*.

4.16. Serviço de Configuração

4.16.1. Descrição Geral

4.16.2.1. Os serviços devem ser executados e planejados por técnicos certificados em gerenciamento de projetos. Fica a cargo da CONTRATANTE a solicitação da comprovação das certificações dos técnicos responsáveis pela realização dos serviços;

4.16.2. Será de responsabilidade da CONTRATADA todo o planejamento e implementação da topologia de rede e de recursos de segurança; A CONTRATADA deve ainda, após a instalação e configuração, monitorar presencialmente a solução pelo prazo mínimo de 2 (dois) dias úteis, sendo possível o *troubleshooting* em caso de problemas ou não conformidades na operação. Durante este período deve ser observado e realizado também o ajuste e configurações que porventura não estarão de acordo com a operação desejada;

4.16.3. Ao final da instalação e monitoramento, deverá ser realizado repasse de conhecimento de toda a solução por um período de 8 (oito) horas corridas;

4.16.4. Os serviços devem ser executados de segunda a sexta-feira, das 8 às 20 horas, nas unidades da CONTRATANTE;

4.16.5. A realização dos serviços deve ser planejada de acordo com disponibilidade de ambas as partes, em prazo máximo de 30 (trinta) dias após a entrega definitiva dos bens ou oficialização da ordem de empenho. O planejamento anterior ao serviço pode ser realizado remotamente através de webconferência ou videoconferência;

4.16.6. O planejamento dos serviços de instalação deve resultar em um documento tipo SOW (em tradução livre, escopo de trabalho). Neste documento devem conter a relação de produtos;

descrição e quantidades de equipamentos e serviços; descrição da infraestrutura atual e desejada; detalhamento dos serviços que serão executados; premissas do projeto; local, horários e condições de execução dos serviços; pontos de contato da CONTRATANTE e CONTRATADA; cronograma faseado do projeto, dividido em etapas, com responsáveis e data de início e fim (se aplicável); relação da documentação a ser entregue ao final da execução dos serviços; responsabilidade da CONTRATANTE e CONTRATADA; plano de gerenciamento de mudanças; itens excluídos no projeto; e termo de aceite. Os serviços não poderão ser iniciados antes da apresentação e assinatura de concordância de ambas as partes;

4.16.7. Ao término dos serviços deve ser criado um relatório detalhado contendo todos os itens configurados no projeto (*as-built*), etapas de execução e toda informação pertinente a posterior continuidade e manutenção da solução instalada;

4.16.8. Serviço referente à solução de Firewall de Próxima Geração (NGFW):

4.16.8.1. Realizar a instalação de acessórios e de todos os componentes que integram a especificação. Os equipamentos devem ser montados nos *racks* padrão 19" existentes e devem ser energizados através da infraestrutura de energia elétrica disponíveis;

4.16.8.2. Realizar a conectorização das interfaces de rede e interface de gerenciamento dos equipamentos;

4.16.8.3. Analisar o ambiente atual como topologia de rede, configurações de camada 2, camada 3 e migração de regras dos *firewalls* em produção no ambiente atual para a nova solução;

4.16.8.4. Efetuar a configuração dos perfis de acesso da solução de gerência com as devidas permissões conforme acordado previamente no planejamento dos serviços utilizando de autenticação integrada ao Microsoft Active Directory (AD) ou servidor radius;

4.16.8.5. Configurar as funcionalidades relevantes a implementação da solução conforme acordado previamente no planejamento dos serviços como: Endereçamento, VLANs, LACP, DHCP e tipos NAT;

4.16.8.6. Configurar o monitoramento da solução via SNMP em sistema de gerenciamento da CONTRATANTE para monitoramento de falhas de hardware, uso de recursos e estatísticas de uso das interfaces de rede;

4.16.8.7. Configurações de roteamento conforme acordado previamente no planejamento dos serviços como configurações de roteamento estático e protocolos dinâmicos como BGP BGP e OSPF para IPv4 ou IPv6;

4.16.8.8. Configuração de interfaces em modos: transparente, camada 2 (L2) ou camada 3 (L3), conforme acordado previamente no planejamento dos serviços;

4.16.8.9. Realizar a configuração das políticas de *firewall* analisando a configuração dos equipamentos atuais e sugerindo novas regras para implementação de controles por zona de segurança, políticas por porta e protocolo, políticas por aplicações, categorias de aplicações, políticas por usuários, grupos de usuários e políticas por geolocalização;

4.16.8.10. Implementar políticas de bloqueios de arquivos conforme acordado no planejamento dos serviços;

4.16.8.11. Configurar limitações de banda por com base no IP de origem, usuários e grupos conforme acordado previamente no planejamento dos serviços;

4.16.8.12. Realizar a criação de assinaturas personalizadas para reconhecimento de aplicações proprietárias da CONTRATANTE conforme acordado previamente no planejamento dos serviços;

4.16.8.13. Configurar regras de IPS, Anti-Malware e Filtro URL arquivos conforme a cordado previamente no planejamento dos serviços;

4.16.8.14. Realizar backup das configurações realizadas;

4.16.9. Deve ser entregue relatório contendo todo o serviço realizado executado;

4.16.10. Deverá ser feita por profissionais devidamente qualificados e certificados pelo fabricante e acompanhada pelos técnicos da CONTRATANTE;

4.16.11. Durante toda a implantação do projeto, o técnico da CONTRATADA deverá demonstrar aos técnicos da CONTRATANTE como instalar e configurar os equipamentos e os softwares fornecidos (instalação assistida). Esta demonstração deverá contemplar os conceitos das tecnologias utilizadas pelo equipamento e a operação dos principais recursos dos produtos ofertados.

4.17 Modelo de execução do Contrato

4.17.1 Rotinas de Execução

4.17.1.1 Procedimentos Para Encaminhamento e Controle de Solicitações

4.17.1.2 Após a assinatura do contrato, a contratante emitirá a Ordem de Fornecimento – OF;

4.17.1.3 A data da emissão da OF deverá expressar a data atual da sua emissão e não as datas de empenho e/ou contrato;

4.17.1.4 A Ordem de Fornecimento deverá ser atendida pela CONTRATADA no prazo máximo estabelecido;

4.17.1.5 A OF indicará as quantidades, os prazos, os responsáveis pelo recebimento e local de entrega do objeto;

4.17.2 Serviço de Suporte Técnico Remoto

4.17.2.1 Deve ser incluído nos custos os serviços de suporte técnico remoto pelo período definido;

4.17.2.2 A equipe técnica da CONTRATANTE poderá abrir, gerenciar status e conferir todo o histórico de chamados de suporte técnico, mediante login e senha de acesso ao sistema;

4.17.2.3 Os chamados abertos por e-mail deverão ter sua abertura automática no portal web;

4.17.2.4 Todo o chamado aberto deverá ter sua resolução técnica registrada no sistema web de help-desk;

4.17.2.5 A contratada deverá prestar o suporte técnico dos produtos, sendo facultado a ela o escalonamento das questões para o respectivo fabricante, ficando, entretanto, a CONTRATADA responsável pelo gerenciamento do chamado e prestação de informações à CONTRATANTE;

4.17.2.6 A CONTRATADA deve indicar, por ocasião do início dos trabalhos, os procedimentos para abertura de suporte técnico;

4.17.2.7 Deverão ser alocadas 04 (quatro) horas por mês para atendimento das demandas;

4.17.2.8 As horas de atendimento serão realizadas normalmente em horário comercial, no período compreendido entre 08:30h e 18:30h, em dias de semana (segunda à sexta);

4.17.3 Prestação de serviços que compreendem, entre outros, os seguintes procedimentos de serviços da Solução de Plataforma de Segurança:

4.17.3.1 Habilitar licenças que porventura sejam adquiridas;

4.17.3.2 Sanar dúvidas relacionadas ao funcionamento dos equipamentos;

4.17.3.3 Administração e configuração da Solução de Gerenciamento Centralizado de firewall;

4.17.3.4 Suporte em caso de indisponibilidade de links e interfaces do cluster de firewall;

4.17.3.5 Resolução de problemas quanto acesso à internet, sites remotos, serviços de rede oferecidos aos funcionários que dependam do cluster de firewall;

4.17.3.6 Suporte à configuração e resolução de problemas de acessos remotos VPNs client-to-site;

4.17.3.7 Suporte à configuração e resolução de problemas de VPNs site-to-site entre o cluster de firewall e outros equipamentos quando solicitado;

4.17.3.8 Suporte quanto a problemas de identificação de usuários;

4.17.3.9 Suporte quanto a de problemas de desconexão de aplicações;

4.17.3.10 Auxílio quanto as atualizações de sistema operacional e assinaturas de aplicação, prevenção de ameaças e filtro de URL;

4.17.3.11 Configurações e resolução de problemas quanto a funcionalidades aplicação, prevenção de ameaças e filtro de URL;

4.17.3.12 Realizar alterações de regras de roteamento estático, roteamento dinâmico (OSPF e BGP), PBF (Policy Base Routing) e tipos de NAT quando solicitado;

4.17.3.13 Realizar liberações ou bloqueios de aplicações quando solicitado;

4.17.3.14 Auxílio na customização de relatórios disponíveis na solução;

4.17.3.15 Verificação de funcionamento de regras;

4.17.3.16 Suporte na configuração de descriptografia HTTPs inbound e outbound;

4.17.3.17 Auxílio na configuração de contextos virtuais;

4.17.3.18 Realizar manutenções preventivas do cluster de firewall quando solicitado;

4.17.3.19 Suporte em demais configurações de segurança, redundância e gerência;

4.17.3.20 Realizar otimização de performance (“tunning”) da solução de firewall;

4.17.3.21 Apoio técnico em configurações de alta disponibilidade, redundância e gerência de controladoras e pontos de acesso;

4.17.3.22 Suporte e administração das políticas e tarefas de backup;

4.17.3.23 Apoio técnico para tarefas de auditoria e análise de logs;

4.17.3.24 Encaminhar incidentes ao fabricante da solução;

4.17.3.25 Suporte técnico para identificação e resolução de problemas em software e hardware.

4.17.3.26 A cada 03 (três) meses deverá ser emitido, apresentado e entregue um relatório de segurança com dados obtidos a partir da solução de segurança contendo:

4.17.3.27 Informações de adoção da solução, apontando configurações individuais para verificar como os recursos de segurança estão sendo aproveitados. Exemplo: Análise da base de regras para identificar se as mesmas estão sendo aproveitadas e se são relevantes;

4.17.3.28 Informações de avaliação de melhores práticas sobre as configurações da solução, identificando os riscos e fornecendo recomendações. Exemplo: A avaliação deverá comparar as configurações atuais às práticas recomendadas devendo apontar qual das práticas recomendadas estão ou não sendo utilizadas;

4.17.3.29 Informações referente as aplicações e as ameaças detectados no ambiente mostrando as aplicações em uso e quais introduzem ameaças na rede, utilização de aplicações SaaS, total de ameaças (malwares conhecidos, malwares desconhecidos e detecções de comando e controle) bem como a movimentações de arquivos (tipos e riscos);

4.17.3.30 Relatório de análise de vulnerabilidade dos serviços publicados externamente que estão protegidos pela solução indicando as vulnerabilidades separadas por: críticas, altas, médias, baixas e informacionais, bem como testes de vulnerabilidade dos próprios dispositivos de segurança fornecidos.

4.18 Atualizações

4.18.1 A CONTRATADA deverá disponibilizar, na vigência do contrato, todas as atualizações dos softwares e firmwares dos equipamentos, concebidas em data posterior ao seu fornecimento, pelo período especificado no termo de referência, sem qualquer ônus adicional para o CONTRATANTE;

4.18.2 As atualizações incluídas devem ser do tipo “minor release” e “major release”, permitindo manter os equipamentos atualizados em sua última versão de software/firmware.

4.19 Mecanismos Formais de Comunicação

4.19.1 A CONTRATADA deverá disponibilizar, cumulativamente, estrutura de suporte técnico por meio de atendimento telefônico, website e e-mail;

4.19.2 As ligações deverão ser gratuitas, adotando-se o sistema 0800;

4.19.3 A CONTRATADA deverá disponibilizar um portal web com disponibilidade de 24 horas por dia, 7 dias por semana e 365 dias por ano, com sistema de help desk para abertura de chamados de suporte técnico;

4.20 Manutenção de Sigilo e Normas de Segurança

4.21 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.

5 DAS OBRIGAÇÕES DA CONTRATANTE

5.1 São obrigações da Contratante:

5.1.1 Receber o objeto no prazo e condições estabelecidas no Edital e seus anexos.

5.1.2 Verificar minuciosamente, no prazo fixado, a conformidade dos bens recebidos provisoriamente com as especificações constantes do Edital e da proposta, para fins de aceitação e recebimento definitivo.

5.1.3 Comunicar à Contratada, por escrito, sobre imperfeições, falhas ou irregularidades verificadas no objeto fornecido, para que seja substituído, reparado ou corrigido.

5.1.4 Acompanhar e fiscalizar o cumprimento das obrigações da Contratada, através da Coordenação do Almoxarifado e/ou Coordenação do Patrimônio.

5.1.5 Efetuar o pagamento à Contratada no valor correspondente ao fornecimento do objeto, no prazo e forma estabelecidos no Edital e seus anexos.

5.2 A Administração não responderá por quaisquer compromissos assumidos pela Contratada com terceiros, ainda que vinculados à execução do presente Termo de Contrato, bem como por qualquer dano causado a terceiros em decorrência de ato da Contratada, de seus empregados, prepostos ou subordinados.

6 DAS OBRIGAÇÕES DA CONTRATADA

6.1 A Contratada deve cumprir todas as obrigações constantes no Edital, seus anexos e sua proposta, assumindo como exclusivamente seus os riscos e as despesas decorrentes da boa e perfeita execução do objeto e, ainda:

6.1.1 Efetuar a entrega do objeto em perfeitas condições, conforme especificações, prazo e local constantes no Termo de Referência e seus anexos, acompanhado da respectiva nota fiscal, na qual constarão as indicações referentes à marca, fabricante, modelo, procedência e prazo de garantia ou validade.

6.1.1.1 O objeto deve estar acompanhado do manual do usuário, com uma versão em português e da relação da rede de assistência técnica autorizada, quando for o caso.

6.1.2 Responsabilizar-se pelos vícios e danos decorrentes do objeto, de acordo com os artigos 12, 13 e 17 a 27, do Código de Defesa do Consumidor (Lei n. 8.078/1990).

6.1.3 Substituir, reparar ou corrigir, às suas expensas, no prazo fixado neste Termo de Referência, o objeto com avarias ou defeitos.

6.1.4 Comunicar à Contratante, no prazo máximo de 24 (vinte e quatro) horas que antecede a data da entrega, os motivos que impossibilitem o cumprimento do prazo previsto, com a devida comprovação.

6.1.5 Manter, durante toda a execução do contrato, em compatibilidade com as obrigações assumidas, todas as condições de habilitação e qualificação exigidas na licitação.

6.1.6 Indicar preposto para representá-la durante a execução do contrato.

7 DA SUBCONTRATAÇÃO

7.1 Não será admitida a subcontratação para fornecimento dos materiais.

8 DA ALTERAÇÃO SUBJETIVA

8.1 É admissível a fusão, cisão ou incorporação da contratada com/em outra pessoa jurídica, desde que sejam observados pela nova pessoa jurídica todos os requisitos de habilitação exigidos na licitação original; sejam mantidas as demais cláusulas e condições do contrato; não haja prejuízo à execução do objeto pactuado e haja a anuência expressa da Administração à continuidade do contrato.

9 DO CONTROLE E FISCALIZAÇÃO DA EXECUÇÃO

9.1 Nos termos do art. 67, da Lei n. 8.666/1993, será designado representante para acompanhar e fiscalizar a entrega dos bens, anotando em registro próprio todas as ocorrências relacionadas com a execução e determinando o que for necessário à regularização de falhas ou defeitos observados.

9.1.1 O recebimento de material de valor superior a R$ 176.000,00 (Cento e Setenta e Seis Mil Reais) será confiado a uma Comissão de, no mínimo, 03 (três) membros, designados pela autoridade competente.

9.2 A fiscalização de que trata este item não exclui nem reduz a responsabilidade da Contratada, inclusive perante terceiros, por qualquer irregularidade, ainda que resultante de imperfeições técnicas ou vícios redibitórios, e, na ocorrência desta, não implica em co-responsabilidade da Administração ou de seus agentes e prepostos, de conformidade com o art. 70, da Lei n. 8.666/1993.

9.3 O representante da Administração anotará em registro próprio todas as ocorrências relacionadas com a execução do contrato, indicando dia, mês e ano, bem como o nome dos funcionários eventualmente envolvidos, determinando o que for necessário à regularização das falhas ou defeitos

observados e encaminhando os apontamentos à autoridade competente para as providências cabíveis.

10 PAGAMENTO

10.1 O pagamento será realizado no prazo máximo de até 30 (trinta) dias, contados a partir do recebimento da Nota Fiscal ou Fatura, através de ordem bancária, para crédito em banco, agência e conta corrente indicados pelo contratado.

> 10.1.1 Os pagamentos decorrentes de despesas cujos valores não ultrapassem o limite de que trata o inciso II do art. 24 da Lei 8.666, de 1993, deverão ser efetuados no prazo de até 05 (cinco) dias úteis, contados da data da apresentação da Nota Fiscal, nos termos do art. 5º, § 3º, da Lei nº 8.666, de 1993.

10.2 Considera-se ocorrido o recebimento da nota fiscal ou fatura no momento em que o órgão contratante atestar a execução do objeto do contrato.

10.3 A Nota Fiscal ou Fatura deverá ser obrigatoriamente acompanhada da comprovação da regularidade fiscal, constatada por meio de consulta on-line ao SICAF ou, na impossibilidade de acesso ao referido Sistema, mediante consulta aos sítios eletrônicos oficiais ou à documentação mencionada no art. 29 da Lei nº 8.666, de 1993.

> 10.3.1 Constatando-se, junto ao SICAF, a situação de irregularidade do fornecedor contratado, deverão ser tomadas as providências previstas no do art. 31 da Instrução Normativa nº 3, de 26 de abril de 2018.

10.4 Havendo erro na apresentação da Nota Fiscal ou dos documentos pertinentes à contratação, ou, ainda, circunstância que impeça a liquidação da despesa, como, por exemplo, obrigação financeira pendente, decorrente de penalidade imposta ou inadimplência, o pagamento ficará sobrestado até que a Contratada providencie as medidas saneadoras. Nesta hipótese, o prazo para pagamento iniciar-se-á após a comprovação da regularização da situação, não acarretando qualquer ônus para a Contratante.

10.5 Será considerada data do pagamento o dia em que constar como emitida a ordem bancária para pagamento.

10.6 Antes de cada pagamento à contratada, será realizada consulta ao SICAF para verificar a manutenção das condições de habilitação exigidas no edital.

10.7 Constatando-se, junto ao SICAF, a situação de irregularidade da contratada, será providenciada sua notificação, por escrito, para que, no prazo de 05 (cinco) dias úteis, regularize sua situação ou, no mesmo prazo, apresente sua defesa. O prazo poderá ser prorrogado uma vez, por igual período, a critério da contratante.

10.8 Previamente à emissão de nota de empenho e a cada pagamento, a Administração deverá realizar consulta ao SICAF para identificar possível suspensão temporária de participação em licitação, no âmbito do órgão ou entidade, proibição de contratar com o Poder Público, bem como ocorrências impeditivas indiretas, observado o disposto no art. 29, da Instrução Normativa nº 3, de 26 de abril de 2018.

10.9 Não havendo regularização ou sendo a defesa considerada improcedente, a contratante deverá comunicar aos órgãos responsáveis pela fiscalização da regularidade fiscal quanto à inadimplência da contratada, bem como quanto à existência de pagamento a ser efetuado, para que sejam acionados os meios pertinentes e necessários para garantir o recebimento de seus créditos.

10.10 Persistindo a irregularidade, a contratante deverá adotar as medidas necessárias à rescisão contratual nos autos do processo administrativo correspondente, assegurada à contratada a ampla defesa.

10.11 Havendo a efetiva execução do objeto, os pagamentos serão realizados normalmente, até que se decida pela rescisão do contrato, caso a contratada não regularize sua situação junto ao SICAF.

10.11.1 Será rescindido o contrato em execução com a contratada inadimplente no SICAF, salvo por motivo de economicidade, segurança nacional ou outro de interesse público de alta relevância, devidamente justificado, em qualquer caso, pela máxima autoridade da contratante

10.12 Quando do pagamento, será efetuada a retenção tributária prevista na legislação aplicável.

10.12.1 A Contratada regularmente optante pelo Simples Nacional, nos termos da Lei Complementar nº 123, de 2006, não sofrerá a retenção tributária quanto aos impostos e contribuições abrangidos por aquele regime. No entanto, o pagamento ficará condicionado à apresentação de comprovação, por meio de documento oficial, de que faz jus ao tratamento tributário favorecido previsto na referida Lei Complementar.

10.13 Nos casos de eventuais atrasos de pagamento, desde que a Contratada não tenha concorrido, de alguma forma, para tanto, fica convencionado que a taxa de compensação financeira devida pela Contratante, entre a data do vencimento e o efetivo adimplemento da parcela, é calculada mediante a aplicação da seguinte fórmula:

EM = I x N x VP, sendo:
EM = Encargos moratórios;
N = Número de dias entre a data prevista para o pagamento e a do efetivo pagamento;
VP = Valor da parcela a ser paga.
I = Índice de compensação financeira = 0,00016438, assim apurado:

$$I = (TX) = \frac{I}{\left(\frac{6}{100}\right)}$$

I = 0,00016438
TX = Percentual da taxa anual = 6%

365

11 DO REAJUSTE
11.1 Os preços são fixos e irreajustáveis no prazo de um ano contado da data limite para a apresentação das propostas.

12 DA GARANTIA DE EXECUÇÃO
12.1 Não haverá exigência de garantia contratual da execução.

13 GARANTIA CONTRATUAL DOS BENS
13.1 O prazo de garantia contratual dos bens, complementar à garantia legal, é de, no mínimo, 60 (sessenta) meses, ou pelo prazo fornecido pelo fabricante, se superior, contado a partir do primeiro dia útil subsequente à data do recebimento definitivo do objeto.

13.1.1 Todos os serviços baseados em assinaturas devem estar disponíveis por, no mínimo, 60 (sessenta) meses também;

13.2 A garantia será prestada com vistas a manter os equipamentos fornecidos em perfeitas condições de uso, sem qualquer ônus ou custo adicional para o Contratante.

13.3 A garantia abrange a realização da manutenção corretiva dos bens pela própria Contratada, ou, se for o caso, por meio de assistência técnica autorizada, de acordo com as normas técnicas específicas.

13.4 Entende-se por manutenção corretiva aquela destinada a corrigir os defeitos apresentados pelos bens, compreendendo a substituição de peças, a realização de ajustes, reparos e correções necessárias.

13.5 As peças que apresentarem vício ou defeito no período de vigência da garantia deverão ser substituídas por outras novas, de primeiro uso, e originais, que apresentem padrões de qualidade e desempenho iguais ou superiores aos das peças utilizadas na fabricação do equipamento.

13.6 Uma vez notificada, a Contratada realizará a reparação ou substituição dos bens que apresentarem vício ou defeito no prazo de até 03 (três) dias úteis, contados a partir da data de retirada do equipamento das dependências da Administração pela Contratada ou pela assistência técnica autorizada.

13.7 O prazo indicado no subitem anterior, durante seu transcurso, poderá ser prorrogado uma única vez, por igual período, mediante solicitação escrita e justificada da Contratada, aceita pelo Contratante.

13.8 Na hipótese do subitem acima, a Contratada deverá disponibilizar equipamento equivalente, de especificação igual ou superior ao anteriormente fornecido, para utilização em caráter provisório pelo Contratante, de modo a garantir a continuidade dos trabalhos administrativos durante a execução dos reparos.

13.9 Decorrido o prazo para reparos e substituições sem o atendimento da solicitação do Contratante ou a apresentação de justificativas pela Contratada, fica o Contratante autorizado a contratar empresa diversa para executar os reparos, ajustes ou a substituição do bem ou de seus componentes, bem como a exigir da Contratada o reembolso pelos custos respectivos, sem que tal fato acarrete a perda da garantia dos equipamentos.

13.10 O custo referente ao transporte dos equipamentos cobertos pela garantia será de responsabilidade da Contratada.

13.11 A garantia legal ou contratual do objeto tem prazo de vigência próprio e desvinculado daquele fixado no contrato, permitindo eventual aplicação de penalidades em caso de descumprimento de alguma de suas condições, mesmo depois de expirada a vigência contratual.

14 DAS SANÇÕES ADMINISTRATIVAS

14.1 Comete infração administrativa nos termos da Lei n. 8.666/1993 e da Lei n. 10.520/2002, a Contratada que:

14.1.1 Inexecutar total ou parcialmente qualquer das obrigações assumidas em decorrência da contratação.

14.1.2 Ensejar o retardamento da entrega dos materiais.

14.1.3 Falhar ou fraudar no fornecimento dos materiais.

14.1.4 Comportar-se de modo inidôneo.

14.1.5 Cometer fraude fiscal.

14.2 Pela inexecução total ou parcial do objeto deste contrato, a Administração pode aplicar à CONTRATADA as seguintes sanções:

14.2.1 Advertência por faltas leves, assim entendidas aquelas que não acarretem prejuízos significativos para a Contratante.

14.2.2 Multa moratória de 1% (um por cento) por dia de atraso injustificado sobre o valor da parcela inadimplida, até o limite de 30 (trinta) dias.

14.2.3 Multa compensatória de 1% (um por cento) sobre o valor total da Nota de Empenho, no caso de inexecução total do objeto (não entrega do material).

14.2.4 Em caso de inexecução parcial, a multa compensatória, no mesmo percentual do subitem acima, será aplicada de forma proporcional à obrigação inadimplida.

14.2.5 Suspensão de licitar e impedimento de contratar com o órgão, entidade ou unidade administrativa pela qual a Administração Pública opera e atua concretamente, pelo prazo de até dois anos.

14.2.6 Impedimento de licitar e contratar com a União com o consequente descredenciamento no SICAF pelo prazo de até cinco anos.

14.2.6.1 A Sanção de impedimento de licitar e contratar prevista neste subitem também é aplicável em quaisquer das hipóteses previstas como infração administrativa no subitem 14.1 deste Termo de Referência.

14.2.7 Declaração de inidoneidade para licitar ou contratar com a Administração Pública, enquanto perdurarem os motivos determinantes da punição ou até que seja promovida a reabilitação perante a própria autoridade que aplicou a penalidade, que será concedida sempre que a Contratada ressarcir a Contratante pelos prejuízos causados.

14.3 As sanções previstas nos subitens 14.2.1, 14.2.5, 14.2.6 e 14.2.7 poderão ser aplicadas à Contratada juntamente com as de multa, descontando-a dos pagamentos a serem efetuados.

14.4 Também ficam sujeitas às penalidades do art. 87, III e IV da Lei n. 8.666/1993, a Contratada que:

14.4.1 Tenha sofrido condenação definitiva por praticar, por meio dolosos, fraude fiscal no recolhimento de quaisquer tributos.

14.4.2 Tenha praticado atos ilícitos visando a frustrar os objetivos da licitação.

14.4.3 Demonstre não possuir idoneidade para contratar com a Administração em virtude de atos ilícitos praticados.

14.5 A aplicação de qualquer das penalidades previstas realizar-se-á em processo administrativo que assegurará o contraditório e a ampla defesa à Contratada, observando-se o procedimento previsto na Lei n. 8.666/1993, e subsidiariamente a Lei n. 9.784/1999.

14.6 As multas devidas e/ou prejuízos causados à Contratante serão deduzidos dos valores a serem pagos, ou recolhidos em favor da União, ou deduzidos da garantia, ou ainda, quando for o caso, serão inscritos na Dívida Ativa da União e cobrados judicialmente.

14.6.1 Caso a Contratante determine, a multa deverá ser recolhida no prazo máximo de 30 (trinta) dias, a contar da data do recebimento da comunicação enviada pela autoridade competente.

14.7 Caso o valor da multa não seja suficiente para cobrir os prejuízos causados pela conduta do licitante, a União ou Entidade poderá cobrar o valor remanescente judicialmente, conforme artigo 419 do Código Civil.

14.8 A autoridade competente, na aplicação das sanções, levará em consideração a gravidade da conduta do infrator, o caráter educativo da pena, bem como o dano causado à Administração, observado o princípio da proporcionalidade.

14.9 Se, durante o processo de aplicação de penalidade, se houver indícios de prática de infração administrativa tipificada pela Lei nº 12.846, de 1º de agosto de 2013, como ato lesivo à administração pública nacional ou estrangeira, cópias do processo administrativo necessárias à apuração da responsabilidade da empresa deverão ser remetidas à autoridade competente, com despacho fundamentado, para ciência e decisão sobre a eventual instauração de investigação preliminar ou Processo Administrativo de Responsabilização - PAR.

14.10 A apuração e o julgamento das demais infrações administrativas não consideradas como ato lesivo à Administração Pública nacional ou estrangeira nos termos da Lei nº 12.846, de 1º de agosto de 2013, seguirão seu rito normal na unidade administrativa.

14.11 O processamento do PAR não interfere no seguimento regular dos processos administrativos específicos para apuração da ocorrência de danos e prejuízos à Administração Pública Federal resultantes de ato lesivo cometido por pessoa jurídica, com ou sem a participação de agente público.

14.12 As penalidades serão obrigatoriamente registradas no SICAF.

15. ESTIMATIVA DE PREÇOS E PREÇOS REFERENCIAIS

15.1 O custo estimado da contratação é de R$ 2.365.883,88 (Dois Milhões, Trezentos e Sessenta e Cinco Mil, Oitocentos e Oitenta e Três Reais e Oitenta e Oito Centavos).

16 DA CONFORMIDADE DO PROCESSO COM A MANIFESTAÇÃO JURÍDICA REFERENCIAL

16.1 Este Termo de Referência para aquisição de material amolda-se à manifestação jurídica referencial correspondente ao PARECER N. 00001/2017/CONSU/PFFUA/PGF/AGU, cujas recomendações restam atendidas no caso concreto.

16.2 Fica assim dispensada a remessa dos autos para exame individualizado pela Procuradoria Federal junto à FUA, conforme autorizado pela Orientação Normativa n. 55, da Advocacia Geral da União.

Manaus-AM, 05 de maio de 2020.

Responsável pela Cotação de Preços e elaboração do Termo de Referência Retificado

RAPHAEL ANTONIO QUEIROZ RUSSO
Coordenador de Licitação de Material de Consumo

Autorização do DEMAT

JOICE RIBEIRO DOS SANTOS
Diretora do DEMAT

Autorização da Autoridade Competente

Eu, RAIMUNDO NONATO PINHEIRO DE ALMEIDA, Pró-Reitor de Administração e Finanças, APROVO o presente Termo de Referência e AUTORIZO a abertura do processo licitatório para aquisição dos materiais.

Termo de Referência - Modelo para Pregão Eletrônico - Compras
Atualização: Dezembro/2019 (disponível em http://www.agu.gov.br/page/content/detail/id_conteudo/244963)

ANEXO II

DECLARAÇÃO DE INEXISTÊNCIA DE VINCULO FAMILAR -

PREGÃO ELETRÔNICO Nº 007/2020

Declaramos que não constam em nossos quadros societários servidores da FUA ou administradores que mantenham vínculo familiar com detentor de cargo em comissão ou função de confiança, atuante na área responsável pela demanda ou contratação, ou de autoridade a ele hierarquicamente superior, em cumprimento ao Acórdão Nº 409/2015 – TCU - Plenário.

Local e data

_____

Assinatura e carimbo
(Representante Legal)

Observação: emitir em papel que identifique a entidade expedidora.

ANEXO III

ATA DE REGISTRO DE PREÇOS N° XXX/20XX

FUNDAÇÃO UNIVERSIDADE DO AMAZONAS

O(A).....(*órgão ou entidade pública que gerenciará a ata de registro de preços*), com sede no(a) ....., na cidade de ....., inscrito(a) no CNPJ/MF sob o nº ....., neste ato representado(a) pelo(a) ..... (*cargo e nome*), nomeado(a) pela Portaria nº ..... de ..... de ..... de 200..., publicada no ..... de ..... de ..... de ....., portador da matrícula funcional nº .....,, considerando o julgamento da licitação na modalidade de pregão, na forma eletrônica, para REGISTRO DE PREÇOS **nº 007/2020**, publicada no ..... de ...../...../200....., processo administrativo n.º ....., RESOLVE registrar os preços da(s) empresa(s) indicada(s) e qualificada(s) nesta ATA, de acordo com a classificação por ela(s) alcançada(s) e na(s) quantidade(s) cotada(s), atendendo as condições previstas no edital, sujeitando-se as partes às normas constantes na Lei nº 8.666, de 21 de junho de 1993 e suas alterações, no Decreto n.º 7.892, de 23 de janeiro de 2013, e em conformidade com as disposições a seguir:

1. DO OBJETO

1.1. A presente Ata tem por objeto o registro de preços para a eventual **aquisição de material de material permanente (fornecimento de solução de proteção de rede de dados com características de Firewall de próxima geração (Next Generation Firewall – NGFW), com suporte de 60 meses, solução de gerenciamento centralizado, serviços de instalação, configuração e treinamento de pessoal), conforme condições, quantidades, exigências e estimativas encaminhadas pelo Centro de Tecnologia da Informação e Comunicação-CTIC da Universidade Federal do Amazonas,** especificado(s) no(s) item(ns)..... do ..... Termo de Referência, anexo I do edital de **Pregão nº 007/2020**, que é parte integrante desta Ata, assim como a proposta vencedora, independentemente de transcrição.

2. DOS PREÇOS, ESPECIFICAÇÕES E QUANTITATIVOS

2.1. O preço registrado, as especificações do objeto, a quantidade, fornecedor(es) e as demais condições ofertadas na(s) proposta(s) são as que seguem:

Item do TR	Fornecedor *(razão social, CNPJ/MF, endereço, contatos, representante)*						
X	Especificação	*Marca (se exigida no edital)*	*Modelo (se exigido no edital)*	Unidade	Quantidade	Valor Un	*Prazo garantia ou validade*

2.2. A listagem do cadastro de reserva referente ao presente registro de preços consta como anexo a esta Ata.

3. DA ADESÃO À ATA DE REGISTRO DE PREÇOS

3.1. A ata de registro de preços, durante sua validade, poderá ser utilizada por qualquer órgão ou entidade da administração pública que não tenha participado do certame licitatório, mediante anuência do órgão gerenciador, desde que devidamente justificada a vantagem e respeitadas, no que couber, as condições e as regras estabelecidas na Lei nº 8.666, de 1993 e no Decreto nº 7.892, de 2013.

3.1.1. A manifestação do órgão gerenciador de que trata o subitem anterior, salvo para adesões feitas por órgãos ou entidades de outras esferas federativas, fica condicionada à realização de estudo, pelos órgãos e pelas entidades que não participaram do registro de preços, que demonstre o ganho de eficiência, a viabilidade e a economicidade para a administração pública federal da utilização da ata de registro de preços, conforme estabelecido em ato do Secretário de Gestão do Ministério do Planejamento, Desenvolvimento e Gestão

3.2. Caberá ao fornecedor beneficiário da Ata de Registro de Preços, observadas as condições nela estabelecidas, optar pela aceitação ou não do fornecimento, desde que este fornecimento não prejudique as obrigações anteriormente assumidas com o órgão gerenciador e órgãos participantes.

3.3. As aquisições ou contratações adicionais a que se refere este item não poderão exceder, por órgão ou entidade, a 50% (cinquenta por cento) dos quantitativos dos itens do instrumento convocatório e registrados na ata de registro de preços para o órgão gerenciador e órgãos participantes.

3.4. As adesões à ata de registro de preços são limitadas, na totalidade, ao dobro do quantitativo de cada item registrado na ata de registro de preços para o órgão gerenciador e órgãos participantes, independente do número de órgãos não participantes que eventualmente aderirem.

3.4.1. Tratando-se de item exclusivo para microempresas e empresas de pequeno porte e cooperativas enquadradas no artigo 34 da Lei n° 11.488, de 2007, o órgão gerenciador somente autorizará a adesão caso o valor da contratação pretendida pelo aderente, somado aos valores das contratações já previstas para o órgão gerenciador e participantes ou já destinadas à aderentes anteriores, não ultrapasse o limite de R$ 80.000,00 (oitenta mil reais) (Acórdão TCU nº 2957/2011 – P).

3.5. Ao órgão não participante que aderir à ata competem os atos relativos à cobrança do cumprimento pelo fornecedor das obrigações contratualmente assumidas e a aplicação, observada a ampla defesa e o contraditório, de eventuais penalidades decorrentes do descumprimento de cláusulas contratuais, em relação as suas próprias contratações, informando as ocorrências ao órgão gerenciador.

3.6. Após a autorização do órgão gerenciador, o órgão não participante deverá efetivar a contratação solicitada em até noventa dias, observado o prazo de validade da Ata de Registro de Preços.

3.6.1. Caberá ao órgão gerenciador autorizar, excepcional e justificadamente, a prorrogação do prazo para efetivação da contratação, respeitado o prazo de vigência da ata, desde que solicitada pelo órgão não participante.

4. VALIDADE DA ATA

4.1. A validade da Ata de Registro de Preços será de **12 meses**, a partir da data de sua homologação, não podendo ser prorrogada.

5. REVISÃO E CANCELAMENTO

5.1. A Administração realizará pesquisa de mercado periodicamente, em intervalos não superiores a 180 (cento e oitenta) dias, a fim de verificar a vantajosidade dos preços registrados nesta Ata.

5.2. Os preços registrados poderão ser revistos em decorrência de eventual redução dos preços praticados no mercado ou de fato que eleve o custo do objeto registrado, cabendo à Administração promover as negociações junto ao(s) fornecedor(es).

5.3. Quando o preço registrado tornar-se superior ao preço praticado no mercado por motivo superveniente, a Administração convocará o(s) fornecedor(es) para negociar(em) a redução dos preços aos valores praticados pelo mercado.

5.4. O fornecedor que não aceitar reduzir seu preço ao valor praticado pelo mercado será liberado do compromisso assumido, sem aplicação de penalidade.

5.4.1. A ordem de classificação dos fornecedores que aceitarem reduzir seus preços aos valores de mercado observará a classificação original.

5.5. Quando o preço de mercado tornar-se superior aos preços registrados e o fornecedor não puder cumprir o compromisso, o órgão gerenciador poderá:

5.5.1. liberar o fornecedor do compromisso assumido, caso a comunicação ocorra antes do pedido de fornecimento, e sem aplicação da penalidade se confirmada a veracidade dos motivos e comprovantes apresentados; e

5.5.2. convocar os demais fornecedores para assegurar igual oportunidade de negociação.

5.6. Não havendo êxito nas negociações, o órgão gerenciador deverá proceder à revogação desta ata de registro de preços, adotando as medidas cabíveis para obtenção da contratação mais vantajosa.

5.7. O registro do fornecedor será cancelado quando:

5.7.1. descumprir as condições da ata de registro de preços;

5.7.2. não retirar a nota de empenho ou instrumento equivalente no prazo estabelecido pela Administração, sem justificativa aceitável;

5.7.3. não aceitar reduzir o seu preço registrado, na hipótese deste se tornar superior àqueles praticados no mercado; ou

5.7.4. sofrer sanção administrativa cujo efeito torne-o proibido de celebrar contrato administrativo, alcançando o órgão gerenciador e órgão(s) participante(s).

5.8. O cancelamento de registros nas hipóteses previstas nos itens 5.7.1, 5.7.2 e 5.7.4 será formalizado por despacho do órgão gerenciador, assegurado o contraditório e a ampla defesa.

5.9. O cancelamento do registro de preços poderá ocorrer por fato superveniente, decorrente de caso fortuito ou força maior, que prejudique o cumprimento da ata, devidamente comprovados e justificados:

5.9.1. por razão de interesse público; ou

5.9.2. a pedido do fornecedor.

6. DAS PENALIDADES

6.1. O descumprimento da Ata de Registro de Preços ensejará aplicação das penalidades estabelecidas no Edital.

6.1.1. As sanções do item acima também se aplicam aos integrantes do cadastro de reserva, em pregão para registro de preços que, convocados, não honrarem o compromisso assumido injustificadamente, nos termos do art. 49, §1º do Decreto nº 10.024/19.

6.2. É da competência do órgão gerenciador a aplicação das penalidades decorrentes do descumprimento do pactuado nesta ata de registro de preço (art. 5º, inciso X, do Decreto nº 7.892/2013), exceto nas hipóteses em que o descumprimento disser respeito às contratações dos órgãos participantes, caso no qual caberá ao respectivo órgão participante a aplicação da penalidade (art. 6º, Parágrafo único, do Decreto nº 7.892/2013).

6.3. O órgão participante deverá comunicar ao órgão gerenciador qualquer das ocorrências previstas no art. 20 do Decreto nº 7.892/2013, dada a necessidade de instauração de procedimento para cancelamento do registro do fornecedor.

7. CONDIÇÕES GERAIS

7.1. As condições gerais do fornecimento, tais como os prazos para entrega e recebimento do objeto, as obrigações da Administração e do fornecedor registrado, penalidades e demais condições do ajuste, encontram-se definidos no Termo de Referência, ANEXO AO EDITAL.

7.2. É vedado efetuar acréscimos nos quantitativos fixados nesta ata de registro de preços, inclusive o acréscimo de que trata o § 1º do art. 65 da Lei nº 8.666/93, nos termos do art. 12, §1º do Decreto nº 7892/13.

7.3. No caso de adjudicação por preço global de grupo de itens, só será admitida a contratação dos itens nas seguintes hipóteses.

7.3.1. contratação da totalidade dos itens de grupo, respeitadas as proporções de quantitativos definidos no certame; ou

7.3.2. contratação de item isolado para o qual o preço unitário adjudicado ao vencedor seja o menor preço válido ofertado para o mesmo item na fase de lances

7.4. A ata de realização da sessão pública do pregão, contendo a relação dos licitantes que aceitarem cotar os bens ou serviços com preços iguais ao do licitante vencedor do certame, compõe anexo a esta Ata de Registro de Preços, nos termos do art. 11, §4º do Decreto n. 7.892, de 2014.

Para firmeza e validade do pactuado, a presente Ata foi lavrada em 02 (duas) vias de igual teor, que, depois de lida e achada em ordem, vai assinada pelas partes *e encaminhada cópia aos demais órgãos participantes (se houver).*

Local e data
Assinaturas

Representante legal do órgão gerenciador e representante(s) legal(is) do(s) fornecedor(s) registrado(s)