1365897 00135.217382/2019-00

MINISTÉRIO DA MULHER, DA FAMÍLIA E DOS DIREITOS HUMANOS
COORDENAÇÃO DE PROCEDIMENTOS LICITATÓRIOS
SCS Quadra 09 - Lote C, Ed. Parque Cidade Corporate, Torre-A, 10º Andar
Brasília, DF. CEP 70308-200. - http://www.mdh.gov.br

EDITAL DE LICITAÇÃO Nº 5/2020

PROCESSO Nº 00135.217382/2019-00

Torna-se público que o Ministério da Mulher, da Família e dos Direitos Humanos - MMFDH, por meio da Coordenação-Geral de Logística, sediada no Setor Comercial Sul, Bloco B, Quadra 09, Lote C, Edifício Parque Cidade Corporate, Torre A, CEP 70308-200, na cidade de Brasília/DF, realizará licitação, na modalidade PREGÃO, na forma ELETRÔNICA, **com critério de julgamento por menor preço do item**, sob a forma de execução indireta, no regime de empreitada por preço global, nos termos da Lei nº 10.520, de 17 de julho de 2002,da Lei nº 8.248, de 22 de outubro de 1991, do Decreto nº 10.024, de 20 de setembro de 2019, do Decreto 9.507, de 21 de setembro de 2018, do Decreto nº 7.746, de 05 de junho de 2012, do Decreto nº 7.174, de 12 de maio de 2010, da Instrução Normativa SGD/ME nº 1, de 4 de abril de 2019, das Instruções Normativas SEGES/MP nº 05, de 26 de maio de 2017 e nº 03, de 26 de abril de 2018 e da Instrução Normativa SLTI/MPOG nº 01, de 19 de janeiro de 2010, 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: 06/11/2020
Horário: 9:00h
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 Solução Integrada de Segurança - Next Generation Firewall (NGFW) corporativo em alta disponibilidade para prover segurança e proteção da rede de computadores, contemplando gerência unificada com garantia de funcionamento pelo período de 60 (sessenta) meses, 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. **DOS RECURSOS ORÇAMENTÁRIOS**

2.1. As despesas para atender a esta licitação estão programadas em dotação orçamentária própria, prevista no orçamento da União para o exercício de 2020, na classificação abaixo:

Gestão/Unidade: 00001/810005

Fonte: 0100

Programa de Trabalho:14.122.0032.2000.0001

Elemento de Despesa: 44.90.52

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, assumir 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 da senha, 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. Não poderão participar desta licitação os interessados:

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

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

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

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

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

4.2.6. entidades empresariais que estejam reunidas em consórcio;

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

4.2.8. instituições sem fins lucrativos (parágrafo único do art. 12 da Instrução Normativa/SEGES nº 05/2017)

4.2.8.1. sociedades cooperativas, considerando a vedação contida no art. 10 da Instrução Normativa SEGES/MP nº 5, de 2017, bem como o disposto no Termo de Conciliação firmado entre o Ministério Público do Trabalho e a AGU.

4.3. Nos termos do art. 5º do Decreto nº 9.507, de 2018, é vedada a contratação de pessoa jurídica na qual haja administrador ou sócio com poder de direção, familiar de:

a) detentor de cargo em comissão ou função de confiança que atue na área responsável pela demanda ou contratação; ou

b) de autoridade hierarquicamente superior no âmbito do órgão contratante.

4.3.1. Para os fins do disposto neste item, considera-se familiar o cônjuge, o companheiro ou o parente em linha reta ou colateral, por consanguinidade ou afinidade, até o terceiro grau (Súmula Vinculante/STF nº 13, art. 5º, inciso V, da Lei nº 12.813, de 16 de maio de 2013 e art. 2º, inciso III, do Decreto n.º 7.203, de 04 de junho de 2010);

4.4. Nos termos do art. 7° do Decreto n° 7.203, de 2010, é vedada, ainda, a utilização, na execução dos serviços contratados, de empregado da futura Contratada que seja familiar de agente público ocupante de cargo em comissão ou função de confiança neste órgão contratante.

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

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

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

4.5.1.2. 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 ou sociedade cooperativa.

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

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

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

4.5.5. 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;

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

4.5.7. 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;

4.5.8. 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.

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

4.5.9.1. a assinalação do campo "não" apenas produzirá o efeito de o licitante não ter direito ao tratamento favorecido previsto no Decreto nº 7.174, de 2010.

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, proposta com a descrição do objeto ofertado e o preço, até a data e o horário estabelecidos para a abertura da sessão pública, quando, então, encerrar-se-á automaticamente a etapa de envio desse documento.

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. PREENCHIMENTO DA PROPOSTA

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

6.1.1. V*alor unitário e total do item*

6.1.2. Descrição do objeto, contendo as informações similares à especificação do Termo de Referência

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 na prestação dos serviços, apurados mediante o preenchimento do modelo de Planilha de Custos e Formação de Preços, conforme anexo deste Edital;

6.3.1. A Contratada deverá arcar com o ônus decorrente de eventual equívoco no dimensionamento dos quantitativos de sua proposta, inclusive quanto aos custos variáveis decorrentes de fatores futuros e incertos, tais como os valores providos com o quantitativo de vale transporte, devendo complementá-los, caso o previsto inicialmente em sua proposta não seja satisfatório para o atendimento do objeto da licitação, exceto quando ocorrer algum dos eventos arrolados nos incisos do §1° do artigo 57 da Lei n° 8.666, de 1993.

6.3.2. Caso o eventual equívoco no dimensionamento dos quantitativos se revele superior às necessidades da contratante, a Administração deverá efetuar o pagamento seguindo estritamente as regras contratuais de faturamento dos serviços demandados e executados, concomitantemente com a realização, se necessário e cabível, de adequação contratual do quantitativo necessário, com base na alínea "b" do inciso I do art. 65 da Lei n. 8.666/93 e nos termos do art. 63, §2° da IN SEGES/MPDG n. 5/2017.

6.4. A empresa é a única responsável pela cotação correta dos encargos tributários. Em caso de erro ou cotação incompatível com o regime tributário a que se submete, serão adotadas as orientações a seguir:

6.4.1. cotação de percentual menor que o adequado: o percentual será mantido durante toda a execução contratual;

6.4.2. cotação de percentual maior que o adequado: o excesso será suprimido, unilateralmente, da planilha e haverá glosa, quando do pagamento, e/ou redução, quando da repactuação, para fins de total ressarcimento do débito.

6.5. Se o regime tributário da empresa implicar o recolhimento de tributos em percentuais variáveis, a cotação adequada será a que corresponde à média dos efetivos recolhimentos da empresa nos últimos doze meses, devendo o licitante ou contratada apresentar ao pregoeiro ou à fiscalização, a qualquer tempo, comprovação da adequação dos recolhimentos, para os fins do previsto no subitem anterior.

6.6. Independentemente do percentual de tributo inserido na planilha, no pagamento dos serviços, serão retidos na fonte os percentuais estabelecidos na legislação vigente.

6.7. A apresentação das propostas implica obrigatoriedade do cumprimento das disposições nelas contidas, em conformidade com o que dispõe o Termo de Referência, assumindo o proponente o compromisso de executar os serviços nos seus termos, bem como de fornecer os materiais, equipamentos, ferramentas e utensílios necessários, em quantidades e qualidades adequadas à perfeita execução contratual, promovendo, quando requerido, sua substituição.

6.8. 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.

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

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

6.10.1. O descumprimento das regras supramencionadas pela Administração por parte dos contratados pode ensejar a responsabilização pelo 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, ilegalidades, ou não apresentem as especificações 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 de sistema eletrônico, sendo imediatamente informados do seu recebimento e do valor consignado no registro.

7.5.1. O lance deverá ser ofertado pelo valor total 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 entre os lances, que incidirá tanto em relação aos lances intermediários quanto em relação à proposta que cobrir a melhor oferta deverá ser de R$100,00 (cem reais).

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 lances 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 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 tempos superior a dez minutos, a sessão pública será suspensa e reiniciada somente após decorridas vinte e quatro horas após a comunicação do fato 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. prestados por empresas brasileiras;

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

7.26.3. 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.

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 prevista deste 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 2 (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. 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. 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 de 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 nº 10.024/2019.

8.2. A análise da exequibilidade da proposta de preços deverá ser realizada com o auxílio da Planilha de Custos e Formação de Preços, a ser preenchida pelo licitante em relação à sua proposta final, conforme anexo deste Edital.

8.3. A Planilha de Custos e Formação de Preços deverá ser encaminhada pelo licitante exclusivamente via sistema, no prazo de 2 (duas) horas, contado da solicitação do Pregoeiro, com os respectivos valores adequados ao lance vencedor e será analisada pelo Pregoeiro no momento da aceitação do lance vencedor.

8.4. A inexequibilidade dos valores referentes a itens isolados da Planilha de Custos e Formação de Preços não caracteriza motivo suficiente para a desclassificação da proposta, desde que não contrariem exigências legais.

8.5. Será desclassificada a proposta ou o lance vencedor, nos termos do item 9.1 do Anexo VII-A da In SEGES/MPDG n. 5/2017, que:

8.5.1. não estiver em conformidade com os requisitos estabelecidos neste edital;

8.5.2. contenha vício insanável ou ilegalidade;

8.5.3. não apresente as especificações técnicas exigidas pelo Termo de Referência;

8.5.4. 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.

8.5.4.1. Quando o licitante não conseguir comprovar que possui ou possuirá recursos suficientes para executar a contento o objeto, será considerada inexequível a proposta de preços ou menor lance que:

8.5.4.2. for insuficiente para a cobertura dos custos da contratação, 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.

8.5.4.3. apresentar um ou mais valores da planilha de custo que sejam inferiores àqueles fixados em instrumentos de caráter normativo obrigatório, tais como leis, medidas provisórias e convenções coletivas de trabalho vigentes.

8.6. Se houver indícios de inexequibilidade da proposta de preço, ou em caso da necessidade de esclarecimentos complementares, poderão ser efetuadas diligências, na forma do § 3° do artigo 43 da Lei n° 8.666, de 1993 e a exemplo das enumeradas no item 9.4 do Anexo VII-A da IN SEGES/MPDG N. 5, de 2017, para que a empresa comprove a exequibilidade da proposta.

8.7. Quando o licitante apresentar preço final inferior a 30% (trinta por cento) da média dos preços ofertados para o mesmo item, e a inexequibilidade da proposta não for flagrante e evidente pela análise da planilha de custos, não sendo possível a sua imediata desclassificação, será obrigatória a realização de diligências para aferir a legalidade e exequibilidade da proposta.

8.8. 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.

8.8.1. Na hipótese de necessidade de suspensão de sessão pública para a realização de diligências, com vista 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.

8.9. O Pregoeiro poderá convocar o licitante para enviar documento digital complementar, por meio de funcionalidade disponível no sistema, no prazo de 2 (duas) horas, sob pena de não aceitação da proposta.

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

8.9.2. Dentre os documentos passíveis de solicitação pelo Pregoeiro, destacam-se as planilhas de custo readequadas com o valor final ofertado.

8.10. Todos os dados informados pelo licitante em sua planilha deverão refletir com fidelidade os custos especificados e a margem de lucro pretendida.

8.11. O Pregoeiro analisará a compatibilidade dos preços unitários apresentados na Planilha de Custos e Formação de Preços com aqueles praticados no mercado em relação aos insumos e também quanto aos salários das categorias envolvidas na contratação;

8.12. Erros no preenchimento da planilha não constituem motivo para a desclassificação da proposta. A planilha poderá ser ajustada pelo licitante, no prazo indicado pelo Pregoeiro, desde que não haja majoração do preço.

8.12.1. O ajuste de que trata este dispositivo se limita a sanar erros ou falhas que não alterem a substância das propostas.

8.12.2. Considera-se erro no preenchimento da planilha passível de correção a indicação de recolhimento de impostos e contribuições na forma do Simples Nacional, quando não cabível esse regime.

8.13. Para fins de análise da proposta quanto ao cumprimento das especificações do objeto, poderá ser colhida a manifestação escrita do setor requisitante do serviço ou da área especializada no objeto.

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

8.15. Havendo necessidade, o Pregoeiro suspenderá a sessão, informando no “chat” a nova data e horário para a sua continuidade.

8.16. 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. 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 licitante será verificada por meio do SICAF, nos documentos por ele abrangidos, em relação à habilitação jurídica, à regularidade fiscal e à qualificação econômica financeira, 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 2 (duas) horas, sob pena de inabilitação.

9.4. Somente haverá a necessidade de comprovação do preenchimento de requisitos mediante a 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 diferentes números de documentos pertinentes ao CND e ao CRF/FGTS, quando for comprovada a centralização do recolhimento dessas contribuições.

9.7. Ressalvado o disposto do item 5.3, os licitantes deverão encaminhar, nos termos deste Edital, a documentação 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. decreto de autorização, em se tratando de sociedade empresária estrangeira em funcionamento no País;

9.8.7. 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 municipal, 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 Municipal 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 municipais relacionados ao objeto licitatório, deverá comprovar tal condição mediante a apresentação de declaração da Fazenda Municipal do seu domicílio ou sede, ou outra equivalente, na forma da lei;

9.10. **Qualificação Econômico-Financeira:**

9.10.1. certidão negativa de falência expedida pelo distribuidor da sede do licitante;

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

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

9.10.2.3. comprovação da boa situação financeira da empresa mediante obtenção de índices de Liquidez Geral (LG), Solvência Geral (SG) e Liquidez Corrente (LC), superiores a 1 (um), obtidos pela aplicação das seguintes fórmulas:

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

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

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

9.10.3. 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 patrimônio líquido de 10% (dez por cento) do valor total estimado da contratação ou do item pertinente.

9.11. **Qualificação Técnica:**

9.11.1. Comprovação de aptidão para a prestação dos serviços em características, quantidades e prazos compatíveis com o objeto desta licitação, ou com o item pertinente, mediante a apresentação de atestado(s) fornecido(s) por pessoas jurídicas de direito público ou privado.

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

9.11.1.2. O atestado de capacidade técnica deverá ser fornecido em nome do licitante, e ser expedido por pessoa jurídica de direito público ou privado, com a comprovação de que a empresa tenha fornecido objeto compatível em quantidade e especificidade com o objeto licitado.

9.11.1.3. Será exigido, para a comprovação de execução de objeto, que a licitante vencedora apresente documento que ateste o fornecimento de 01 (um) equipamento similar para o respectivo item, caso a

licitante obtenha menor preço em relação ao item.

9.11.1.4. O atestado deverá ser obrigatoriamente emitido por pessoa jurídica de direito público ou privado, devendo ainda ser emitido em papel timbrado e conter:

a) Razão Social, CNPJ e Endereço Completo da Empresa Emitente;

b) Razão Social da Contratada;

c) Número e vigência do contrato, se for o caso;

d) Objeto do contrato;

e) Declaração de que foram atendidas as expectavas do cliente quanto ao cumprimento de cronogramas pactuados;

f) Local e Data de Emissão;

g) Identificação do responsável pela emissão do atestado, Cargo, Contato (telefone e correio eletrônico);

h) Assinatura do responsável pela emissão do atestado;

i) Devem ser originais ou autenticados, se cópias, e legíveis.

9.11.1.5. No caso de apresentação de atestado de empresas privadas, não serão considerados aqueles apresentados por empresas participantes do mesmo grupo empresarial da contratada. Serão consideradas como de mesmo grupo, empresas controladas pela contratada, ou que tenham pelo menos uma pessoa física ou jurídica que seja sócia da empresa emitente e da contratada.

9.11.2. Os atestados deverão referir-se a serviços prestados no âmbito de sua atividade econômica principal ou secundária especificadas no contrato social vigente;

9.11.3. Somente serão aceitos atestados expedidos após a conclusão do contrato ou se decorrido, pelo menos, um ano do início de sua execução, exceto se firmado para ser executado em prazo inferior, conforme item 10.8 do Anexo VII-A da IN SEGES/MPDG n. 5, de 2017.

9.11.4. O licitante disponibilizará todas as informações necessárias à comprovação da legitimidade dos atestados apresentados, apresentando, dentre outros documentos, cópia do contrato que deu suporte à contratação, endereço atual da contratante e local em que foram prestados os serviços, consoante o disposto no item 10.10 do Anexo VII-A da IN SEGES/MPDG n. 5/2017.

9.11.5. O licitante deverá entregar preenchido e assinado pelo responsável legal, o **Termo de Integridade,** conforme modelo Anexo G do TR, que deverá ser assinado quando da assinatura do contrato, sob pena de desclassificação da licitante.

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 microempresa, empresa de pequeno porte ou sociedade cooperativa equiparada, 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. 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 2 (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. apresentar a planilha de custos e formação de preços, devidamente ajustada ao lance vencedor, em conformidade com o modelo anexo a este instrumento convocatório.

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

10.1.4. A licitante deverá ainda informar em sua proposta o endereço no sítio oficial do fabricante, de modo que possam ser evidenciadas as especificações técnicas exigidas no edital e informadas na proposta de preços;

10.1.5. A licitante deverá Informar os meios de comunicação (e-mail, número de telefone 0800, serviço de abertura de chamado via web) para abertura de chamados;

10.1.6. Deverá informar o site do fabricante do equipamento na Internet, onde se possam efetuar consultas;

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 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. O Pregoeiro declarará o vencedor e, depois de decorrida a fase de regularização fiscal e trabalhista de microempresa ou empresa de pequeno porte, se for o caso, concederá 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, 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**

14.1. Será exigida a prestação de garantia na presente contratação, conforme regras constantes do Termo de Referência.

15. **DO TERMO DE CONTRATO OU INSTRUMENTO EQUIVALENTE**

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

15.2. 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.

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

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

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

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

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

15.3.3. 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.

15.4. O prazo de vigência da contratação é de 12 meses prorrogáveis conforme previsão no instrumento contratual ou no termo de referência.

15.5. 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.

15.5.1. 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.

15.5.2. 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.

15.6. Na assinatura do contrato, 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.

15.7. Na hipótese de o vencedor da licitação não comprovar as condições de habilitação consignadas no edital ou se recusar a assinar o contrato, 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.

16. **DO REAJUSTAMENTO EM SENTIDO GERAL**

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

17. **DO RECEBIMENTO DO OBJETO E DA FISCALIZAÇÃO**

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

18. **DAS OBRIGAÇÕES DA CONTRATANTE E DA CONTRATADA**

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

19. **DO PAGAMENTO**

19.1. As regras acerca do pagamento são as estabelecidas no Termo de Referência, anexo a este Edital.

19.1.1. É admitida a cessão de crédito decorrente da contratação de que trata este Instrumento Convocatório, nos termos do previsto na minuta contratual anexa a este Edital.

20. **DAS SANÇÕES ADMINISTRATIVAS**

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

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

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

20.1.3. apresentar documentação falsa;

20.1.4. deixar de entregar os documentos exigidos no certame;

20.1.5. ensejar o retardamento da execução do objeto;

20.1.6. não mantiver a proposta;

20.1.7. cometer fraude fiscal;

20.1.8. comportar-se de modo inidôneo;

20.2. 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.

20.3. 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.

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

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

20.4.2. Multa de 10% (dez por cento) sobre o valor estimado do(s) item(s) prejudicado(s) pela conduta do licitante;

20.4.3. 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;

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

20.4.5. 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;

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

20.6. 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.

20.7. 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.

20.8. 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.

20.9. 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.

20.10. 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.

20.11. 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.

20.12. As penalidades serão obrigatoriamente registradas no SICAF.

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

21. DA IMPUGNAÇÃO AO EDITAL E DO PEDIDO DE ESCLARECIMENTO

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

21.2. A impugnação poderá ser realizada por forma eletrônica, pelo e-mail: licitacao@mdh.gov.br, ou por petição dirigida ou protocolada no endereço constante no preâmbulo deste Edital.

21.3. 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.

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

21.5. 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.

21.6. O pregoeiro responderá aos pedidos de esclarecimentos no prazo de dois dias úteis, contados da data do recebimento do pedido e poderá requisitar subsídios formais aos responsáveis pela elaboração do

edital e dos anexos.

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

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

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

22. **DAS DISPOSIÇÕES GERAIS**

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

22.2. 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.

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

22.4. 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.

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

22.6. 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.

22.7. 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.

22.8. 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.

22.9. 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.

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

22.11. O Edital está disponibilizado, na íntegra, no endereço eletrônico https://www.gov.br/mdh/pt-br, e também poderão ser lidos e/ou obtidos no endereço descrito no preâmbulo deste Edital, nos dias úteis, no horário das 09:00 horas às 17:00 horas, mesmo endereço e período no qual os autos do processo administrativo permanecerão com vista franqueada aos interessados.

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

22.12.1. ANEXO I - Termo de Referência;

22.12.2. ANEXO II - Minuta de Termo de Contrato;

22.12.3. ANEXO III- Estudo Técnico Preliminar da Contratação

Brasília - DF, ... de ..... de 2020.

autoridade competente

0.1.

Documento assinado eletronicamente por **Maria Aparecida Fabri Pessanha**, **Pregoeiro(a)**, em 22/10/2020, às 09:21, conforme o § 1º do art. 6º e art. 10 do Decreto nº 8.539/2015.

A autenticidade deste documento pode ser conferida no site https://sei.mdh.gov.br/autenticidade, informando o código verificador **1365897** e o código CRC **F48F4DE7**.

1366522 00135.217382/2019-00

MINISTÉRIO DA MULHER, DA FAMÍLIA E DOS DIREITOS HUMANOS
COORDENAÇÃO DE INFRAESTRUTURA E SERVIÇOS
Setor Comercial Sul, quadra 09, Edifício Parque Cidade Corporate, Torre A
Brasília, DF. CEP 70308-200. - http://www.mdh.gov.br

TERMO DE REFERÊNCIA

PROCESSO Nº 00135.217382/2019-00

1. DO OBJETO

1.1. Aquisição de Solução Integrada de Segurança - Next Generation Firewall (NGFW) corporativo em alta disponibilidade para prover segurança e proteção da rede de computadores, contemplando gerência unificada com garantia de funcionamento pelo período de 60 (sessenta) meses.

2. DESCRIÇÃO DA SOLUÇÃO DE TIC

2.1. A solução proposta trata de hardware (equipamento) do tipo Next Generation Firewall. As especificações e o valor unitário se referem a 1 (um) equipamento.

2.1.1. Para atendimento da demanda do Ministério, e considerando a criticidade da solução a ser contratada, faz-se necessária a disponibilização de dois equipamentos, que trabalharão em cluster, promovendo assim alta disponibilidade.

2.2. Decorrente da estruturação da área TI do MMFDH, constata-se a necessidade de aquisição de uma solução de segurança de perímetro - firewall, para o data center, que tem por objetivo aplicar as diretrizes da Política de Segurança da Informação e Comunicação, PoSIC, visando atender plenamente às demandas atuais e futuras de segurança e vazão de tráfego.

2.3. Uma solução de Firewall consiste em um dispositivo de rede de computadores que tem por objetivo aplicar regras de segurança a uma determinada rede. Sua função consiste em regular o tráfego de dados entre redes distintas e impedir a transmissão e/ou recepção de acessos nocivos ou não autorizados de uma rede para outra (invasão), protegendo assim os recursos de hardware e software. Este equipamento controla todas as comunicações que passam de uma rede a outra, permitindo ou negando seu tráfego. Nesta função, um firewall examina o tipo de serviço, tipo de portas, protocolos, podendo até mesmo inspecionar pacotes de informação.

2.4. Estão incluídos todos os softwares e suas licenças de uso, gerenciamento centralizado, serviços de implantação, garantia de atualização contínua e suporte técnico durante o período de garantia com repasse de conhecimento da solução a fim de atender às necessidades do Ministério da Mulher, da Família e dos Direitos Humanos.

2.5. O Ministério da Mulher, da Família e dos Direitos Humanos assim como os diversos órgãos da esfera pública, necessita de proteção e segurança sobre o conteúdo armazenado e manipulado internamente nos respectivos ambientes para que sejam mantidas a confidencialidade, a integridade e a disponibilidade das informações existentes.

2.6. Apresenta-se a seguir detalhamento do item a ser contratado:

Item	Descrição	CATMAT	Qtde	Valor Unitário Máximo Aceitável	Valor Máximo Aceitável
1	Solução de Next Generation Firewall (hardware), incluindo IPS, prevenção contra ameaças de vírus, spywares, malwares “Zero Day”, Filtro de URL com suporte técnico, licenciamento e garantia por 60 meses.	BR0150100	2	R$ 994.461,27	**R$ 1.988.922,54**

2.7. Portanto, conclui-se que a contratação terá valor estimado de **R$ 1.988.922,54 (Um milhão, novecentos e oitenta e oito mil, novecentos e vinte e dois reais e cinquenta e quatro centavos)**, sendo este o valor máximo aceito pelo Ministério, aceito para contratação.

3. **JUSTIFICATIVA E OBJETIVO DA CONTRATAÇÃO**

3.1. O MMFDH detém vários sistemas sob sua responsabilidade. Tais sistemas abarcam muitas informações importantes para a tomada de decisão e eficiência dos processos em todas as áreas do órgão. Exemplo disso são as informações contidas no Sistema Eletrônico de Informações (SEI), o qual foi implantado em meados de 2015, otimizando o trâmite de processos administrativos no Órgão, agora realizado eletronicamente, eliminando a tramitação de processos físicos (papel).

3.2. Assim como o SEI, outros sistemas que lidam com informações sensíveis merecem a devida atenção quanto à segurança e proteção de ataques maliciosos por crackers ou criminosos do gênero, segue o exemplo de alguns sistemas.

a) O documento (1167123) possui a listagem dos sistemas que são executados na infraestrutura do MMFDH.

b) A solução de firewall atual em uso trabalha com os seguintes serviços ativos: anti malware, Sistema de Prevenção de Intrusos - IPS e Web Filtro, porém é possível observar picos de processamento de até 80% quanto ao uso do equipamento atual.

3.3. Existe ainda necessidade de expandir os acessos VPN SSL tendo em vista que o atual número licenças é insuficiente para as atribuições da TI e dos demais usuários.

3.4. **Alinhamento aos Instrumentos de Planejamento Institucionais**

ALINHAMENTO AOS PLANOS ESTRATÉGICOS	
ID	**Objetivos Estratégicos**
A5	Prover soluções tecnológicas integradas, seguras e de alto desempenho

ALINHAMENTO AO PDTIC 2017-2019 *	
ID	**Necessidades Elencadas no PDTIC**
1	Modernização da Infraestrutura Tecnológica de Software e Soluções de TI;
2	Estruturação de Plataforma de Gestão de Serviços para o Cidadão;
3	Manutenção da Continuidade Operacional;

(*) Trata-se de uma demanda iniciada na vigência do PDTIC 2017-2019.

A Equipe de Planejamento da Contratação foi devidamente atualizada PORTARIA Nº 6, DE 10 DE FEVEREIRO DE 2020, Dispõe sobre a criação da equipe de planejamento para a Contratação de empresa especializada no fornecimento de soluções de segurança de redes compostas de firewall corporativo e multifuncional para prover segurança e proteção da rede de computadores, para atendimento das necessidades do Ministério da Mulher, da Família e dos Direitos Humanos.

ALINHAMENTO AOS PLANOS ESTRATÉGICOS	
ID	**Objetivos Estratégicos**
A5	Prover soluções tecnológicas integradas, seguras e de alto desempenho

ALINHAMENTO AO PDTIC 2020-2021			
ID	**Ação do PDTIC**	**ID**	**Meta do PDTIC associada**
A52	Adquirir Solução de Firewall	M5	Aprimorar a segurança e o controle no acesso, armazenamento e disponibilidade da informação

Alinhamento ao PAC								
Nº	**Tipo**	**Código**	**Descrição**	**Descrição**	**Unidade de**	**Quantidade a ser**	**Ação**	**Justificativa para**

do Item	do item	do item		sucinta do objeto	fornecimento	contratada ou adquirida	orçamentária	aquisição ou contratação
123	Serviço	150100	FIREWALL	FIREWALL	CGTI	2 Unidades	2000 - Administração da Unidade	Manter a segurança da informação do MMFDH

3.5. **Estimativa da demanda**

3.5.1. Atender a essa demanda por alta qualidade e eficiência com economia, confiabilidade, flexibilidade, agilidade e racionalização de fluxos de trabalho, é preocupação constante da alta direção dos órgãos, o que tornou a Tecnologia da Informação e Comunicação ferramenta estratégica que deve estar alinhada com as áreas de negócios da Instituição.

3.5.2. Os seguintes fatores motivaram essa contratação:

I - Os ataques cibernéticos estão cada vez mais especializados e mais perigosos;

II - Necessidade cada vez maior de manter a disponibilidade dos sistemas;

III - Término da garantia e licenciamento do produto atual.

3.6. **Resultados e Benefícios a Serem Alcançados**

3.6.1. A contratação visa como benefício a conformidade com os objetivos estratégicos do Ministério, baseado em padrões e frameworks de mercados bem como reduzir os esforços empregados no controle da Segurança da Informação quanto a questões legais no que tangem aos assuntos relacionados à Governança, Risco e Conformidade.

3.6.2. A modernização pretendida permitirá ao Ministério da Mulher, da Família e dos Direitos Humano agregar disponibilidade, desempenho e qualidade de serviços a todo o corpo funcional, dando um salto qualitativo na adoção de soluções que visam atender de forma eficiente e racional à demanda operacional interna verificada para acesso imediato às informações e sistemas corporativos.

3.6.3. Desse modo, com a implementação desta nova solução será possível:

I - Maior proteção contra ataques de cyber criminosos;

II - Maior disponibilidade de aplicações extremamente críticas;

III - Manter a solução atual de firewall com cluster;

IV - Redução de custos e esforços associados ao tratamento de infecções do ambiente tecnológico.

4. **DA CLASSIFICAÇÃO DOS BENS COMO COMUNS**

4.1. O objeto a ser contratado enquadra-se na categoria de bens comuns de que trata o parágrafo único do art. 1º da Lei nº 10.520, de 17 de julho de 2002 e o Decreto nº 10.024, de 20 de setembro de 2019, por possuir padrões de desempenho e qualidade objetivamente definidos, mediante as especificações usuais do mercado, podendo, portanto, ser licitado por meio da modalidade Pregão na forma eletrônica.

4.2. A licitação em tela, objeto deste Termo de Referência, será levada a cabo por meio de seleção de propostas pela modalidade de Pregão Eletrônico, do tipo Menor Preço Global, na forma prevista no art. 45, §1º, I da Lei nº 8.666, de 1993.

4.3. Ao amparo da Lei nº 10.520, de 2002, e Decreto nº 10.024, de 20 de setembro de 2019, o objeto afigura-se à definição de serviço comum, ou seja, cujos padrões de desempenho e qualidade possam ser objetivamente definidos pelo edital, por meio de especificações usuais no mercado, senão vejamos:

4.4. Conforme advoga Marçal Justen Filho, *in verbis*: “bem ou serviço comum é aquele que se apresenta sob identidade e características padronizadas e que se encontra disponível, a qualquer tempo, num mercado próprio”.

4.5. Portanto, a definição de “bens e serviços comuns” inclui o simples, o padronizado, o rotineiro e ainda os que possam ser objetivamente descritos, sendo este o entendimento do Tribunal de Contas da União. Podendo, portanto, ser licitado por meio da modalidade Pregão.

5. **ENQUADRAMENTO EM SOLUÇÃO DE TI E REQUISITOS LEGAIS**

5.1. A instrução normativa nº 1, de 4 de abril de 2019 considera, em seu inciso VII, do art. 2º, que solução de TIC: conjunto de bens e/ou serviços que apoiam processos de negócio, mediante a conjugação de recursos, processos e técnicas utilizados para obter, processar, armazenar, disseminar e fazer uso de informações

5.2. Em virtude da consideração acima, o entendimento acerca da conceituação apresentada na IN n° 01/2019 SGD/ME se baseia na integração de bens, serviços de TI e automação, tendo como finalidade o alcance dos resultados

pretendidos pela contratação, que, no processo em questão, refere-se à solução de softwares e serviços especializados no produto com repasse de conhecimento e serviços técnicos especializados .

5.3. Considerando que uma solução de TI engloba todos os elementos (bens, serviços de TI e automação) necessários que se integram para o alcance dos resultados pretendidos com a contratação, de modo a atender à necessidade que a desencadeou, pode-se afirmar que a contratação em questão compreende uma solução de tecnologia, uma vez que compreende uma solução integrada de software e serviços especializados numa infraestrutura computacional própria do MMFDH.

5.4. Portanto, a contratação ora pretendida enquadra-se em solução de TI, pois refere-se à contratação de uma solução de tecnologia da informação o qual deverá seguir o estabelecido na IN n° 01/2019 SGD/ME que dispõe sobre o processo de contratação de Soluções de Tecnologia da Informação pelos órgãos integrantes do Sistema de Administração dos Recursos de Informação e Informática (SISP) do Poder Executivo Federal.

5.5. O objeto a ser contratado enquadra-se na categoria de bens comuns, de que tratam a Lei nº 10.520/02 e nº Decreto nº 10.024/2019, por possuir padrões de desempenho e características gerais e específicas, que podem ser definidos de forma objetiva nas especificações técnicas, que são usualmente encontradas no mercado, podendo, portanto, ser licitado por meio da modalidade Pregão.

6. ESPECIFICAÇÃO DOS REQUISITOS DA CONTRATAÇÃO

6.1. Requisitos Prazo e do local de entrega

6.1.1. Os objetos especificados neste Termo de Referência deverão ser entregues pela CONTRATADA no endereço:

- UNIDADE - MMFDH - Parque Cidade Corporate;
- LOCALIDADE - SCS Quadra 09 - Lote C, Ed. Parque Cidade Corporate, Torre-A, Sala 902-G, Asa Sul; CEP: 70.308-200

6.1.2. A CONTRATANTE solicitará a entrega dos equipamentos por meio de Ordem de Serviço - OS, que deverá ser cumprida no prazo máximo de até 45 (quarenta e cinco) dias corridos, a partir da sua emissão.

6.1.3. A OS indicará a quantidade, os endereços de entrega e da instalação e nome do responsável pelo recebimento, acompanhado de e-mail e/ou telefone para contato, além da solicitação de entrega do Projeto de Instalação - PI.

6.1.4. A CONTRATADA deverá informar à CONTRATANTE, quando da entrega dos equipamentos com, no mínimo, 5 (cinco) dias corridos de antecedência, ficando a CONTRATADA responsável pelo transporte e entrega dos equipamentos e partes componentes da solução integrada de segurança da informação.

6.1.5. A CONTRATADA será responsável por elaborar e entregar o PI dos equipamentos em até 10 (dez) dias corridos, contados a partir da solicitação da CONTRATANTE, constante no item 6.2, ou seja, da emissão da OS.

6.1.6. A CONTRATANTE solicitará a instalação dos equipamentos e da solução por meio de uma Ordem de Serviço - OS, que deverá ser cumprida no prazo máximo de até 15 (quinze) dias corridos, a partir da sua emissão.

6.1.7. A substituição do equipamento que apresentar divergência na especificação técnica, falhas de componentes, defeitos de fabricação e operação ou qualquer outro defeito apresentado durante o transporte, a entrega e a instalação dos equipamentos deverão ser efetuadas em até 5 (cinco) dias úteis, contados a partir da notificação da ocorrência por parte da CONTRATANTE, observado o disposto neste TR.

6.1.8. A CONTRATADA e a CONTRATANTE deverão aprovar o Projeto Instalação - PI em até 2 (dois) dias úteis após a instalação, observadas as condições estabelecidas neste TR.

6.2. Projeto de instalação - PI

6.2.1. No Projeto de Instalação - PI deverá, no mínimo, relação de materiais e serviços que comporão a entrega, croquis e plantas de instalação, topologia física e lógica, detalhamento da configuração do equipamento, relatório de vistoria, planos de migração e ativação e plano de retorno.

6.2.2. Cabe a CONTRATADA verificar durante o planejamento da instalação e vistorias, o padrão da CONTRATANTE quanto à: arquitetura de cabeamento, padrão de conectores ópticos, patch panels, tomadas elétricas e entregar os equipamentos dentro desses padrões ou com as adaptações necessárias.

6.2.3. A CONTRATADA será responsável por elaborar e entregar o PI dos equipamentos em até 10 (dez) dias corridos, contados a partir da solicitação da CONTRATANTE.

6.2.4. A CONTRATANTE fará análise e validação do Projeto de Instalação - PI, em até 3 (três) dias úteis, apontando as devidas correções e ou ajustes no documento, ficando a CONTRATADA responsável por ajustar o plano em até 2 (dois) dias úteis, a partir da comunicação da CONTRATANTE das não conformidades e das alterações necessárias, apontadas pela CONTRATANTE.

6.2.5. Após entrega dos equipamentos e do Projeto Provisório de Instalação já ajustado pela CONTRATADA, a CONTRATANTE emitirá, em até 5 (cinco) dias úteis, a Ordem de Serviço da Instalação – OS.

6.3. **Da instalação**

6.3.1. Os equipamentos descritos no ANEXO A deverão ser entregues instalados e operacionais, incluindo todos os acessórios necessários para o seu pleno funcionamento, no prazo do item 6.5, deste T.R.

6.3.2. Fica a critério da CONTRATANTE, definir o horário de instalação e configuração dos equipamentos e softwares, podendo tais procedimentos serem executados em feriados ou finais de semana e em horário noturno, conforme as necessidades da CONTRATANTE.

6.3.3. A CONTRATADA deverá fornecer todos os materiais necessários à instalação básica completa, à configuração e ao perfeito funcionamento da totalidade dos itens adquiridos.

6.3.4. Constatada a ocorrência de divergência na especificação técnica, falhas de componentes, defeitos de fabricação e operação ou qualquer outro defeito apresentado durante o transporte, a entrega e a instalação dos equipamentos, fica a CONTRATADA obrigada a providenciar a substituição do equipamento, no prazo do item 6.5.1, sujeitando-se a CONTRATADA às penalidades previstas na legislação vigente e neste edital.

6.3.5. Eventuais despesas de custeio com deslocamento de técnicos da CONTRATADA ao local de instalação, bem como todas as despesas de transporte, diárias, seguro ou quaisquer outros custos envolvidos ficam a cargo exclusivo da CONTRATADA.

6.3.6. A CONTRATADA deverá comunicar a CONTRATANTE a conclusão da instalação dos equipamentos e entregar toda documentação técnica prevista, dentro do prazo definido no item 6.5.2.

6.3.7. A CONTRATADA entregará toda a documentação de instalação física dos equipamentos descritos no ANEXO A, a qual deverá prover nível de informação suficiente para que um técnico possa entender e refazer, caso necessário, as instalações e configurações dos equipamentos adquiridos e implantados.

6.3.8. Após a CONTRATADA concluir toda a instalação dos equipamentos, deixando-os completamente operacionais, e a entrega de toda documentação técnica e do PI, conforme condições e prazos exigidos neste TR, a CONTRATANTE emitirá o Termo de Recebimento Provisório, em até 5 (cinco) dias úteis, contados a partir da comunicação de conclusão da instalação.

6.3.9. Após 15 (quinze) dias úteis da emissão do Termo de Recebimento Provisório, sendo confirmada a operação e desempenho a contento dos equipamentos, nos termos das especificações técnicas e do atestado de homologação, a CONTRATANTE emitirá o Termo de Recebimento Definitivo, verificada a condição estabelecida no item 11.15.1.

6.4. **Escopo do Serviço de Instalação**

6.4.1. A CONTRATADA deverá prover o fornecimento de ferragens e todos os acessórios necessários para instalação dos equipamentos em rack padrão 19” polegadas, conforme descrito no Anexo deste TR.

6.4.2. A CONTRATADA deverá prover o fornecimento de todos os serviços necessários ao planejamento e a execução da instalação, incluindo projetos, configuração dos equipamentos, planos de retorno e contingenciamento, de acordo com as necessidades da CONTRATANTE.

6.4.3. A CONTRATADA deverá executar todas as atividades (físicas e lógicas) de migração dos serviços que se encontrem em operação, incluindo a elaboração do De/Para de portas e a configuração dos equipamentos quando for o caso. A CONTRATANTE deverá disponibilizar a topologia de rede existente para que estas atividades sejam efetuadas.

6.4.4. O plano de retorno e contingenciamento visa garantir a disponibilidade total dos serviços durante e imediatamente após o processo de instalação dos novos equipamentos. Assim, a CONTRATADA, no caso de algum incidente que comprometa os serviços da CONTRATANTE, deverá retornar toda solução conforme estado imediatamente anterior ao processo de instalação. Isso inclui fallback tanto de eventuais configurações alteradas (lógicas), bem como também do respectivo cabeamento (físico).

6.4.5. Para garantir esse perfeito funcionamento e a transição das mudanças, a CONTRATADA deverá disponibilizar, conforme acionamento da CONTRATANTE, durante o período de aceitação previsto neste Termo de Referência, um técnico qualificado, com as respectivas ferramentas necessárias, para solucionar o problema ou restabelecer a rede original em até 2 (duas) horas. Caso não seja obedecido o prazo anterior, a CONTRATADA estará sujeita as penalidades previstas na Tabela 3 - Descumprimento dos Níveis Mínimos de Serviço e Penalidades, conforme severidade apontada na Tabela 2 – Classificação de Eventos.

6.4.6. A CONTRATADA deverá ainda, independente de outras atividades necessárias para garantir a disponibilidade total dos serviços, executar:

a) Todos os backups necessários e relacionados à atividade em questão dos equipamentos da rede em produção;

b) Todos os testes, antes e após as atividades de intervenção e/ou instalação, dos serviços em funcionamento no órgão que tenham relação com os equipamentos em questão.

6.4.7. A CONTRATADA deverá fornecer à equipe de gestão da implantação do órgão demandante, com antecedência mínima de 5 (cinco) dias úteis anteriores a instalação dos equipamentos, em cada localidade indicada pela CONTRATANTE, os nomes dos técnicos, juntamente com os respectivos números de documento de identidade, para que sejam identificados durante o procedimento de instalação.

6.4.8. Os serviços de instalação deverão ser executados e supervisionados por pelo menos 1 (um) técnico certificado pelo fabricante da solução proposta.

6.4.9. Os acessórios, peças e manuais não utilizados durante a instalação, assim como as embalagens dos equipamentos deverão ser removidas pela CONTRATADA antes da emissão do Termo de Recebimento Definitivo, para que não permaneça no local de instalação nenhum resíduo da embalagem ou qualquer peça solta. Tal exigência é condicionante para emissão do Termo de Recebimento Definitivo.

6.4.10. Somente será considerado instalado o equipamento entregue, quando instalado no respectivo rack de 19´´ polegadas, cabeado, operacional, em plenas condições de funcionamento, integrado com a rede local e com capacidade de permitir acesso remoto por parte da equipe da CONTRATANTE.

6.4.11. A CONTRATADA deverá realizar a configuração inicial do equipamento para acesso remoto, assim como prestar o fornecimento de quaisquer outros acessórios e serviços que sejam necessários para a completa operacionalização da rede, de acordo com as necessidades da CONTRATANTE.

6.4.12. Cabe à CONTRATADA realizar a instalação dos firmwares necessários para o funcionamento e a operação completa dos equipamentos, sendo obrigatória a inclusão no equipamento, no momento da instalação, da versão estável mais atual de todos os firmwares.

6.4.13. Todos os softwares necessários à operação dos equipamentos e soluções devem, igualmente, ser entregues instalados e operacionais. Também devem estar incluídos e licenciados (se for o caso) todos os componentes de software básico necessários ao funcionamento dos equipamentos, tais como: sistemas operacionais, controladores de dispositivos e outros pertinentes.

6.5. **Documentação técnica**

6.5.1. A documentação técnica de instalação deverá conter, no mínimo:

a) Descrição dos recursos de hardware e software utilizados nos equipamentos.

b) Lista de todos os elementos instalados contendo: nome e endereço IP do equipamento, juntamente com todas as interconexões básicas (equipamento/porta origem e equipamento/porta destino), local de instalação (prédio, andar, sala), número de série, número do bem utilizado pelo CONTRATANTE, data da instalação, data de aquisição, data de vencimento da garantia.

c) Listagem das configurações dos equipamentos com comentários sobre os principais comandos e as justificativas das opções de parametrização

d) Plantas de instalação e by-plan dos racks usados na instalação dos equipamentos

e) Com relação às configurações dos equipamentos, a CONTRATADA deverá implementar todas as funcionalidades requisitadas pela CONTRATANTE, estando essas minimamente restritas aos requisitos constantes na especificação técnica aqui presentes. Nas implementações dos ativos a serem instalados que dependam de integração com os demais elementos da rede, a CONTRATANTE será responsável por disponibilizar as informações à CONTRATADA, necessárias à harmonização desses novos ativos com os equipamentos preexistentes na rede local da CONTRATANTE.

f) Configuração dos equipamentos segundo as especificações da CONTRATANTE, o que pode incluir, por exemplo, ativação de mecanismos avançados de segurança de rede local e integração com serviços de diretório para autenticação de usuários.

6.5.2. O Projeto de Instalação – PI, conforme estabelecido neste Termo de Referência.

6.5.3. Toda documentação exigida neste Termo de Referência deverá ser entregue em mídia eletrônica.

6.5.4. A documentação técnica deverá garantir a transferência de conhecimento à CONTRATANTE, a fim de proporcionar o nível de informação necessário à operação da rede e possíveis intervenções.

6.6. **Requisitos de segurança**

6.6.1. Os exigidos pela Política de Segurança da Informação e Comunicações do MMFDH.

6.6.2. A Contratada deverá garantir a segurança das informações do MINISTÉRIO DA MULHER, DA FAMÍLIA E DOS DIREITOS HUMANOS e se compromete a não divulgar ou fornecer a terceiros quaisquer dados e informações que tenha recebido deste Ministério no curso da prestação dos serviços, a menos que autorizado formalmente e por escrito para tal.

6.6.3. Deverá ser celebrado TERMO DE CONFIDENCIALIDADE DE INFORMAÇÕES entre a Contratada e a Contratante para garantir a segurança das informações do MMFDH.

6.6.4. A Contratada, após a assinatura do contrato, por meio de seu representante, assinará **TERMO DE COMPROMISSO DE SIGILO E SEGURANÇA DA INFORMAÇÃO** (ANEXO D) em que se responsabilizará pela manutenção de sigilo e confidencialidade das informações a que possa ter acesso em decorrência da contratação.

6.7. **Requisito de arquitetura tecnológica**

6.7.1. A arquitetura tecnológica, especificações e peculiaridades da solução consta assentada no ANEXO "A" - ESPECIFICAÇÕES TÉCNICAS DA SOLUÇÃO.

6.8. **Requisitos de garantia e manutenção**

6.8.1. Durante o período de garantia, a CONTRATADA deverá estar apta a atender chamados encaminhados pela CONTRATANTE ao Centro de Atendimento da CONTRATADA, sem ônus adicional para o CONTRATANTE, oferecendo, no mínimo, os seguintes serviços:

6.8.2. Deve ser possível tanto acionamento via número 0800, quanto via Web, disponível 24 (vinte e quatro) horas por dia, 7 (sete) dias por semana, para solução de problemas decorrentes de defeitos e falhas nos produtos ou equipamento/software, ou seja, problemas decorrentes do fato do ativo de rede não realizar uma funcionalidade especificada ou esperada. Poderá ainda, esse serviço, ser usado para solicitar informações quanto às dúvidas, funcionalidades e quanto a procedimentos para configuração dos itens do objeto contratado.

6.8.3. Todos os custos decorrentes da retirada de equipamentos ou componentes para a prestação do serviço de garantia serão de responsabilidade da CONTRATADA, bem como seu retorno aos locais onde serão instalados os equipamentos pela empresa contratada.

6.8.4. No atendimento dos chamados, caso a CONTRATADA não consiga resolver o problema por meio da assistência remota, deverá a CONTRATADA realizar uma ação On-Site (no local onde está o equipamento) para sanar o problema e restabelecer o funcionamento normal do equipamento, obedecendo ao disposto no item 12.10.1 e atendendo aos prazos previstos na Tabela 1 - Níveis Mínimos de Serviço do item 12.10, responsabilizando-se pelas despesas de deslocamento de seu técnico/especialista.

6.8.5. Em qualquer caso, a CONTRATADA deverá arcar com todos os procedimentos necessários à solução do problema, incluindo a substituição de quaisquer módulos defeituosos no(s) equipamento(s), bem como a substituição do(s) próprio(s) equipamentos(s), se for necessário, devendo ser atendida as seguintes condições:

6.8.6. Os chamados serão registrados e informados à CONTRATANTE, nos prazos da Tabela 1, e deverão estar disponíveis, via sistema web, para acompanhamento pela equipe designada pela CONTRATANTE, contendo data e hora do chamado, o problema ocorrido, a solução, data e hora de conclusão.

6.8.7. Decorrido os prazos previstos na Tabela 1 – Instrumento de Medição de Resultados - IMR do item 12.10, sem o atendimento devido, fica a CONTRATANTE autorizada a penalizar a CONTRATADA dentro dos parâmetros explicitados neste TR, respeitado o direito ao contraditório e ampla defesa.

6.8.8. A CONTRATADA deverá encaminhar ao fiscal técnico do contrato o Relatório de Acompanhamento de Nível Mínimo de Serviço, com informações de TODOS os chamados abertos pela CONTRATANTE, em sua central de atendimento, contendo, pelo menos, as seguintes informações:

a) Data, hora da abertura do chamado;

b) Número de série do equipamento alvo do atendimento;

c) Data e hora da chegada do técnico ao local;

d) Data e hora da resolução do problema;

e) Descrição do problema, incidente ou solicitação atendida e Procedimentos efetuados.

f) Ateste(s) de atendimento e solução do(s) problema(s)

6.9. **Garantia dos equipamentos e serviços – disposições gerais**

6.9.1. A CONTRATADA deverá garantir a completa interoperabilidade e compatibilidade entre os Firewalls a serem adquiridos no presente Termo de Referência e os Ativos já em funcionamento na CONTRATANTE. Não podendo se escusar de suas responsabilidades quanto à prestação da solução técnica para possíveis falhas ou inconsistências, bem como o auxílio

técnico necessário à interoperação da rede, a fim de garantir o perfeito funcionamento dos ativos adquiridos e com os demais ativos com os quais deverão interoperar.

6.9.2. Sendo a CONTRATADA designada para realizar a instalação dos Firewalls, será de sua responsabilidade a correção das falhas decorrentes de erros durante as atividades de instalação, sejam operacionais ou por problemas de mau funcionamento, responsabilizando-se por todos os custos envolvidos na correção dos desvios, sejam de interoperabilidade, incompatibilidade ou quaisquer outras falhas que impeçam a instalação ou o perfeito funcionamento dos Firewalls adquiridos.

6.9.3. A CONTRATADA deverá garantir o pleno funcionamento dos Firewalls, prestando o serviço de garantia remoto e on-site (quando, a critério da CONTRATANTE, for necessário), por um período de 60 (sessenta) meses, contados a partir da data de emissão do Termo de Recebimento Definitivo.

6.9.4. A CONTRATADA deve garantir o funcionamento dos equipamentos, considerados isoladamente ou interligados aos demais, de acordo com as características descritas nos manuais e nas especificações aplicáveis, desde que o restante dos equipamentos de rede da CONTRATANTE esteja em condições normais de operação.

6.9.5. Para a referida garantia, serão considerados os eventos descritos conforme a Tabela 2 - Classificação de Eventos do item 12.10, devendo ser considerado para o enquadramento o grau de impacto para o serviço ou cliente afetado.

6.9.6. A CONTRATADA, no caso da atualização de equipamento para corrigir falhas apresentadas, deve se responsabilizar pelos custos envolvidos, inclusive eventuais trocas de hardware, cabendo à CONTRATANTE a emissão de documento fiscal ou equivalente necessário ao transporte do equipamento, quando for o caso.

6.10. **Garantia de Hardware**

6.10.1. A troca de qualquer unidade defeituosa deverá ser realizada em conformidade com os prazos estabelecidos na Tabela 1 – Instrumento de Medição de Resultados - IMR do item 12.10.

6.10.2. A CONTRATADA deve garantir que os equipamentos fornecidos são apropriados para suportar as condições climáticas, conforme características exigidas nas especificações técnicas constantes no ANEXO A.

6.11. **Garantia de Software**

6.11.1. A CONTRATADA deve disponibilizar, sem quaisquer custos adicionais à CONTRATANTE, a atualização de nova(s) versão(ões) do(s) software(s) e firmware(s) fornecido(s), ou de parte(s) dele(s), decorrentes da evolução funcional ou correções do(s) anteriormente fornecido(s), durante o prazo da garantia do equipamento da solução integrada, ou seja, 60 meses a partir do Termo de Recebimento Definitivo estabelecido no ANEXO C - Modelo de Termo de Recebimento Definitivo.

6.11.2. Cabe à CONTRATADA informar, por intermédio de carta ou mensagem eletrônica, a disponibilidade de novas versões e atualizações, assim como quanto aos respectivos procedimentos de instalação. Por nova versão, entende-se por aquele que, mesmo sendo comercializado com novo nome, número de versão ou marca, retenha as funcionalidades exigidas na presente especificação técnica.

6.11.3. A CONTRATANTE reserva-se o direito de aceitar ou não atualizações no software ou parte dele.

6.11.4. A CONTRATADA deve garantir que uma nova versão do software ou firmware mantenha a compatibilidade e contenha todas as funções das versões anteriores e que a introdução desta não prejudique a interoperabilidade da mesma na rede.

6.11.5. A CONTRATADA deve garantir a independência entre a correção de defeitos (patches) e a geração de novas versões do software, sem ônus adicional à CONTRATANTE, em função da necessidade de atualização de componente para suportar nova versão do software.

6.11.6. A CONTRATADA deverá garantir o correto funcionamento de todo software instalado no equipamento durante um período de garantia de 60 (sessenta) meses, a contar da data do Termo de Recebimento Definitivo

6.11.7. Durante todo o período da garantia do equipamento, a CONTRATADA obriga-se a substituir, recuperar e/ou modificar os softwares e firmwares instalados, sem ônus de qualquer natureza à CONTRATANTE, nos casos comprovados de mau funcionamento e de outras falhas, de modo a ajustá-los aos resultados que atendam às especificações técnicas solicitadas para o equipamento, conforme ANEXO A.

7. **OBRIGAÇÕES DA CONTRATANTE**

7.1. Exigir o cumprimento de todas as obrigações assumidas pela Contratada, de acordo com as cláusulas contratuais e os termos de sua proposta;

7.2. Exercer o acompanhamento e a fiscalização dos serviços, por servidor especialmente designado, anotando em registro próprio as falhas detectadas, indicando dia, mês e ano, bem como o nome dos empregados eventualmente envolvidos, e encaminhando os apontamentos à autoridade competente para as providências cabíveis;

7.3. Notificar a Contratada por escrito da ocorrência de eventuais imperfeições, falhas ou irregularidades constatadas no curso da execução dos serviços, fixando prazo para a sua correção, certificando-se que as soluções por ela propostas sejam as mais adequadas;

7.4. Pagar à Contratada o valor resultante da prestação do serviço, no prazo e condições estabelecidas neste Termo de Referência;

7.5. Efetuar as retenções tributárias devidas sobre o valor da Nota Fiscal/Fatura da contratada, no que couber, em conformidade com o item 6 do Anexo XI da IN SEGES/MP n. 5/2017.

7.6. Não praticar atos de ingerência na administração da Contratada, tais como:

7.7. exercer o poder de mando sobre os empregados da Contratada, devendo reportar-se somente aos prepostos ou responsáveis por ela indicados, exceto quando o objeto da contratação previr o atendimento direto, tais como nos serviços de recepção e apoio ao usuário;

7.8. direcionar a contratação de pessoas para trabalhar nas empresas Contratadas;

7.9. considerar os trabalhadores da Contratada como colaboradores eventuais do próprio órgão ou entidade responsável pela contratação, especialmente para efeito de concessão de diárias e passagens.

7.10. Fornecer por escrito as informações necessárias para o desenvolvimento dos serviços objeto do contrato;

7.11. Realizar avaliações periódicas da qualidade dos serviços, após seu recebimento;

7.12. Cientificar o órgão de representação judicial da Advocacia-Geral da União para adoção das medidas cabíveis quando do descumprimento das obrigações pela Contratada;

7.13. Arquivar, entre outros documentos, projetos, "as built", especificações técnicas, orçamentos, termos de recebimento, contratos e aditamentos, relatórios de inspeções técnicas após o recebimento do serviço e notificações expedidas;

7.14. Fiscalizar o cumprimento dos requisitos legais, quando a contratada houver se beneficiado da preferência estabelecida pelo art. 3º, § 5º, da Lei nº 8.666, de 1993.

8. **OBRIGAÇÕES DA CONTRATADA**

8.1. Executar os serviços conforme especificações deste Termo de Referência e de sua proposta, com a alocação dos empregados necessários ao perfeito cumprimento das cláusulas contratuais, além de fornecer e utilizar os materiais e equipamentos, ferramentas e utensílios necessários, na qualidade e quantidade mínimas especificadas neste Termo de Referência e em sua proposta;

8.2. Reparar, corrigir, remover ou substituir, às suas expensas, no total ou em parte, no prazo fixado pelo fiscal do contrato, os serviços efetuados em que se verificarem vícios, defeitos ou incorreções resultantes da execução ou dos materiais empregados;

8.3. Responsabilizar-se pelos vícios e danos decorrentes da execução do objeto, bem como por todo e qualquer dano causado à União ou à entidade federal, devendo ressarcir imediatamente a Administração em sua integralidade, ficando a Contratante autorizada a descontar da garantia, caso exigida no edital, ou dos pagamentos devidos à Contratada, o valor correspondente aos danos sofridos;

8.4. Utilizar empregados habilitados e com conhecimentos básicos dos serviços a serem executados, em conformidade com as normas e determinações em vigor;

8.5. Vedar a utilização, na execução dos serviços, de empregado que seja familiar de agente público ocupante de cargo em comissão ou função de confiança no órgão Contratante, nos termos do artigo 7° do Decreto n° 7.203, de 2010;

8.6. Quando não for possível a verificação da regularidade no Sistema de Cadastro de Fornecedores – SICAF, a empresa contratada deverá entregar ao setor responsável pela fiscalização do contrato, até o dia trinta do mês seguinte ao da prestação dos serviços, os seguintes documentos: 1) prova de regularidade relativa à Seguridade Social; 2) certidão conjunta relativa aos tributos federais e à Dívida Ativa da União; 3) certidões que comprovem a regularidade perante a Fazenda Municipal ou Distrital do domicílio ou sede do contratado; 4) Certidão de Regularidade do FGTS – CRF; e 5) Certidão Negativa de Débitos Trabalhistas – CNDT, conforme alínea "c" do item 10.2 do Anexo VIII-B da IN SEGES/MP n. 5/2017;

8.7. Responsabilizar-se pelo cumprimento das obrigações previstas em Acordo, Convenção, Dissídio Coletivo de Trabalho ou equivalentes das categorias abrangidas pelo contrato, por todas as obrigações trabalhistas, sociais, previdenciárias, tributárias e as demais previstas em legislação específica, cuja inadimplência não transfere a responsabilidade à Contratante;

8.8. Comunicar ao Fiscal do contrato, no prazo de 24 (vinte e quatro) horas, qualquer ocorrência anormal ou acidente que se verifique no local dos serviços.

8.9. Prestar todo esclarecimento ou informação solicitada pela Contratante ou por seus prepostos, garantindo-lhes o acesso, a qualquer tempo, ao local dos trabalhos, bem como aos documentos relativos à execução do empreendimento.

8.10. Paralisar, por determinação da Contratante, qualquer atividade que não esteja sendo executada de acordo com a boa técnica ou que ponha em risco a segurança de pessoas ou bens de terceiros.

8.11. Promover a guarda, manutenção e vigilância de materiais, ferramentas, e tudo o que for necessário à execução dos serviços, durante a vigência do contrato.

8.12. Promover a organização técnica e administrativa dos serviços, de modo a conduzi-los eficaz e eficientemente, de acordo com os documentos e especificações que integram este Termo de Referência, no prazo determinado.

8.13. Conduzir os trabalhos com estrita observância às normas da legislação pertinente, cumprindo as determinações dos Poderes Públicos, mantendo sempre limpo o local dos serviços e nas melhores condições de segurança, higiene e disciplina.

8.14. Submeter previamente, por escrito, à Contratante, para análise e aprovação, quaisquer mudanças nos métodos executivos que fujam às especificações do memorial descritivo.

8.15. Não permitir a utilização de qualquer trabalho do menor de dezesseis anos, exceto na condição de aprendiz para os maiores de quatorze anos; nem permitir a utilização do trabalho do menor de dezoito anos em trabalho noturno, perigoso ou insalubre;

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

8.17. Cumprir, durante todo o período de execução do contrato, a reserva de cargos prevista em lei para pessoa com deficiência ou para reabilitado da Previdência Social, bem como as regras de acessibilidade previstas na legislação, quando a contratada houver se beneficiado da preferência estabelecida pela Lei nº 13.146, de 2015.

8.18. Guardar sigilo sobre todas as informações obtidas em decorrência do cumprimento do contrato;

8.19. Arcar com o ônus decorrente de eventual equívoco no dimensionamento dos quantitativos de sua proposta, inclusive quanto aos custos variáveis decorrentes de fatores futuros e incertos, tais como os valores providos com o quantitativo de vale transporte, devendo complementá-los, caso o previsto inicialmente em sua proposta não seja satisfatório para o atendimento do objeto da licitação, exceto quando ocorrer algum dos eventos arrolados nos incisos do § 1º do art. 57 da Lei nº 8.666, de 1993.

8.20. Cumprir, além dos postulados legais vigentes de âmbito federal, estadual ou municipal, as normas de segurança da Contratante;

8.21. Prestar os serviços dentro dos parâmetros e rotinas estabelecidos, fornecendo todos os materiais, equipamentos e utensílios em quantidade, qualidade e tecnologia adequadas, com a observância às recomendações aceitas pela boa técnica, normas e legislação;

8.22. Assegurar à CONTRATANTE, em conformidade com o previsto no subitem 6.1, “a”e “b”, do Anexo VII – F da Instrução Normativa SEGES/MP nº 5, de 25/05/2017:

8.23. O direito de propriedade intelectual dos produtos desenvolvidos, inclusive sobre as eventuais adequações e atualizações que vierem a ser realizadas, logo após o recebimento de cada parcela, de forma permanente, permitindo à Contratante distribuir, alterar e utilizar os mesmos sem limitações;

8.24. Os direitos autorais da solução, do projeto, de suas especificações técnicas, da documentação produzida e congêneres, e de todos os demais produtos gerados na execução do contrato, inclusive aqueles produzidos por terceiros subcontratados, ficando proibida a sua utilização sem que exista autorização expressa da Contratante, sob pena de multa, sem prejuízo das sanções civis e penais cabíveis.

9. GARANTIA DE EXECUÇÃO

9.1. A Contratada, no prazo de dez dias úteis após a assinatura do Termo de Contrato prestará garantia no valor correspondente a 5% (cinco por cento) do valor do Contrato, que será liberada de acordo com as condições previstas no Edital, conforme disposto no Art. 56 da Lei nº 8.666, de 1993, desde que cumpridas as obrigações contratuais.

9.2. Caberá ao contratado optar por uma das seguintes modalidades de garantia:

9.2.1. caução em dinheiro ou em títulos da dívida pública, devendo estes ter sido emitidos sob a forma escritural, mediante registro em sistema centralizado de liquidação e de custódia autorizado pelo Banco Central do Brasil e avaliados pelos seus valores econômicos, conforme definido pelo Ministério da Economia;

9.2.2. seguro-garantia;

9.2.3. fiança bancária.

9.3. A garantia em dinheiro deverá ser efetuada em favor da Contratante, na Caixa Econômica Federal, com correção monetária, em favor do contratante.

9.4. No caso de alteração do valor do contrato, ou prorrogação de sua vigência, a garantia deverá ser readequada ou renovada nas mesmas condições.

9.5. A Contratante executará a garantia na forma prevista na legislação que rege a matéria.

9.6. A garantia prestada pelo contratado será liberada ou restituída após a execução do contrato e, quando em dinheiro, atualizada monetariamente. (artigo 56, §4º da Lei nº 8666/93).

10. **MODELO DE EXECUÇÃO DO CONTRATO**

10.1. **Reunião de alinhamento**

10.2. Deverá ser realizada reunião de alinhamento com o objetivo de identificar as expectativas, nivelar os entendimentos acerca das condições estabelecidas no Contrato, Edital e Anexos, e esclarecer possíveis dúvidas acerca da execução dos serviços.

10.3. Deverão participar dessa reunião, no mínimo o Gestor do Contrato no MMFDH e o Preposto da Contratada.

10.4. A reunião realizar-se-á no MMFDH em até 15 (quinze) dias úteis a contar da data de assinatura do Contrato, conforme agendamento efetuado pelo Gestor do Contrato no MMFDH.

10.5. Nessa reunião a Contratada deverá apresentar oficialmente seu Preposto, por meio de Ofício de designação.

10.6. Todos os entendimentos da reunião de alinhamento deverão constar da Ata de reunião a ser lavrada pelo Gestor do Contrato no MMFDH e assinada por todos os participantes.

10.7. A Contratada cumprirá as instruções complementares do MMFDH quanto à execução e horário de realização do serviço, permanência e circulação de seu (s) técnico (s) nas dependências do MMFDH.

10.8. **Interação entre Contratante e Contratada**

10.9. São mecanismos formais de comunicação entre a Contratada e a Contratante:

a) E-mails: forma rápida de comunicação para tratar de informações pouco críticas;

b) Ofícios: Comunicação para tratar de assuntos gerais;

c) Ordem de Serviço: elaborada, por demanda, pela Contratante e encaminhada à Contratada, com a função de demandar serviços contratados;

d) Termo de Recebimento Provisório: termo elaborado pela Contratante e encaminhado à Contratada;

e) Termo de Recebimento Definitivo: termo elaborado pela Contratante e encaminhado à Contratada.

f) Toda a comunicação entre a Administração Pública e a Contratada deverá ser sempre formal como regra, exceto em casos excepcionais que justifiquem outro canal de comunicação.

10.10. **Vínculo Empregatício**

10.10.1. A prestação dos serviços não gera vínculo empregatício entre os empregados da Contratada e a Administração Contratante, vedando-se qualquer relação entre estes que caracterize pessoalidade e subordinação direta, e não há dedicação de mão de obra exclusiva.

10.10.2. Os profissionais e representantes da Contratada não terão nenhum vínculo empregatício com o MMFDH, correndo por conta exclusiva da Contratada, todas as obrigações decorrentes da legislação trabalhista, previdenciária, infortunística do trabalho, fiscal, comercial e outras correlatas, as quais a Contratada se obriga a saldar na época devida.

10.11. **Modelo de Prestação de Serviço**

10.12. Após a assinatura do Contrato, de acordo com a necessidade, a Contratante emitirá a(s) Ordem(ns) de Serviço – OS.

10.13. A data de emissão da OS deverá sempre expressar a data atual de sua emissão e não as datas de empenho e/ou contrato.

10.14. Todas as Ordens de Serviço deverão ser atendidas pela Contratada no prazo máximo especificado no item Do Pagamento;

10.15. A OS indicará as quantidades, os prazos, os responsáveis pelo recebimento e os locais de entrega conforme a relação endereços das localidades.

10.16. Deve ser assinado por todos os empregados da Contratada e empresas indicadas pela Contratada que venham a participar da prestação dos serviços o termo de sigilo e confidencialidade, conforme o TERMO DE CONFIDENCIALIDADE DA INFORMAÇÃO.

10.17. Só poderá ser emitido Ordem de Serviço para itens previamente contratados;

10.18. Não há óbice no fatiamento da quantidade de um mesmo item constante do contrato em várias Ordens de Serviços, desde que o somatório das quantidades de cada item em cada Ordem de Serviço não ultrapasse a quantidade total de cada item previamente contratado.

10.19. **Fornecimento dos Softwares**

10.19.1. Conforme estabelecido no ANEXO A - ESPECIFICAÇÕES TÉCNICAS DA SOLUÇÃO deste Termo de Referência.

10.20. **Serviço de Instalação e Configuração**

10.20.1. Conforme estabelecido no ANEXO A - ESPECIFICAÇÕES TÉCNICAS DA SOLUÇÃO deste Termo de Referência.

10.21. **Direitos de Propriedade Intelectual e Direitos Autorais da Solução de Tecnologia da Informação**

10.21.1. Em conformidade com a IN n° 01/2019 SGD/ME, artigo 17, letra h, define-se a seguir quais serão os direitos a propriedade intelectual que caberá à administração, fruto do fornecimento pertinente a esta contratação, a saber:

10.21.2. Não se aplicará direito de propriedade intelectual à administração sobre o código fonte, visto que a execução dos serviços não envolve desenvolvimento de software e/ou aplicativo.

10.21.3. Destaca-se que a administração pretende adquirir hardware e software prontos, onde não se aplicar-se-á o direito de propriedade intelectual.

10.21.4. Não se aplicará direito de propriedade intelectual à administração sobre a documentação original que acompanha a plataforma de hardware e software, visto que a execução do fornecimento não envolve desenvolvimento de software e/ou aplicativo e/ou manuais.

10.21.5. Se aplicará direito de propriedade intelectual à administração sobre toda e qualquer documentação fruto da execução dos serviços prestados, exceto para a citada anteriormente.

11. **MODELO DE GESTÃO DO CONTRATO**

11.1. **Rotinas de Execução**

11.2. A Contratada, na execução dos serviços, deverá adotar a Metodologia de Gerenciamento de Projetos, a Metodologia de Desenvolvimento de Software e a Metodologia de Administração de Dados, além de seguir os padrões de arquitetura de software definidos.

11.3. **Ordem de Serviço / Fornecimento de Bens**

11.4. A execução dos serviços será condicionada à abertura e autorização prévia de ordem de serviço (OS) emitida pelo sistema próprio de gestão de demandas da Contratante, que também controlará prazos, quantidades e produtos/serviços a serem entregues.

11.5. As OS registrarão as etapas, os prazos, o detalhamento dos serviços, as atividades previstas, os padrões a serem seguidos, os produtos a serem entregues, o custo estimado, bem como demais informações técnicas necessárias para a execução dos serviços por parte da Contratada.

11.6. Após aprovação das demandas, o Gestor do Contrato encaminhará a OS para a Contratada, bem como as informações necessárias para sua execução.

11.7. Cada demanda deverá ser executada atendendo as especificações, de acordo com a arquitetura, aspectos metodológicos, estrutura, padrões e melhores práticas, além das que constarem da OS.

11.8. Será gerada OS complementar sempre que houver alguma alteração na OS original. Portanto, não serão aceitas justificativas para não cumprimento de prazos devido a alterações no escopo da OS.

11.9. Uma OS poderá ser suspensa por decisão do usuário gestor, do gestor do contrato ou de um dos fiscais técnicos do contrato. Nesse momento, os prazos serão suspensos e redefinidos, caso a OS seja retomada.

11.10. No cancelamento de uma OS, deverá ser apurado o serviço já realizado e discutido com o gestor do contrato a forma de faturamento, se necessário.

11.11. O modelo de ordem de serviço está descrito no ANEXO F deste Termo de Referência.

11.12. **Critérios de Aceitação**

11.13. Todo e qualquer fornecimento se dará mediante demanda da Contratante, situação em que será emitida a Ordem de Serviços - OS.

11.14. Os serviços serão executados nos locais e endereços descritos nas Ordens de Serviço.

11.15. Os serviços que compõem a solução serão recebidos:

11.15.1. **Provisoriamente**, no ato da entrega dos comprovantes de emissão da licença e dos pacotes de extensão será lavrado um termo de recebimento provisório da Ordem de Fornecimento, em até 5 (cinco) dias úteis.

11.15.2. **Definitivamente**, o recebimento definitivo será emitido após a instalação, configuração e verificação do correto funcionamento do software, bem como da interação com os módulos já instalados da solução, em até 30 (trinta) dias.

11.16. A Administração rejeitará, no todo ou em parte, a entrega dos serviços em desacordo com as especificações técnicas exigidas.

11.17. A recusa parcial ou total no atendimento de uma OS emitida, será oficiada à Contratada pela Contratante, que deverá prontamente prestar o serviço de acordo com o estabelecido na respectiva Ordem de Serviço;

11.18. A aceitação definitiva dar-se-á após a assinatura do termo de recebimento definitivo, correspondente a cada Ordem de serviço.

11.19. **Da transição contratual**

11.19.1. Em casos de interrupção contratual e ocorrendo mudança de fornecedor da solução, todo conhecimento adquirido ou desenvolvido, bem como toda informação produzida e/ou utilizada para a execução dos projetos e serviços contratados deverão ser disponibilizados à contratante ou empresa por ela designada em até 30 (trinta) dias corridos após o encerramento do contrato.

11.19.2. A empresa contratada deverá elaborar o Plano de Transição, no prazo de 60 (sessenta) dias corridos antes do encerramento do contrato, para a transferência integral e irrestrita dos conhecimentos e das competências necessárias e suficientes para promover a continuidade dos serviços. A contratante poderá estabelecer prazo inferior caso haja rescisão contratual.

11.19.3. Nenhum pagamento será devido à empresa contratada pela elaboração ou pela execução do Plano de Transição. O fato da empresa contratada ou seus representantes não cooperarem ou reterem qualquer informação ou dado solicitado pela contratante, que venha a prejudicar, de alguma forma, o andamento da transição das tarefas e serviços para um novo prestador, constituirá quebra de contrato, sujeitando-a as obrigações em relação a todos os danos causados à contratante.

11.20. **Procedimentos de Teste e Inspeção**

11.20.1. Os serviços serão recebidos após a verificação do atendimento dos Níveis Mínimos de Serviços Exigidos.

11.20.2. Todas as atividades devem ser relacionadas e fornecidas à fiscalização do MMFDH.

12. **ACOMPANHAMENTO E FISCALIZAÇÃO DO CONTRATO**

12.1. O acompanhamento e a fiscalização da execução do contrato consistem na verificação da conformidade da prestação dos serviços e da alocação dos recursos necessários, de forma a assegurar o perfeito cumprimento do ajuste, devendo ser exercidos por um ou mais representantes da Contratante, especialmente designados, na forma dos arts. 67 e 73 da Lei nº 8.666, de 1993, e do Decreto n° 9.507/2018.

12.2. O representante da Contratante deverá ter a experiência necessária para o acompanhamento e controle da execução dos serviços e do contrato.

12.3. A verificação da adequação da prestação do serviço deverá ser realizada com base nos critérios previstos neste Termo de Referência.

12.4. A execução dos contratos deverá ser acompanhada e fiscalizada por meio de instrumentos de controle, que compreendam a mensuração dos aspectos mencionados no IN SEGES/MP nº 5, de 26 de maio de 2017, quando for o caso.

12.5. O fiscal ou gestor do contrato, ao verificar que houve subdimensionamento da produtividade pactuada, sem perda da qualidade na execução do serviço, deverá comunicar à autoridade responsável para que esta promova a adequação contratual à produtividade efetivamente realizada, respeitando-se os limites de alteração dos valores contratuais previstos no § 1º do artigo 65 da Lei nº 8.666, de 1993.

12.6. A conformidade do material a ser utilizado na execução dos serviços deverá ser verificada juntamente com o documento da Contratada que contenha a relação detalhada dos mesmos, de acordo com o estabelecido neste Termo de Referência e na proposta, informando as respectivas quantidades e especificações técnicas, tais como: marca, qualidade e forma de uso.

12.7. O representante da Contratante deverá promover o registro das ocorrências verificadas, adotando as providências necessárias ao fiel cumprimento das cláusulas contratuais, conforme o disposto nos §§ 1º e 2º do art. 67 da Lei nº 8.666, de 1993.

12.8. O descumprimento total ou parcial das demais obrigações e responsabilidades assumidas pela Contratada ensejará a aplicação de sanções administrativas, previstas neste Termo de Referência e na legislação vigente, podendo culminar em rescisão contratual, conforme disposto nos artigos 77 e 80 da Lei nº 8.666, de 1993.

12.9. A fiscalização da execução dos serviços abrange, ainda, as seguintes rotinas:

a) Observar o fiel adimplemento das disposições contratuais;

b) Solicitar a imediata substituição de funcionário da Contratada que embaraçar ou dificultar o seu atendimento e a sua fiscalização, a seu exclusivo critério;

c) Rejeitar, no todo ou em parte, os produtos fornecidos em desacordo com as especificações deste Termo de Referência;

d) Suspender a execução do fornecimento ou dos serviços contratados, sem prejuízo das penalidades a que se sujeita a Contratada, garantido o contraditório e a ampla defesa.

e) A fiscalização de que trata esta cláusula não exclui nem reduz a responsabilidade da Contratada, inclusive perante terceiros, por qualquer irregularidade, ainda que resultante de imperfeições técnicas, vícios redibitórios, ou emprego de material inadequado ou de qualidade inferior e, na ocorrência desta, não implica em corresponsabilidade da Contratante ou de seus agentes e prepostos, de conformidade com o art. 70 da Lei nº 8.666, de 1993.

12.10. **Instrumento de Medição de Resultado - IMR Exigidos**

Severidade	**Medidas para o indicador (Prazo de Resolução)**
A	4 horas
B	6 horas
C	24 horas

Tabela 1 - IMR Mínimos de Serviço

12.10.1. A abertura do chamado com fornecimento do seu número de identificação (protocolo de atendimento) deve ocorrer no prazo máximo de 15 minutos a partir da tentativa de contato pela CONTRATANTE com o número fornecido pela CONTRATADA.

12.10.2. O atendimento aos chamados pode ocorrer remotamente ou de forma presencial. Atendimentos remotos não resolvidos que ultrapassem 12 horas devem ser continuados de forma presencial ao final deste prazo e condicionado à Tabela 3.

(A) Emergencial	São consideradas como “Emergência” todas as falhas cujas consequências tenham impactos negativos, gerando indisponibilidade sobre o serviço e o tráfego e/ou recursos. São situações que exijam atenção imediata. Exemplo: Situação de indisponibilidade total do equipamento, funcionamento intermitente ou parcial do equipamento, que possa levar à interrupção intermitente, parcial ou total de serviços ou perda de tráfego.
(B) Grave	Problemas que não prejudicam significativamente o funcionamento dos sistemas/serviços do equipamento. São problemas sérios ou perturbações, que afetam uma área específica ou determinada funcionalidade do equipamento. Exemplo: Perda de redundância, reinicialização de módulos, slots ou portas com defeitos, degradação de desempenho, perda de funcionalidades.
(C) Pedido de Informação	Solicitação de informações sobre o funcionamento dos equipamentos, possíveis configurações ou usos, que não gerem interrupções, nem indisponibilidade de determinada área ou uma funcionalidade específica.

Tabela 2 - Classificação de Eventos

12.10.3. Um chamado classificado de acordo com essas severidades não pode ser reclassificado à medida que é resolvido em outra. A severidade deve levar em conta o fator que foi usado na sua abertura e seguir esse mesmo critério até a sua completa solução.

13. **DESCUMPRIMENTO DO INSTRUMENTO DE MEDIÇÃO DE RESULTADO COM PROCEDIMENTO DE PENALIDADES**

13.0.1. O descumprimento total ou parcial das obrigações assumidas pela CONTRATADA, referente ao não atendimento do Instrumento de Medição de Resultado da Tabela 1, do item 12.10, resguardados os procedimentos legais pertinentes, sem prejuízo nas demais sanções cabíveis, acarretará às seguintes penalidades de acordo com a Tabela 3 – Descumprimento do IMR e Penalidades:

Descrição	**Penalidade**
Até 4 horas corridas de atraso, além do prazo	1) Advertência;

indicado na Tabela 1 - Instrumento de Medição de Resultado.	2) Havendo recorrência, multa de 0,1% (zero vírgula um por cento) por hora de atraso, calculada sobre o valor da solução.
Superior a 4 horas e inferior ou igual a 8 horas corridas de atraso, além do prazo definido no Instrumento de Medição de Resultado..	3) Multa de 0,2% (zero vírgula dois por cento) por hora de atraso, calculada sobre o valor da solução, sem prejuízo ao item anterior.
Superior a 8 horas corridas, além do prazo indicado na Tabela 1 – Instrumento de Medição de Resultado..	4) Multa de 0,4% (zero vírgula quatro por cento) por hora de atraso, calculada sobre o valor da solução, sem prejuízo ao item anterior, e outras sanções administrativas a critério da CONTRATANTE.

Tabela 3 – Descumprimento do IMR e Penalidades.

13.0.2. Deverão ser consideradas ainda as especificações contidas no ANEXO A - ESPECIFICAÇÕES TÉCNICAS DA SOLUÇÃO

14. **DO PAGAMENTO**

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

14.2. 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 5 (cinco) dias úteis, contados da data da apresentação da Nota Fiscal/Fatura, nos termos do art. 5º, § 3º, da Lei nº 8.666, de 1993.

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

14.4. 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.

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

14.5. Havendo erro na apresentação da Nota Fiscal/Fatura 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.

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

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

14.8. Constatando-se, junto ao SICAF, a situação de irregularidade da contratada, será providenciada sua notificação, por escrito, para que, no prazo de 5 (cinco) dias, regularize sua situação ou, no mesmo prazo, apresente sua defesa. O prazo poderá ser prorrogado uma vez, por igual período, a critério da contratante.

14.9. 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, observando o disposto no art. 29, da Instrução Normativa nº 3 de 26 de abril de 2018

14.10. 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.

14.11. 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.

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

14.13. Constatando-se, junto ao SICAF, a situação de irregularidade da contratada, será providenciada sua notificação, por escrito, para que, no prazo de 5 (cinco) dias, regularize sua situação ou, no mesmo prazo, apresente sua defesa. O prazo poderá ser prorrogado uma vez, por igual período, a critério da contratante.

14.14. 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.

14.15. 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.

14.16. 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.

14.16.1. 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.

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

14.17.1. 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.

14.18. 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:

14.18.1. EM = I x N x VP, sendo:

14.18.2. EM = Encargos moratórios;

14.18.3. N = Número de dias entre a data prevista para o pagamento e a do efetivo pagamento;

14.18.4. VP = Valor da parcela a ser paga.

14.18.5. I = Índice de compensação financeira = 0,00016438, assim apurado:

I = (TX)	I =	(6 / 100) 365	I = 0,00016438 TX = Percentual da taxa anual = 6%

15. **DA SUBCONTRATAÇÃO**

15.1. Não será admitida a subcontratação do objeto licitatório.

16. **ALTERAÇÃO SUBJETIVA**

16.1. 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.

17. **REAJUSTE**

17.1. Os preços são fixos e irreajustáveis durante a vigência do contrato.

18. **DAS SANÇÕES ADMINISTRATIVAS.**

18.1. Comete infração administrativa, nos termos da Lei nº 10.520, de 2002, a Contratada que:

18.1.1. Inexecução total ou parcialmente qualquer das obrigações assumidas em decorrência da contratação;

18.1.2. Ensejar o retardamento da execução do objeto;

18.1.3. Falhar ou fraudar na execução do objeto;

18.1.4. Comportar-se de modo inidôneo;

18.1.5. Cometer fraude fiscal;

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

18.2.1. advertência por faltas leves, assim entendidas como aquelas que não acarretarem prejuízos significativos para a Contratante;

18.2.2. multa moratória de 0,33% (zero vírgula trinta e três por cento) por dia de atraso, calculada sobre o valor da prestação ou fornecimento em atraso, cabível nos casos de atraso injustificado de até 30 (trinta) dias no cumprimento dos prazos previstos neste instrumento para os compromissos assumidos;

18.2.3. multa compensatória de 10% (cinco por cento) sobre o valor total do contrato, no caso de inexecução total do objeto;

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

18.2.5. 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;

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

18.2.6.1. A Sanção de impedimento de licitar e contratar prevista neste subitem também é aplicável em quaisquer das hipóteses previstas como infração administrativa no subitem 18.1 deste Termo de Referência.

18.2.7. 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;

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

18.4. Também ficam sujeitas às penalidades do art. 87, III e IV da Lei n] 8.666, de 1993, as empresas ou profissionais que:

18.4.1. tenham sofrido condenação definitiva por pratica, por meio dolosos, fraude fiscal no recolhimento de qualquer tributos;

18.4.2. tenham praticado atos ilícitos visando a frustar os objetivos da licitação;

18.4.3. demonstrem não possuir idoneidade para contratar com a Administração em virtude de aos ilícitos praticados.

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

18.6. 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 da Divida Ativa da União e cobrados judicialmente.

18.6.1. Caso a Contratante determine, a multa deverá ser recolhida no prazo máximo de 05 (cinco), a contar da data do recebimento da comunicação enviada pela autoridade competente.

18.7. 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.

18.8. 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.

18.9. Se, durante o processo de aplicação de penalidade, 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.

18.10. 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.

18.11. 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.

18.12. As penalidades serão obrigatoriamente registradas no SICAF.

19. **ESTIMATIVA DE PREÇOS**

19.1. O valor estimado da referida aquisição é de R$ **1.988.922,54** (um milhão, novecentos e oitenta e oito mil, novecentos e vinte e dois reais e cinquenta e quatro centavos), conforme demonstrado na tabela abaixo:

Item	Descrição	Qtde	Valor Unitário Máximo Aceitável	Valor Total Máximo Aceitável
1	Solução de Next Generation Firewall (hardware), incluindo IPS, prevenção contra ameaças de vírus, spywares, malwares "Zero Day", Filtro de URL com suporte técnico, licenciamento e garantia por 60 meses.	2	R$ 994.461,27	R$ **1.988.922,54**

19.2. Os valores estimados relativos a cada um dos itens constantes da tabela supra, configuram o valor máximo a ser aceito pelo Ministério para contratação.

20. **DOS RECURSOS ORÇAMENTÁRIOS**

20.1. As despesas decorrentes deste projeto correrão à conta dos recursos consignados no Orçamento Geral da União para o exercício de 2020, a cargo do MINISTÉRIO DA MULHER, DA FAMÍLIA E DOS DIREITOS HUMANOS , Ação 2000, PO 000F, elemento da despesa 44.90.52.37.

20.2. **Estimativa de impacto econômico financeiro**

20.2.1. Para o item de Aquisição de Solução Integrada de Segurança - Firewall com garantia e implementação (1) o pagamento será efetuada em cota única após em até 30 dias após a emissão do Termo de Recebimento Definitivo.

20.2.2. A tabela abaixo sintetiza as etapas de execução da contratação. O prazo em todas as etapas tem como referência inicial o fim da etapa anterior:

Etapa	Descrição	Prazo
1	Assinatura do contrato	-
1.1	Entrega dos objetos	Até 45 dias corridos após assinatura do contrato
1.2	Emissão do termo de aceite provisório	No ato da entrega do objeto, incluindo a validação presencial (se necessária) juntamente com o documento fiscal emitido pela CONTRATADA.
1.3	Emissão do termo de aceite definitivo	Até 10 (dez) dias úteis após o Recebimento Provisório
1.4	Pagamento dos Objetos	Até 10 (dez) dias úteis após emissão de Recebimento Definitivo

21. **VIGÊNCIA DO CONTRATO**

21.1. A vigência do contrato será de 12 meses prorrogáveis até 60 (sessenta) meses, contados a partir da data de sua assinatura.

21.1.1. A vigência contratual perpassará mais de um exercício financeiro, haja vista a necessidade de embasar contratualmente a vigência do licenciamento e do serviço de suporte técnico, que serão de 60 (sessenta) meses.

21.1.2. Portanto, já que o prazo não trará obrigação financeira futura para a Administração, mas sim gerará vantajem econômica na contratação, e considerando que a cotação de preço por prazo estendido proporciona a diminuição do valor de fornecimento, convencionou-se por definir a vigência em 60 (sessenta) meses.

22. **CRITÉRIOS DE SELEÇÃO DO FORNECEDOR**

22.1. **Tipo da Licitação**

22.1.1. A Licitação será executada na modalidade Pregão Eletrônico do tipo Menor Preço por Item.

22.1.1.1. O objeto da pretendida contratação, bem como a composição do item do escopo de fornecimento, que formam o conjunto de bens e serviços a serem contratados, configuram uma única solução de Tecnologia da Informação.

22.1.1.2. Assim posto, o presente TR está em conformidade com o artigo 3º, inciso I, da IN 01/2019 e alterações, que preceitua que: "Não poderão ser objeto de contratação mais de uma Solução de Tecnologia da Informação em um único contrato".

22.1.1.3. O Item levou em consideração questões técnicas, sem prejuízo a ampla competitividade, uma vez que existem no mercado várias empresas com capacidade de fornecer os produtos na forma em que estão agrupados neste TR.

> A Lei nº 10.520/2002 traz em seu art. 1º, parágrafo único, o conceito de bens e serviços comuns como sendo "aqueles cujos padrões de desempenho e qualidade possam ser objetivamente definidos pelo edital, por meio de especificações usuais no mercado". Da mesma forma, o Decreto nº 7.174/2010 complementa tal conceito em seu art. 9º, acrescentando que, além do padrão objetivo de desempenho e qualidade, para ser considerado comum, é necessário que as especificações do bem ou serviço sejam atendidas por vários fornecedores, ainda que existam outras soluções disponíveis no mercado;

22.1.1.4. Assim posto, resta claro que o Item pretendido, mas sim, estritamente necessário a aquisição de elementos de forma agrupada, sejam eles de serviços ou produtos, não cabendo assim, o fatiamento do fornecimento de outra forma, que o

apresentado neste documento.

22.1.1.5. Portanto, não será aplicado o disposto no Art. 8º do Decreto nº 8.538 de 06 de outubro de 2015, considerando a inviabilidade técnica e econômica para o parcelamento do objeto da presente contratação, bem como consideradas as suas respectivas peculiaridades, interdependência e natureza acessória entre as parcelas do objeto.

22.2. **Justificativa para aplicação do direito de preferência**

22.2.1. Em razão de este TR tratar da aquisição de equipamentos de segurança de TI:

22.2.2. Lei no 8.666, de 21 de junho de 1993 e suas alterações.

22.2.2.1. Lei nº 10.520, de 17 de julho de 2002 que institui a modalidade Pregão.

22.2.2.2. Lei Complementar nº 123, de 14 de dezembro de 2006, que institui o Estatuto Nacional da Microempresa e da Empresa de Pequeno Porte.

22.2.2.3. Lei nº 7.596, de 10 de abril de 1987.

22.2.2.4. Decretos nº 10.183, de 20 de setembro de 2019; 10.024, de 20 de setembro de 2019 e 7.892, de 23 de janeiro de 2013.

22.2.2.5. Decreto nº 7.174/2010 - Regulamenta a contratação de bens e serviços de informática e automação pela administração pública federal, direta ou indireta, pelas fundações instituídas ou mantidas pelo Poder Público e pelas demais organizações sob o controle direto ou indireto da União.

22.2.2.6. IN/SLTI/MPOG nº 01/2019, que trata da contratação de serviços de Tecnologia da Informação (TI).

22.2.2.7. Nota Técnica nº 01/2008 - SEFTI/TCU - Estabelece o conteúdo mínimo do Termo de Referência ou Projeto Básico para contratação de serviços de Tecnologia da Informação e Comunicações – TIC.

22.2.2.8. Nota Técnica nº 02/2008 - SEFTI/TCU - Estabelece o uso do pregão para aquisição de bens e serviços de Tecnologia da Informação.

22.3. **Habilitação Técnica**

22.3.1. A habilitação técnica será feita por intermédio de atestados ou declarações de capacidade técnica.

22.3.2. O atestado de capacidade técnica deverá ser fornecido em nome do licitante, e ser expedido por pessoa jurídica de direito público ou privado, com a comprovação de que a empresa tenha fornecido objeto compatível em quantidade e especificidade com o objeto licitado.

22.3.3. Será exigido, para a comprovação de execução de objeto equivalente ao deste Termo de Referência, que a licitante vencedora apresente documento que ateste o fornecimento de 01 (um) equipamento similar para o respectivo item, caso a licitante obtenha menor preço em relação ao item.

22.3.4. O atestado deverá ser obrigatoriamente emitido por pessoa jurídica de direito público ou privado, devendo ainda ser emitido em papel timbrado e conter:

a) Razão Social, CNPJ e Endereço Completo da Empresa Emitente;

b) Razão Social da Contratada;

c) Número e vigência do contrato, se for o caso;

d) Objeto do contrato;

e) Declaração de que foram atendidas as expectavas do cliente quanto ao cumprimento de cronogramas pactuados;

f) Local e Data de Emissão;

g) Identificação do responsável pela emissão do atestado, Cargo, Contato (telefone e correio eletrônico);

h) Assinatura do responsável pela emissão do atestado;

i) Devem ser originais ou autenticados, se cópias, e legíveis.

22.3.5. No caso de apresentação de atestado de empresas privadas, não serão considerados aqueles apresentados por empresas participantes do mesmo grupo empresarial da contratada. Serão consideradas como de mesmo grupo, empresas controladas pela contratada, ou que tenham pelo menos uma pessoa física ou jurídica que seja sócia da empresa emitente e da contratada.

22.4. **Proposta de Preços**

22.4.1. A licitante deverá apresentar sua proposta, conforme modelo do Anexo E - Modelo de Proposta de Preços, com a indicação detalhada do produto ofertado citando a marca, modelo, tipo e fabricante;

22.4.2. Os preços deverão ser expressos em reais (R$) com duas casas decimais e conter todos os custos operacionais, encargos previdenciários, trabalhistas, tributários, comerciais e quaisquer outros que incidam direta ou indiretamente no fornecimento dos equipamentos e da prestação dos serviços relativos a esta contratação. Ou seja, a Proposta de Preços deverá ser preenchida com os preços cotados para cada item do lote com todos os custos inclusos.

22.4.3. Não serão aceitas descrições genéricas, onde não estiverem indicados os itens/subitens atendidos. Por exemplo: Se for usado um manual do equipamento, deverá ser indicada a página e parágrafo onde a informação de cada item/subitem está comprovada;

22.4.4. Não serão aceitas descrições que não sejam acompanhadas individualmente por item/subitem de documento comprobatório como os pedidos acima;

22.4.5. Todos os padrões, especificações, certificações ou definições utilizadas neste documento deverão ser considerados como o mínimo necessário, podendo ser atendidos por versões mais atuais, desde que contenham todos os recursos e requisitos das versões aqui citadas.

22.4.6. Não será aceita cópia de trecho(s) do presente Termo de Referência como descritivo ou em qualquer documentação comprobatória apresentada.

22.4.7. Não será aceita citação ao Edital ou Termo de Referência como descritivo ou em qualquer documentação comprobatória apresentada

22.4.8. A licitante deverá ainda informar em sua proposta o endereço no sítio oficial do fabricante, de modo que possam ser evidenciadas as especificações técnicas exigidas no edital e informadas na proposta de preços;

22.4.9. A licitante deverá Informar os meios de comunicação (e-mail, número de telefone 0800, serviço de abertura de chamado via web) para abertura de chamados;

22.4.10. Deverá informar o site do fabricante do equipamento na Internet, onde se possam efetuar consultas;

22.4.11. A proposta deverá ser apresentada com os valores unitários e totais, conforme planilha constante do modelo de proposta.

22.4.12. Deverão constar nos documentos acima citados as demais informações referentes às dimensões físicas, quantidade de U's para instalação em rack, necessidade de espaço de guarda, mecanismo de refrigeração, consumo de energia, dissipação térmica e peso que demonstrem o atendimento aos requisitos técnicos estabelecidos neste documento.

22.4.13. No caso de entender tais documentos como insuficientes para a análise, poderá o pregoeiro, suportado pelo grupo técnico de apoio, solicitar complementação, e/ou realizar diligência(s) para obter informações mais detalhadas sobre os produtos ofertados, conforme previsto no parágrafo § 3º do Art. 43 da Lei nº 8.666/93.

22.4.14. Ainda, juntamente com sua proposta, a Licitante deverá entregar, preenchido e assinado pelo responsável legal, o **Termo de Integridade,** conforme modelo Anexo G. Tendo em vista, que este termo siga a mesma regra do **Termo de Compromisso de Sigilo e Segurança da Informação** (ANEXO D), que seja assinado quando da assinatura do contrato, sob pena de desclassificação da licitante durante a sessão pública.

23. CONSÓRCIO

23.1. A possibilidade de participação ou não em licitações de empresas em consórcio fica ao juízo discricionário da Administração, conforme amplamente discutido na Jurisprudência, como, por exemplo, os Acórdãos n° 1.165/2012-Plenário, 1.946/2006-Plenário, 22/2003-Plenário, abaixo transcritos.

> Assim, como é de amplo conhecimento daqueles que lidam com licitações, a jurisprudência desta Corte aponta para o caráter discricionário no que concerne à decisão acerca da participação de consórcios nos diversos eventos licitatórios, a teor do art. 33 da Lei de Licitações. Acórdão 1165/2012-Plenário.
>
> Acórdão TCU nº 1.946/2006 – Plenário: a permissão da participação de consórcio é uma escolha discricionária do administrador, a ser analisada em cada caso concreto, dependendo do requisito de alta complexidade ou relevante vulto da obra, o qual não se acha presente na licitação do TST.
>
> Acórdão nº 22/2003 – Plenário: No mesmo sentido é a regra insculpida no art. 33 da Lei nº 8.666/93, que estipula as normas a serem seguidas pela Administração nas hipóteses em que for permitida a participação de consórcios na licitação. Trata-se de escolha discricionária da Administração, a ser verificada caso a caso. Muitas vezes, a formação de consórcio pode ensejar redução no caráter competitivo, pois facilitaria que empresas, que seriam naturalmente competidoras entre si, acordassem para participar da licitação.

23.2. No caso, portanto, deste certame, não será permitida a participação de consórcios nem a subcontratação, por não se tratar de objeto de grande vulto nem de execução de alta complexidade e por considerar-se que, dessa forma, será ampliado o caráter competitivo.

24. CRITÉRIOS DE SUSTENTABILIDADE AMBIENTAL

24.1. A Contratada deverá atender no que couber, os critérios de sustentabilidade ambiental. Destaca-se, as recomendações contidas no Capítulo III, DOS BENS E SERVIÇOS, com ênfase no art. 5º da Instrução Normativa nº 01/2010 STI/MPOG, bem como, o Decreto nº 7.746/2012 que estabelece critérios, práticas e diretrizes para a promoção do desenvolvimento nacional sustentável e a Lei nº 12.305/2010 que institui a política de resíduos sólidos, no que couber.

24.2. É dever da Contratada observar entre outras: o menor impacto sobre recursos naturais como flora, fauna, ar, solo e água; preferência para materiais, tecnologias e matérias-primas de origem local; maior eficiência na utilização de recursos naturais como água e energia; maior geração de empregos, preferencialmente com mão de obra local; maior vida útil e menor custo de manutenção do bem e da obra; uso de inovações que reduzam a pressão sobre recursos naturais; e origem ambientalmente regular dos recursos naturais utilizados nos bens, serviços e obras.

24.3. O ambiente físico da Contratada para fins de execução do serviço deve ser compatível com o disposto na NR17 do Ministério do Trabalho e Emprego – MTE e na recomendação técnica DSST nº 01/2005 do Ministério do Planejamento, Desenvolvimento e Gestão.

24.4. O objeto a ser contratado deve estar adequado a Política Nacional de Resíduos Sólidos (PNRS), Lei Nº 12.305/2010, foi aprovada em agosto de 2010, dispondo sobre seus princípios, objetivos e instrumentos, bem como sobre as diretrizes relativas à gestão integrada e ao gerenciamento de resíduos sólidos, incluindo os perigosos, às responsabilidades dos geradores e do poder público e aos instrumentos econômicos aplicáveis

25. **DISPOSIÇÕES GERAIS**

25.1. Fazem parte deste Termo de Referência os seguintes anexos:

25.1.1. ANEXO A - Especificações Técnicas da Solução.

25.1.2. ANEXO B - Modelo de Termo de Recebimento Provisório.

25.1.3. ANEXO C - Modelo de Termo de Recebimento Definitivo.

25.1.4. ANEXO D - Modelo de Termo de Compromisso de Sigilo e Segurança da Informação.

25.1.5. ANEXO E - Modelo de Proposta de Preços.

25.1.6. ANEXO F - Modelo de Ordem de Fornecimento.

25.1.7. ANEXO G - Modelo de Termo de Integridade.

26. **EQUIPE DE PLANEJAMENTO DA CONTRATAÇÃO E APROVAÇÃO**

26.1. A Equipe de Planejamento da Contratação foi designada pela PORTARIA Nº 6, DE 10 DE FEVEREIRO DE 2020 (1076342).

26.2. Conforme o §6º do art. 12 da IN SGD/ME nº 01, de 2019, o Termo de Referência segue assinado pela Equipe de Planejamento da Contratação, pela autoridade máxima da Área de TIC e aprovado pela autoridade competente.

INTEGRANTE TÉCNICO	INTEGRANTE REQUISITANTE	INTEGRANTE ADMINISTRATIVO
(Assinado eletronicamente) **Henrique Alcântara Veloso Mota** Mat. 1527028	*(Assinado eletronicamente)* **Helder Mota Gomes** Mat. 1584672	*(Assinado eletronicamente)* **Tatiana Fernandes da Silva** Mat. 1979086

AUTORIDADE MÁXIMA DA ÁREA DE TIC
(Assinado eletronicamente) **HELDER MOTA GOMES** Coordenador-Geral de Tecnologia da Informação

AUTORIDADE COMPETENTE

APROVO o presente Termo de Referência, mediante competência contida no inciso I do art. 1º da Portaria nº 132, de 8 de fevereiro de 2019, conforme dispõe o inciso II do art. 14 do Decreto Nº 10.024, de 20 de setembro de 2019.

(*Assinado Eletronicamente)*
LUCIANO BRAGAGNOLO
Subsecretário de Orçamento e Administração

ANEXOS DO TERMO DE REFERÊNCIA

ANEXO A - ESPECIFICAÇÕES TÉCNICAS DA SOLUÇÃO

Os requisitos especificados neste TR são definidos como condições mínimas necessárias ao atendimento da necessidade e devem ser igualados ou superados pela Contratada.

1. **Lote Único**

1.1. O objeto da presente licitação é a Contratação de empresa especializada no fornecimento de soluções de segurança de redes compostas de firewall corporativo e multifuncional para prover segurança e proteção da rede de computadores, contemplando gerência unificada com garantia de funcionamento pelo período de 60 (sessenta) meses, incluídos todos os softwares e suas licenças de uso, gerenciamento centralizado, serviços de implantação, garantia de atualização contínua e suporte técnico durante o período de garantia com repasse de conhecimento da solução a fim de atender às necessidades do Ministério da Mulher, da Família e dos Direitos Humanos, conforme condições, quantidades e exigências estabelecidas neste Edital e seus anexos.

1.2. A licitação será realizada em único item.

Item	Objeto	Descrição	Qtde
1	Aquisição de Solução Integrada de Segurança - Firewall	Solução de Next Generation Firewall em alta disponibilidade incluindo IPS, prevenção contra ameaças de vírus, spywares, malwares “Zero Day”, Filtro de URL com suporte técnico, licenciamento e garantia por 60 meses.	2

2. **ESPECIFICAÇÕES - REQUISITOS GERAIS**

2.1. Todos os equipamentos firewall e a solução de gerência integrada devem ser do mesmo fabricante, inclusive os sistemas operacionais executados por esses equipamentos;

2.2. Todos os equipamentos e seus componentes deverão ser novos, sem uso, e entregues em perfeito estado de funcionamento, sem marcas, amassados, arranhões ou outros problemas físicos, acondicionados em suas embalagens originais e acompanhados de todos os acessórios, cabos, conectores, kits de fixação, trilhos, fibras óticas (incluindo sua fusão, se necessário), patchcords, transceivers, etc, necessários às suas instalações e operação em rack de 19”;

2.3. Não serão aceitos equipamentos em modo End of Support durante a vigência da garantia e que estejam em modo End of Life no ato da assinatura do contrato;

2.3.1. A exigência acima encontra fundamento na necessidade que a Administração Pública tem de resguardar seus interesses, no sentido de estabelecer exigências mínimas objetivando evitar que ocorra aquisição de equipamentos que tenham

seu ciclo de vida descontinuado em um curto prazo, ou para os quais não haja mais suporte técnico e atualizações antes do fim do período de garantia, que é de 60 (sessenta) meses.

2.3.2. No ato da assinatura do contrato, caso o equipamento registrado em ata não atenda o disposto no item 2.1, poderá ser aceito equipamento de capacidade técnica igual ou superior, da mesma série ou linha ou família, desde que atenda a todos os requisitos técnicos disposto no edital.

2.4. O fabricante deverá atualizar firmwares e softwares da solução para novas versões durante toda a vigência da garantia.

2.5. Todas as funcionalidades adquiridas de hardware e software devem operar conforme disposto neste Termo de Referência durante o prazo de garantia dos equipamentos, ou seja, o fornecedor deve garantir a atualização completa das funcionalidades no prazo referido, não sendo permitida a cobrança de quaisquer valores adicionais pelo uso dos hardwares e softwares para esse período. As funcionalidades deverão permanecer ativas, mesmo que não sejam atualizadas após o fim do prazo da garantia.

2.5.1. Após o prazo da garantia, os equipamentos deverão permanecer com todas as funcionalidades operacionais, com as atualizações imediatamente anteriores a data final da garantia dos equipamentos.

3. Por plataforma de segurança entende-se hardware e software integrados do tipo appliance.

3.1. A plataforma de segurança deve possuir a capacidade e as características abaixo, por equipamento:

3.2. Throughput de 4 Gbps com a funcionalidade de controle de aplicação habilitada para todas as assinaturas que o fabricante possuir;

3.3. Throughput de 2.1 Gbps com as seguintes funcionalidades habilitadas simultaneamente para todas as assinaturas que a plataforma de segurança possuir devidamente ativadas e atuantes: controle de aplicação IPS, Antivírus e Antispyware. Caso o fabricante divulgue múltiplos números de desempenho para qualquer uma destas funcionalidades, somente o de menor valor será aceito;

3.4. 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 as sanções previstas em lei;

3.5. Os documentos públicos devem comprovar os throughputs aferidos com tráfego HTTP ou blend de protocolos definidos pelo fabricante como tráfego real (real-word traffic blend ou similar);

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

3.7. Suporte a, no mínimo, 900.000 conexões simultâneas;

3.8. Suporte a, no mínimo, 50.000 novas conexões por segundo;

3.9. Fonte redundante 120/240 AC ou DC;

3.10. Disco Solid State Drive (SSD) de, no mínimo, 240 GB;

3.11. 12 (doze) interfaces de rede 1 Gbps, sendo pelo menos 4 do tipo SFP;

3.12. Suportar 04 (quatro) interfaces de rede 10 Gbps SFP+;

3.13. 2 (duas) interfaces de 1Gbps dedicadas para alta disponibilidade;

3.14. 1 (uma) interface de rede 1 Gbps dedicada para gerenciamento;

3.15. 1 (uma) interface do tipo console ou similar;

3.16. Suporte a, no mínimo, 150 (cento e cinquenta) zonas de segurança;

3.17. Estar licenciada para ou suportar sem o uso de licença, pelo menos 1.000 (um mil) clientes de VPN SSL simultâneos;

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

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

5. 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;

6. 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;

7. 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.

CARACTERÍSTICAS GERAIS

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

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

7.3. 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;

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

7.5. 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;

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

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

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

7.9. Suporte a 4094 VLAN Tags 802.1q;

7.10. Agregação de links 802.3ad e LACP;

7.11. Policy based routing ou policy based forwarding;

7.12. Roteamento multicast (PIM-SM);

7.13. DHCP Relay;

7.14. DHCP Server;

7.15. Jumbo Frames;

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

7.17. Suportar sub-interfaces ethernet logicas.

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

7.19. 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;

7.20. Deve suportar os seguintes tipos de NAT:

7.21. Nat dinâmico (Many-to-1);

7.22. Nat dinâmico (Many-to-Many);

7.23. Nat estático (1-to-1);

7.24. NAT estático (Many-to-Many);

7.25. Nat estático bidirecional 1-to-1;

7.26. Tradução de porta (PAT);

7.27. NAT de Origem;

7.28. NAT de Destino;

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

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

7.31. Deve implementar o protocolo ECMP;

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

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

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

7.35. 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, quatro links;

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

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

7.38. 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;

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

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

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

7.42. Proteção contra anti-spoofing;

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

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

7.45. 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;

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

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

7.48. Suportar a OSPF graceful restart;

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

7.50. 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;

7.51. 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);

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

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

7.54. 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;

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

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

7.57. Em modo transparente;

7.58. Em layer 3;

7.59. A configuração em alta disponibilidade deve sincronizar:

7.60. Sessões;

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

7.62. Certificados de-criptografados;

7.63. Associações de Segurança das VPNs;

7.64. Tabelas FIB;

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

7.66. 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.

7.67. A solução deve possuir a capacidade de detectar e bloquear tentativas de resolução de domínios gerados de forma automática através de algoritmos (Domain generation algorithm - DGA);

7.68. A solução deve mostrar nos logs as seguintes informações sobre domínios DGA:

7.69. Domínio suspeito identificado;

7.70. ID de assinatura de detecção;

7.71. Usuário logado na estação/servidores que originou o tráfego;

7.72. Aplicação;

7.73. Porta de destino;

7.74. IP de origem;

7.75. IP de destino;

7.76. Horário;

7.77. Ação do firewall;

7.78. Severidade;

7.79. A solução deve possuir sistema de análise automático para detectar e bloquear encapsulamento de DNS com fins de roubo de dados e comunicações de comando e controle;

7.80. A análise automática deve incluir, no mínimo, as seguintes características:

7.81. Padrões de consulta;

7.82. Entropia;

7.83. Análise de frequência n-gram de domínios;

7.84. Taxa de consultas.

CONTROLE POR POLÍTICA DE FIREWALL

7.85. Deverá suportar controles por zona de segurança.

7.86. Controles de políticas por porta e protocolo.

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

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

7.89. 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.

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

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

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

7.93. Controle, inspeção e de-criptografia de SSL por política para tráfego de entrada (Inbound) e Saída (Outbound).

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

7.95. Deve de-criptografar tráfego Inbound e Outbound em conexões negociadas com TLS 1.2;

7.96. Deve de-criptografar sites e aplicações que utilizam certificados ECC, incluindo Elliptical Curve Digital Signature Algorithm (ECDSA);

7.97. Controle de inspeção e de-criptografia de SSH por política;

7.98. A de-criptografia de SSH deve possibilitar a identificação e bloqueio de tráfego caso o protocolo esteja sendo usado para tunelar aplicações como técnica evasiva para burlar os controles de segurança;

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

7.100. É permitido uso de appliance externo, específico para a de-criptografia de (SSL e TLS), com espelhamento de cópia do tráfego de-criptografado tanto para o firewall, quanto para as soluções de análise.

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

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

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

7.104. Suporte a objetos e regras IPV6.

7.105. Suporte a objetos e regras multicast.

7.106. Deve suportar no mínino 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;

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

CONTROLE DE APLICAÇÕES

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

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

7.110. 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;

7.111. 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;

7.112. Deve inspecionar o payload de 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;

7.113. 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;

7.114. 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.

7.115. 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;

7.116. 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 especificas 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;

7.117. 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;

7.118. 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;

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

7.120. Atualizar a base de assinaturas de aplicações automaticamente;

7.121. Reconhecer aplicações em IPv6;

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

7.123. 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;

7.124. 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;

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

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

7.127. 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;

7.128. 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:

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

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

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

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

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

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

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

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

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

7.138. Tecnologia utilizada na aplicações (Client-Server, Browse Based, Network Protocol, etc).

7.139. Nível de risco da aplicação.

7.140. Categoria e sub-categoria de aplicações.

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

PREVENÇÃO DE AMEAÇAS

7.142. 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.

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

7.144. 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.

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

7.146. 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;

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

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

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

7.150. Deve permitir o bloqueio de vulnerabilidades.

7.151. Deve permitir o bloqueio de exploits conhecidos.

7.152. Deve incluir proteção contra ataques de negação de serviços.

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

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

7.155. Análise de padrões de estado de conexões;

7.156. Análise de decodificação de protocolo;

7.157. Análise para detecção de anomalias de protocolo;

7.158. Análise heurística;

7.159. IP Defragmentation;

7.160. Remontagem de pacotes de TCP;

7.161. Bloqueio de pacotes malformados.

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

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

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

7.165. 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;

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

7.167. Possuir assinaturas para bloqueio de ataques de buffer overflow;

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

7.169. 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;

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

7.171. 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;

7.172. Suportar bloqueio de arquivos por tipo;

7.173. Identificar e bloquear comunicação com botnets;

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

7.175. Deve suportar referência cruzada com CVE;

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

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

7.178. Deve suportar a captura de pacotes (PCAP), por assinatura de IPS e Antyspyware;

7.179.

7.180. 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;

7.181. 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;

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

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

7.184. Deve incluir proteção contra vírus em conteúdo HTML e javascript, software espião (spyware) e worms.

7.185. Proteção contra downloads involuntários usando HTTP de arquivos executáveis. maliciosos.

7.186. Rastreamento de vírus em pdf.

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

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

ANÁLISE DE MALWARES MODERNOS

7.189.

7.190. 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 dever possuir funcionalidades para análise de Malwares não conhecidos incluídas na própria ferramenta ou entregue com composição com outro fabricante;

7.191. 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;

7.192. 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;

7.193. 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.;

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

7.195. Suportar a análise de arquivos maliciosos em ambiente controlado com, no mínimo, sistema operacional Windows XP e Windows 7 (64 bits);

7.196. 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;

7.197. 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;

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

7.199. 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;

7.200. 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);

7.201. 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;

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

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

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

7.205. 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.

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

7.207. Caso seja necessário 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;

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

7.209. Suportar a análise de arquivos do pacote office (.doc, .docx, .xls, .xlsx, .ppt, .pptx), arquivos java (.jar e class), Android APKs, MacOS (mach-O, DMG e PKG), Linux (ELF), RAR e 7-ZIP no ambiente de sandbox;

7.210. Deve atualizar a base com assinaturas para bloqueio dos malwares identificados em sand-box com frequência de pelo menos, 5 minutos

7.211. Permitir o envio de arquivos e links para análise no ambiente controlado via de forma automática via API.

7.212. Deve permitir o envio para análise em sand-box de malwares bloqueados pelo antivírus da solução;

FILTRO DE URL

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

7.214. 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);

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

7.216. 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.

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

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

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

7.220. Suporta base ou cache de URLs local no appliance, evitando delay de comunicação/validação das URLs;

7.221. Possui pelo menos 60 categorias de URLs;

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

7.223. Suporta a criação categorias de URLs customizadas;

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

7.225. Permite a customização de página de bloqueio;

7.226. 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;

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

7.228. 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);

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

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

IDENTIFICAÇÃO DE USUÁRIOS

7.231. 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;

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

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

7.234. 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;

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

7.236. 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;

7.237. 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);

7.238. Suporte a autenticação Kerberos;

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

7.240. 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;

7.241. 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;

7.242. 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;

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

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

QOS

7.245. 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.

7.246. Suportar a criação de políticas de QoS por:

7.247. Endereço de origem

7.248. Endereço de destino

7.249. Por usuário e grupo do LDAP/AD.

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

7.251. Por porta;

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

7.253. Banda Garantida

7.254. Banda Máxima

7.255. Fila de Prioridade.

7.256. Suportar priorização RealTime de protocolos de voz (VOIP) como H.323, SIP, SCCP, MGCP e aplicações como Skype.

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

7.258. Deve implemetar 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);

7.259. Disponibilizar estatísticas RealTime para classes de QoS.

7.260. Deve suportar QOS (traffic-shapping), em interface agregadas;

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

7.262.

FILTRO DE DADOS

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

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

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

7.266. Suportar identificação de arquivos compactados e a aplicação de politicas sobre o conteúdo desses tipos de arquivos;

7.267. 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;

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

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

GEO-LOCALIZAÇÃO

7.270. Suportar a criação de políticas por Geo Localização, permitindo o tráfego de determinado País/Países sejam bloqueados.

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

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

VPN

7.273. Suportar VPN Site-to-Site e Cliente-To-Site;

7.274. Suportar IPSec VPN;

7.275. Suportar SSL VPN;

7.276. A VPN IPSEc deve suportar:

7.277. 3DES;

7.278. Autenticação MD5 e SHA-1;

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

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

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

7.282. Autenticação via certificado IKE PKI.

7.283. Deve possuir interoperabilidade com os seguintes fabricantes:

7.284. Cisco;

7.285. Checkpoint;

7.286. Juniper;

7.287. Palo Alto Networks;

7.288. Fortinet;

7.289. Sonic Wall;

7.290. 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 throubleshooting;

7.291. A VPN SSL deve suportar:

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

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

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

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

7.296. 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;

7.297. 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;

7.298. Atribuição de DNS nos clientes remotos de VPN;

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

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

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

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

7.303. 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;

7.304. 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;

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

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

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

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

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

7.310. 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;

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

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

7.313. O agente de VPN a ser instalado nos equipamentos desktop e laptops, dever 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;

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

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

7.316. Antes do usuário autenticar na estação;

7.317. Após autenticação do usuário na estação;

7.318. Sob demanda do usuário;

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

7.320. 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;

7.321. 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;

7.322. 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;

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

CONSOLE DE GERÊNCIA E MONITORAÇÃO

7.324. Deve possuir solução de gerenciamento centralizado, possibilitando o gerenciamento de diversos equipamentos.

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

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

7.327. O gerenciamento centralizado poderá ser entregue como appliance físico ou virtual. Caso seja entregue em appliance fisíco deve ser compatível com rack 19 polegadas e possuir todos acessórios necessários para sua instalação. Caso seja entregue em appliance virtual dever ser compatível com VMware ESXi;

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

7.329. 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;

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

7.331. 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;

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

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

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

7.335. 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;

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

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

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

7.339. 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;

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

7.341. O gerenciamento deve permitir/possuir:

7.342. Criação e administração de políticas de firewall e controle de aplicação;

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

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

7.345. Monitoração de logs;

7.346. Ferramentas de investigação de logs;

7.347. Debugging;

7.348. Captura de pacotes.

7.349. Acesso concorrente de administradores;

7.350. 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;

7.351. 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.

7.352. 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 mesmos na configuração do dispositivo;

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

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

7.355. 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 cliente-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;

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

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

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

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

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

7.361. Deve atribuir sequencialmente um número a cada regra de firewall, NAT, QOS e regras de DOS;

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

7.363. Criação de regras com data de expiração;

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

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

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

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

7.368. Validação de regras antes da aplicação;

7.369. 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.

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

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

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

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

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

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

7.376. 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;

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

7.378. 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;

7.379. 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;

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

7.381. 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;

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

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

7.384. Deve possuir mecanismo "Drill-Down" para navegação nos relatórios em RealTime;

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

7.386. 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;

7.387. 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;

7.388. Deve ser possível exportar os logs em CSV;

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

7.390. Rotação do log;

7.391. 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;

7.392. 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;

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

7.394. Situação do dispositivo e do cluster;

7.395. Principais aplicações;

7.396. Principais aplicações por risco;

7.397. Administradores autenticados na gerência da plataforma de segurança;

7.398. Número de sessões simultâneas;

7.399. Status das interfaces;

7.400. Uso de CPU;

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

7.402. Resumo gráfico de aplicações utilizadas;

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

7.404. Principais aplicações por taxa de transferência de bytes;

7.405. Principais hosts por número de ameaças identificadas;

7.406. 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;

7.407. Deve permitir a criação de relatórios personalizados;

7.408. 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;

7.409. Gerar alertas automáticos via:

7.410. Email;

7.411. SNMP;

7.412. Syslog;

7.413. A plataforma de segurança deve permitir através de API-XML (Application Program Interface) a integração com sistemas existentes no ambiente da contratante de forma a possibilitar que aplicações desenvolvidas na contratante possam interagir em RealTime com a solução possibilitando assim que regras e políticas de segurança de possam ser modificadas por estas aplicações com a utilização de scripts em linguagens de programação como Perl ou PHP.

ANEXO B - MODELO DE TERMO DE RECEBIMENTO PROVISÓRIO

MINUTA DO TERMO DE RECEBIMENTO PROVISÓRIO	
Contrato N°:	
Nº da OS/OFB:	
Objeto:	
Contratante	MINISTÉRIO DA MULHER, DA FAMÍLIA E DOS DIREITOS HUMANOS
Contratada:	
TERMOS Por este instrumento, atestamos, para fins de cumprimento do disposto no art. 2º inciso XXI, instrução normativa nº 1, de 4 de abril de 2019, emitida pela Secretaria de Governo Digital, que os serviços e/ou ou bens, integrantes da OS/OFB acima identificada, ou conforme definido no Modelo de Execução do contrato supracitado, foram recebidos nesta data e serão objetos de avaliação quanto à adequação da Solução de Tecnologia da Informação e à conformidade de qualidade, de acordo com os Critérios de Aceitação previamente definidos no Modelo de Gestão do contrato pela Contratante. Ressaltamos que o recebimento definitivo destes serviços e/ou bens ocorrerá em até 10 dias, desde que não ocorram problemas técnicos ou divergências quanto às especificações constantes do Termo de Referência do Contrato acima identificado.	

ANEXO C - MODELO DE TERMO DE RECEBIMENTO DEFINITIVO

MINUTA DO TERMO DE RECEBIMENTO DEFINITIVO	
Contrato N°:	
Nº da OS/OFB:	
Objeto:	

Contratante	MINISTÉRIO DA MULHER, DA FAMÍLIA E DOS DIREITOS HUMANOS
Contratada:	

TERMOS
Por este instrumento, atestamos, para fins de cumprimento do disposto no art. 2º inciso XXI, instrução normativa nº 1, de 4 de abril de 2019, emitida pela Secretaria de Governo Digital, que os serviços e/ou ou bens, integrantes da OS/OFB acima identificada, ou conforme definido no Modelo de Execução do contrato supracitado, foram recebidos nesta data e serão objetos de avaliação quanto à adequação da Solução de Tecnologia da Informação e à conformidade de qualidade, de acordo com os Critérios de Aceitação previamente definidos no Modelo de Gestão do contrato pela Contratante.

De acordo

Em _____/_____/_____

Gestor do Contrato	**Fiscal Requisitante**
_____ Assinatura/Carimbo	_____ Assinatura/Carimbo

Recebido

Em _____/_____/_____.

Preposto do Contrato

_____
Assinatura/Carimbo

ANEXO D- TERMO DE COMPROMISSO DE SIGILO E SEGURANÇA DA INFORMAÇÃO

TERMO DE COMPROMISSO DE SIGILO E SEGURANÇA DA INFORMAÇÃO

Este TERMO DE COMPROMISSO (“TERMO”) é celebrado entre:

A. CONTRATANTE Ministério da Mulher, da Família e dos Direitos Humanos - MMFDH, Endereço: SCS Quadra 9, Lote C, Ed. Parque Cidade Corporate, Torre A, 10° Andar, Asa Sul, CEP 70308-200, Brasília/DF, inscrito no CNPJ/MF XX, neste ato representado pelo Gestor do Contrato xx/xxxx, e

B. CONTRATADA xxxxxxxx, Endereço xxxxxxxx, inscrita no CNPJ/MF xxxxxx, personificação xxxxxx, neste ato representada por seus respectivos procuradores abaixo assinados, na forma de seus respectivos Contratos Sociais. O MMFDH e a CONTRATADA podem ser referidas individualmente como PARTE e coletivamente como PARTES, onde o contexto assim o exigir.

CONSIDERANDO QUE as PARTES estabeleceram ou estão considerando estabelecer uma relação de negócio que inclui o XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX;

CONSIDERANDO QUE as PARTES podem divulgar entre si INFORMAÇÕES CONFIDENCIAIS, conforme definido abaixo neste instrumento, sobre aspectos de seus respectivos negócios, e em consideração da divulgação destas INFORMAÇÕES CONFIDENCIAIS; CONSIDERANDO QUE as PARTES desejam ajustar as condições de revelação das INFORMAÇÕES CONFIDENCIAIS, bem como definir as regras relativas ao seu uso e proteção;

RESOLVEM as PARTES celebrar o presente TERMO DE COMPROMISSO DE MANUTENÇÃO DE SIGILO, o qual se regerá pelas considerações acima, bem como pelas cláusulas e condições a seguir:

1. Para a finalidade deste Termo, “INFORMAÇÕES CONFIDENCIAIS” significarão todas e quaisquer informações divulgadas por uma PARTE (de acordo com este instrumento, a “Parte Divulgadora”) à outra PARTE (de acordo com este instrumento, a “Parte Recebedora”), em forma escrita ou verbal, tangível ou intangível, patenteada ou não, de natureza técnica, operacional, comercial, jurídica, a qual esteja claramente marcada como CONFIDENCIAL, incluindo, entre outras, mas não se limitando a, segredos comerciais, know-how, patentes, pesquisas, planos de negócio,

informações de marketing, informações de usuários, situação financeira, métodos de contabilidade, técnicas e experiências acumuladas, e qualquer outra informação técnica, comercial e/ou financeira, seja expressa em notas, cartas, fax, memorandos, acordos, termos, análises, relatórios, atas, documentos, manuais, compilações, código de software, e-mail, estudos, especificações, desenhos, cópias, diagramas, modelos, amostras, fluxogramas, programas de computador, discos, disquetes, fitas, pareceres e pesquisas, ou divulgadas verbalmente e identificadas como confidenciais por ocasião da divulgação.

2. Não serão incluídas nas INFORMAÇÕES CONFIDENCIAIS quaisquer informações que: (i) sejam geralmente conhecidas, ou subsequentemente se tornem disponíveis ao comércio ou ao público; (ii) estejam na posse legal da Parte Recebedora antes da divulgação pela Parte Divulgadora; ou (iii) sejam legalmente recebidas pela Parte Recebedora de um terceiro, desde que essas informações não tenham chegado ao conhecimento da Parte Recebedora através do referido terceiro, direta ou indiretamente, a partir da Parte Divulgadora numa base confidencial.

3. Quando a divulgação de INFORMAÇÕES CONFIDENCIAIS for necessária para estrito atendimento de ordem judicial ou agência governamental, o mesmo se procederá da seguinte maneira: (i) a Parte Recebedora fica obrigada a comunicar o teor da determinação judicial à Parte Divulgadora no prazo de 2 (dois) dias úteis a contar do recebimento da ordem, no caso de se tratar de determinação para cumprimento em prazo máximo de 5 (cinco) dias; ou no prazo de uma hora a contar do recebimento, no caso de se tratar de ordem judicial para cumprimento no prazo máxima de até 48 (quarenta e oito) horas; e (ii) fica a Parte Recebedora obrigada também a enviar à Parte Divulgadora cópia da resposta dada à determinação judicial ou administrativa concomitantemente ao atendimento da mesma. A Parte Recebedora cooperará com a Parte Divulgadora para possibilitar que a Parte Divulgadora procure uma liminar ou outra medida de proteção para impedir ou limitar a divulgação dessas Informações Confidenciais.

4. A Parte Recebedora não divulgará nenhuma INFORMAÇÃO CONFIDENCIAL da Parte Divulgadora a nenhum terceiro, exceto para a finalidade do cumprimento deste Termo e com o consentimento prévio por escrito da Parte Divulgadora. Além disso:

A. A Parte Recebedora, (i) não usará as INFORMAÇÕES CONFIDENCIAIS para interferir, direta ou indiretamente, com nenhum negócio real ou potencial da Parte Divulgadora, e (ii) não usará as Informações Confidenciais para nenhuma finalidade, exceto avaliar uma possível relação estratégica entre as Partes.

B. As Partes deverão proteger as INFORMAÇÕES CONFIDENCIAIS que lhe forem divulgadas, usando o mesmo grau de cuidado utilizado para proteger suas próprias INFORMAÇÕES CONFIDENCIAIS.

C. A Parte Recebedora não revelará, divulgará, transferirá, cederá, licenciará ou concederá acesso a essas INFORMAÇÕES CONFIDENCIAIS, direta ou indiretamente, a nenhum terceiro, sem o prévio consentimento por escrito da Parte Divulgadora, estando este terceiro, condicionado à assinatura de um Termo de Compromisso de Manutenção de Sigilo prevendo as mesmas condições e obrigações estipuladas neste Termo.

D. A Parte Recebedora informará imediatamente à Parte Divulgadora de qualquer divulgação ou uso não autorizado das Informações Confidenciais da Parte Divulgadora por qualquer pessoa, e tomará todas as medidas necessárias e apropriadas para aplicar o cumprimento das obrigações com a não divulgação e uso limitado das obrigações das empreiteiras e agentes da Parte Recebedora.

E. A Parte Recebedora deverá manter procedimentos administrativos adequados à prevenção de extravio ou perda de quaisquer documentos ou INFORMAÇÕES CONFIDENCIAIS, devendo comunicar à Parte Divulgadora, imediatamente, a ocorrência de incidentes desta natureza, o que não excluirá sua responsabilidade.

F. A Parte Recebedora obrigará seu pessoal que possa ter acesso às INFORMAÇÕES CONFIDENCIAIS que cumpram tais obrigações de sigilo, assinando o TERMO DE CIÊNCIA.

5. As Partes se comprometem e se obrigam a tomar todas as medidas necessárias à proteção da informação confidencial da outra Parte, bem como para evitar e prevenir revelação a terceiros, exceto se devidamente autorizado por escrito pela Parte Divulgadora. De qualquer forma, a revelação é permitida para empresas coligadas, assim consideradas as empresas que direta ou indiretamente controlem ou sejam controladas pela Parte neste Termo. Além disso, cada Parte terá direito de revelar a informação a seus funcionários que precisem conhecê-la, para os fins deste Termo; tais funcionários deverão estar devidamente avisados acerca da natureza confidencial de tal informação, e estarão vinculados aos termos e condições do presente Termo de Compromisso de Manutenção de Sigilo independentemente de terem sido avisados do caráter confidencial da informação, ficando a Parte Recebedora responsável perante a Parte Divulgadora por eventual descumprimento do Termo.

6. O intercâmbio de informações nos termos deste instrumento não será interpretado de maneira a constituir uma obrigação de uma das Partes para celebrar qualquer Termo ou acordo de negócio, nem obrigarão a comprar quaisquer produtos ou serviços da outra ou oferecer para a venda quaisquer produtos ou serviços usando ou incorporando as Informações Confidenciais.

7. Cada Parte reconhece que em nenhuma hipótese este Termo será interpretado como forma de transferência de propriedade ou qualquer tipo de direito subsistido nas Informações Confidenciais da parte Divulgadora para a parte Recebedora, exceto o direito limitado para utilizar as Informações Confidenciais conforme estipulado neste Termo.

8. Este TERMO entrará em vigor por ocasião da assinatura pelas Partes. Os compromissos deste instrumento também serão obrigatórios às coligadas, subsidiárias ou sucessoras das Partes e continuará a ser obrigatório a elas até a ocasião em que a substância das Informações Confidenciais tenha caído no domínio público sem nenhum descumprimento ou negligência por parte da Parte Recebedora, ou até que a permissão para liberar essas Informações seja especificamente concedida por escrito pela Parte Divulgadora.

9. A omissão ou atraso em aplicar qualquer disposição deste Termo não constituirá uma renúncia de qualquer aplicação futura dessa disposição ou de quaisquer de seus termos. Se qualquer disposição deste Termo, ou sua aplicação, por qualquer razão e em qualquer medida for considerada inválida ou inexequível, o restante deste Termo e a aplicação de tal disposição a outras pessoas e/ou circunstâncias serão interpretados da melhor maneira possível para atingir a intenção das Partes signatárias.

10. As PARTES concordam que a violação do presente Termo, pelo uso de qualquer Informação Confidencial pertencente à Parte Divulgadora, sem sua devida autorização, causar-lhe-á danos e prejuízos irreparáveis, para os quais não existe remédio na lei. Desta forma, a Parte Divulgadora poderá, imediatamente, tomar todas as medidas extrajudiciais e judiciais, inclusive de caráter cautelar, como antecipação de tutela jurisdicional, que julgar cabíveis à defesa de seus direitos.

11. A Parte Recebedora deverá devolver, íntegros e integralmente, todos os documentos a ela fornecidos, inclusive as cópias porventura necessárias, na data estipulada pela Parte Reveladora para entrega, ou quando não mais for necessária a manutenção das Informações Confidenciais, comprometendo-se a não reter quaisquer reproduções (incluindo reproduções magnéticas), cópias ou segundas vias, sob pena de incorrer nas penalidades previstas neste Termo.

12. A Parte Recebedora deverá destruir quaisquer documentos por ela produzidos que contenham Informações Confidenciais da Parte Divulgadora, quando não mais for necessária a manutenção dessas Informações Confidenciais, comprometendo-se a não reter quaisquer reproduções (incluindo reproduções magnéticas), cópias ou segundas vias, sob pena de incorrer nas penalidades previstas neste Termo.

13. A inobservância de quaisquer das disposições de confidencialidade estabelecidas neste Termo sujeitará a Parte infratora, como também o agente causador ou facilitador, por ação ou omissão ou qualquer daqueles relacionados neste TERMO, ao pagamento, recomposição, de todas as perdas e danos, comprovadamente suportados ou demonstrados pela outra Parte, bem como as de responsabilidade civil e criminal respectivas, as quais serão apuradas em regular processo.

14. As obrigações de confidencialidade decorrentes do presente Termo, tanto quanto as responsabilidades e obrigações outras derivadas do presente Termo, vigorarão durante o período de 5 (cinco) anos após a divulgação de cada Informação Confidencial à Parte Recebedora.

15. O não exercício por qualquer uma das Partes de direitos assegurados neste instrumento não importará em renúncia aos mesmos, sendo tal ato considerado como mera tolerância para todos os efeitos de direito.

16. Alterações do número, natureza e quantidade das Informações Confidenciais disponibilizadas para a Parte Recebedora não descaracterizarão ou reduzirão o compromisso ou as obrigações pactuadas neste Termo de Compromisso de Manutenção de Sigilo, que permanecerá válido e com todos os efeitos legais em qualquer das situações especificadas neste Termo.

17. O acréscimo, complementação, substituição ou esclarecimento de qualquer das Informações Confidenciais disponibilizadas para a Parte Recebedora, em razão do presente objeto, serão incorporadas a este Termo, passando a fazer dele parte integrante, para todos os fins e efeitos, recebendo também a mesma proteção descrita para as informações iniciais disponibilizadas, não sendo necessário, nessas hipóteses, assinatura ou formalização de Termo Aditivo.

18. Este instrumento não deve ser interpretado como criação ou envolvimento das Partes, ou suas Afiliadas, nem em obrigação de divulgar informações confidenciais para a outra Parte.

19. O fornecimento de INFORMAÇÕES CONFIDENCIAIS pela Parte Divulgadora ou por uma de suas Afiliadas não implica em renúncia, cessão a qualquer título, autorização de uso, alienação ou transferência de nenhum direito, já obtido ou potencial, associado a tais informações, que permanecem como propriedade da Parte Divulgadora ou de suas Afiliadas, para os fins que lhe aprouver.

20. Nenhum direito, licença, direito de exploração de marcas, invenções, direitos autorais, patentes ou direito de propriedade intelectual estão aqui implícitos, incluídos ou concedidos por meio do presente Termo, ou ainda, pela

transmissão de Informações Confidenciais entre as Partes.

21. A CONTRATADA declara conhecer todas as Normas, Políticas e Procedimentos de Segurança estabelecidos pela Contratante para execução do CONTRATO, tanto nas dependências da Contratante como externamente.

22. A CONTRATADA responsabilizar-se-á integralmente e solidariamente, pelos atos de seus empregados praticados nas dependências da Contratante, ou mesmo fora dele, que venham a causar danos ou colocar em risco o patrimônio da CONTRATANTE.

23. Este TERMO contém o acordo integral de confidencialidade entre as PARTES com relação ao seu objeto. Quaisquer outros acordos, declarações, garantias anteriores ou contemporâneos com relação à proteção das Informações Confidenciais, verbais ou por escrito, serão substituídos por este Termo. Este Termo será aditado somente firmado pelos representantes autorizados de ambas as Partes.

24. Quaisquer controvérsias em decorrência deste Termo serão solucionadas de modo amistoso através do representante legal das PARTES, baseando-se nas leis da República Federativa do Brasil. E por estarem assim justas e contratadas, as Partes firmam o presente Instrumento em 03 (três) vias de igual teor e forma, na presença das testemunhas abaixo indicadas.

Brasília, ___ de _____ de 20XX.

DE ACORDO	
CONTRATANTE Nome Cargo SIAPE	CONTRATADA Nome CPF
Testemunha 1 Nome CPF	Testemunha 2 Nome CPF

Por este instrumento, os funcionários abaixo-assinados declaram ter ciência e conhecer o teor do Termo de Compromisso de Manutenção de Sigilo e as normas de segurança vigentes na Contratante.

ANEXO E - MODELO DE PROPOSTA DE PREÇOS

PROPOSTA DE PREÇOS

AO MINISTÉRIO DA MULHER, DA FAMÍLIA E DOS DIREITOS HUMANOS

Proposta que faz a empresa _____,CNPJ_____, para a o fornecimento dos seguintes itens ao Ministério da Mulher, da Família e dos Direitos Humanos, em conformidade com o Edital do Pregão Eletrônico nº _____/2020.

Item	**Descrição**	**Unidade**	**Quant.**	**Val. Unit.**	**Val.**

					Total
1					
VALOR TOTAL					

Declaro que no preço cotado estão inclusas todas as despesas que incidem direta e indiretamente sobre o objeto a ser fornecido, tais como impostos, taxas, tributos, insumos, mão-de-obra, Garantia e Suporte Técnico pelo período determinado no Termo de Referência, a contar da data de recebimento definitivo da solução, e outras.

Dados da empresa:
Razão Social:
CNPJ (MF) nº:
Inscrição Estadual nº:
Endereço:
Fone/Fax:
Cidade:

Estado:

CEP:

A presente proposta tem validade de 90 (noventa) dias.

Local e data:

_____

Assinatura e carimbo do Representante Legal da Empresa

Observação: Emitir em papel que identifique a licitante

ANEXO F - MODELO ORDEM DE FORNECIMENTO

IDENTIFICAÇÃO DA ORDEM DE SERVIÇO/FORNECIMENTO			
Nº DA OF	DATA DE EMISSÃO	Nº DO CONTRATO	DATA DO CONTRATO

Nome da Empresa:		
CNPJ:	Inscrição Estadual:	
Endereço:		
Cidade:		UF:
CEP:	Telefone:	E-mail

Descrição:				
Localidade/Endereço	Qtd	Data	Valor	Responsável pelo recebimento

A análise do fornecimento dos produtos permite concluir pelo encerramento da Ordem de Fornecimento, com as seguintes observações: Relatório de glosas: CIDADE, _____ de _____ de 20_____

Gestor / carimbo ou Assinatura Digital	Empresa / carimbo ou Assinatura Digital

A análise do fornecimento dos produtos permite concluir pelo encerramento da Ordem de Fornecimento, com as seguintes observações: CIDADE, _____ de _____ de 20_____

Gestor / carimbo	Empresa / carimbo

ANEXO G - MODELO DE TERMO DE INTEGRIDADE

TERMO DE INTEGRIDADE
Termo de Integridade e Ética: Eu,_____, representante legal da empresa_____, regularmente inscrita no CNPJ sob o n._____, declaro, para os devidos fins, que a empresa/organização ora qualificada não pratica e nem permite que pratiquem, sob sua esfera de atuação, atos contrários às leis, normas, regras e regulamentos vigentes no ordenamento jurídico brasileiro, que importem lesão à Administração Pública Nacional ou Estrangeira, nos termos do art. 5º da Lei nº 12.846 de 1º de agosto de 2013 - Lei Anticorrupção. Outrossim, declaro que a empresa envida os melhores esforços para prevenir, mitigar e erradicar condutas inadequadas da sua atuação e se determina de acordo com as melhores práticas do mercado. Reconheço que o que subscrevo é verdade, sob as penas da lei. LOCAL, DATA. Assinatura Cargo CPF

Documento assinado eletronicamente por **Henrique Alcântara Veloso Mota**, **Coordenador(a) de Infraestrutura Tecnológica**, em 16/10/2020, às 19:48, conforme o § 1º do art. 6º e art. 10 do Decreto nº 8.539/2015.

Documento assinado eletronicamente por **Helder Mota Gomes**, **Coordenador(a) Geral de Tecnologia da Informação**, em 16/10/2020, às 19:59, conforme o § 1º do art. 6º e art. 10 do Decreto nº 8.539/2015.

Documento assinado eletronicamente por **Tatiana Fernandes da Silva**, **Integrante Administrativo**, em 20/10/2020, às 13:39, conforme o § 1º do art. 6º e art. 10 do Decreto nº 8.539/2015.

Documento assinado eletronicamente por **Luciano Angelo Seffrin Bragagnolo**, **Subsecretário(a) de Orçamento e Administração**, em 20/10/2020, às 17:08, conforme o § 1º do art. 6º e art. 10 do Decreto nº 8.539/2015.

A autenticidade deste documento pode ser conferida no site https://sei.mdh.gov.br/autenticidade, informando o código verificador **1366522** e o código CRC **2B80FAAA**.

Referência: Processo nº 00135.217382/2019-00 SEI nº 1366522

1080218 00135.217382/2019-00

MINISTÉRIO DA MULHER, DA FAMÍLIA E DOS DIREITOS HUMANOS
COORDENAÇÃO DE INFRAESTRUTURA E SERVIÇOS
Setor Comercial Sul, quadra 09, Edifício Parque Cidade Corporate, Torre A Brasília, DF. CEP 70308-200. - http://www.mdh.gov.br

ESTUDO TÉCNICO PRELIMINAR DA CONTRATAÇÃO

PROCESSO Nº 00135.217382/2019-00

INTRODUÇÃO

A presente análise tem por objetivo demonstrar a viabilidade técnica e econômica da contratação de uma nova solução de segurança de redes - Firewall para o Ministério da mulher, da família e dos direitos humanos (MMFDH), bem como fornecer informações necessárias para subsidiar o respectivo processo.

Referência: Art. 11 da IN SGD/ME nº 1/2019.

1. DEFINIÇÃO E ESPECIFICAÇÃO DAS NECESSIDADES E REQUISITOS

1.1. Em virtude da MEDIDA PROVISÓRIA Nº 870, DE 1º DE JANEIRO DE 2019 que trata da organização básica dos órgãos da Presidência da República e dos Ministérios, a Secretaria Nacional de Juventude e a Comissão de Anistia passaram a integrar a pasta do MMFDH.

1.2. Além dessas duas entidades, também foram criadas novas secretarias e conselhos dentro da pasta do MMFDH e isso trouxe um aumento considerável por recursos de tecnologia da informação.

1.3. A pasta de trabalho do MMFDH, exemplificada no organograma acima, é segmentada em quatro localidades físicas - prédios, que são conectadas através de quatro links do SERPRO (Infovia) e interligadas no data center deste ministério. A solução de firewall atual controla e aplica regras de segurança nos quatro links da infovia além do link de saída para a internet.

1.4. A imagem abaixo descreve sucintamente a topologia de rede do MMFDH:

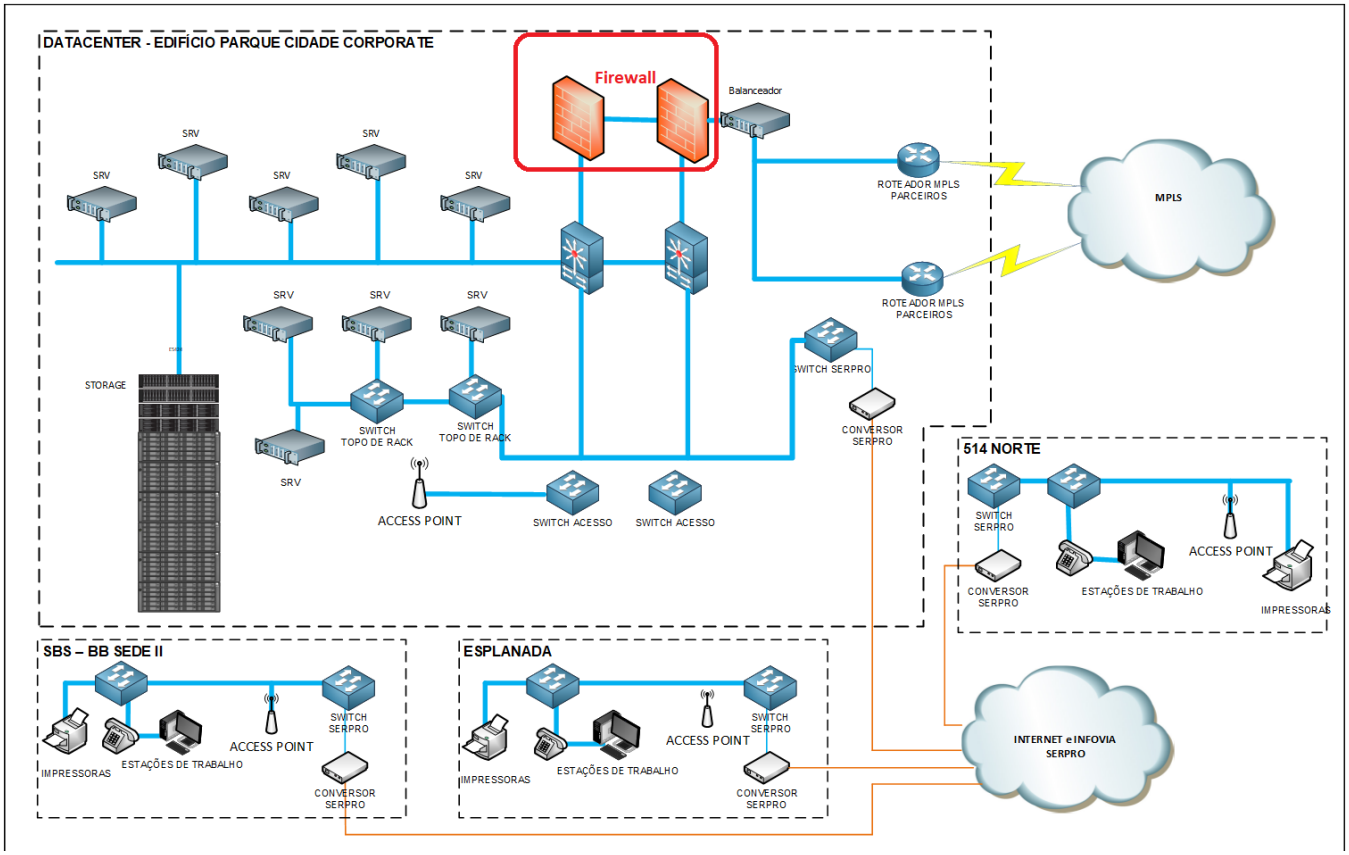

Imagem 2 - Topologia de Redes do MMFDH.

1.5. Decorrente da estruturação da área de TI do MMFDH, constata-se a necessidade de aquisição de uma solução de segurança de perímetro - firewall, para o data center, que tem por objetivo aplicar as diretrizes da Política de Segurança da Informação e Comunicação, PoSIC, visando atender plenamente às demandas atuais e futuras de segurança e vazão de tráfego.

1.6. Uma solução de Firewall consiste em um dispositivo de rede de computadores que tem como função aplicar regras de segurança a uma determinada rede. Seu fim de forma geral consiste em regular o tráfego de dados entre redes distintas e impedir a transmissão e/ou recepção de acessos nocivos ou não autorizados de uma rede para outra (invasão), protegendo assim os recursos de hardware e software. Este equipamento controla todas as comunicações que passam de uma rede a outra, permitindo ou negando seu tráfego. Nesta função, um firewall examina o tipo de serviço, tipo de portas, protocolos, podendo até mesmo inspecionar pacotes de informação.

1.7. O cenário atual de segurança cibernética demanda que as soluções de Firewall possuam recursos avançados de identificação de usuários, prevenção contra intrusos (IPS), controle de aplicações da Web 2.0 e identificação e prevenção de malwares.

1.8. Tais requisitos para uma solução de Firewall formam o conceito, definido pelo Gartner, como Next-Generation Firewall ou NGFW.

1.9. Outro quesito a ser considerado no ambiente de segurança cibernética é a evolução das ameaças digitais com lançamento de ameaças que não são detectadas através de tecnologias de prevenção tradicionais baseadas em padrões já conhecidos (assinaturas), tais ameaças são conhecidas como ameaças avançadas (em inglês, Advanced Threat Prevention – APT).

1.10. Os dispositivos de segurança NGFW existem na forma de software e de hardware, a combinação de ambos normalmente é chamado de "appliance". A complexidade de instalação depende do tamanho da rede, da política de segurança, da quantidade de regras que controlam o fluxo de entrada e saída de informações e do grau de segurança desejado.

1.11. O MMFDH conta hoje com uma solução de Cluster de Firewall, marca Fortigate, modelo Fortinet 1000C adquirida no início de 2014 através do contrato 37/2014 e o suporte e garantia dessa solução de firewall findou em dezembro de 2019.

1.12. Nesse período de 2014, o MMFDH era a antiga Secretaria de Direitos Humanos da Presidência da República, hoje com a atual estrutura de ministério, houve um aumento de demandas por recursos de conexão e segurança de redes, aumento do quantitativos de usuários e de sistemas em produção na infraestrutura do MMFDH.

1.13. Devido a esse aditamento de demandas e recursos de segurança, a solução de firewall está operando com carga de 60% e picos que chegam a 80% de processamento e de memória ram. Tal fato coloca o Ministério em situação de risco operacional, pois com a previsão de implementação de novos sistemas e, consequentemente, aumento do tráfego, caso ocorram ataques hackers à rede do Ministério existe grande chance deste equipamento atingir 100% de carga de processamento, o que levaria a indisponibilidade dos sistemas deste órgão.

1.14. Visto que o contrato de suporte e garantia da solução está próximo do fim e que o equipamento possui mais de cinco anos em produção, é essencial que se faça uma nova aquisição de solução de segurança de perímetro.

a) Em consulta ao documento Fortinet Product Life Cycle Information (0866429) que trata do ciclo de vida dos produtos da fabricante Fortinet, foi analisado que a data do fim do suporte da solução de firewall Fortigate 1000C está agendada para 17 de janeiro de 2022.

1.15. Fim da data de suporte (EOS): O marco final no ciclo de vida do produto é a data do fim do suporte. Após esta data, a Fortinet não venderá, fabricará ou melhorará o produto e não estará sob obrigação de prestar serviços de apoio. Em geral, a EOS para hardware ocorre 60 meses após fim da data do pedido."

1.16. Este projeto visa a aquisição de uma solução de firewall para um período de 60 meses e devido ao end of life do produto Fortigate 1000C não suportar os 60 meses, a renovação do suporte e garantia da solução Fortigate 1000C será excluído do escopo de análises de soluções.

1.17. Este projeto vai ao encontro dos objetivos estratégicos do MMFDH, no que tange a manter a segurança da informação institucional do ministério, a aderência aos normativos de segurança da informação do Gabinete de Segurança Institucional da Presidência da República e a nova lei geral de proteção de dados - Lei nº 13.709/2018.

1.18. Organizações realizam investimentos significativos em segurança da informação, com o intuito de garantir confidencialidade, disponibilidade e integridade das informações institucionais.

1.19. A contratação em questão visa a aquisição de uma solução de firewall capaz de garantir a confidencialidade, disponibilidade e integridade das informações institucionais. Para tanto esta solução necessariamente deverá possuir adequada capacidade de tráfego, bem como assegurar redundância física e lógica e melhorar a visibilidade do ambiente de rede deste ministério.

2. IDENTIFICAÇÃO DAS NECESSIDADES DE NEGÓCIO

2.1. O Ministério da mulher, da família e dos direitos humanos, assim como os diversos órgãos da esfera pública, necessita de proteção e segurança sobre o conteúdo armazenado e manipulado internamente nos respectivos ambientes para que sejam mantidas a confidencialidade, a integridade e a disponibilidade das informações existentes.

2.2. O MMFDH detém muitos sistemas sob sua responsabilidade. Tais sistemas abarcam muitas informações importantes para a tomada de decisão e eficiência dos processos em todas as áreas do órgão. Exemplo disso são as informações contidas no Sistema Eletrônico de Informações (SEI), o qual foi implantado em meados de 2015, otimizando o trâmite de processos administrativos no Órgão, agora realizado eletronicamente, eliminando a tramitação de processos físicos (papel).

2.3. Assim como o SEI, outros sistemas que lidam com informações sensíveis merecem a devida atenção quanto à segurança e proteção de ataques maliciosos por crackers ou criminosos do gênero, segue o exemplo de alguns sistemas.

a) ~~a)~~ O documento (0849262) possui a listagem dos sistemas que são executados na infraestrutura do MMFDH.

2.4. A solução de firewall atual em uso trabalha de forma estável com os seguintes serviços ativos: anti malware, Sistema de Prevenção de Intrusos - IPS e Filtro Web.

2.5. Existe ainda necessidade de se prover um quantitativo maior de acessos VPN SSL tendo em vista que o atual número licenças é insuficiente para as atribuições da TI e dos demais usuários.

2.6. Devido ao novo contrato de desenvolvimento - fábrica de software, do ministério, as demandas por recursos de conexão de VPN aumentaram consideravelmente.

2.7. A Portaria Nº 621, de 28 de dezembro de 2018 (Regula o teletrabalho no MMFDH) também trouxe demandas para uso de VPN.

2.8. Outro problema da atual situação do Ministério é que o serviço de inspeção de tráfego SSL não consegue funcionar concomitante com o sistema de prevenção de intrusos, fazendo com que 40% do tráfego de rede interno não seja inspecionado.

2.9. É importante ressaltar que o MMFDH possui a solução F5 que contém o serviço de inspeção de *tráfego criptografado.*

3. IDENTIFICAÇÃO DAS NECESSIDADES TECNOLÓGICAS

3.1. Capacidade para executar funcionalidades: anti-malware, Sistema de Prevenção de Intrusos - IPS, anti-bot, inspeção de tráfego criptografado SSL, filtro de conteúdo web, análise de malwares avançados e proteção de DNS, sem que haja perda de performance ou impacto nas transações e comunicações.

3.2. Suporte e Garantia 24 X 7 para 60 meses para a solução a ser adquirida.

3.3. Suporte ao controle de tráfego externo de 301Mb (Infovia) mais a possibilidade de suportar um segundo link de internet redundante. Além disso, a performance do equipamento é necessária para suportar o crescimento de 30% do tráfego interno ao longo do contrato.

3.4. É necessário também contar com o apoio de suporte técnico especializado, fornecido por empresa certificada pelo fabricante do software/hardware bem como apta a prestar suporte a ambientes corporativos críticos com comprovada excelência.

3.5. É necessário que a contratada realize o transferência de conhecimento da solução ofertada para a equipe de tecnologia do MMFDH.

3.6. É mandatório que toda a solução ofertada seja entregue, instalada, configurada no ambiente de redes do MMFDH.

4. DEMAIS REQUISITOS NECESSÁRIOS E SUFICIENTES À ESCOLHA DA SOLUÇÃO DE TIC

4.7. Gerenciamento centralizado de tráfego inbound/outbound e de eventos de segurança.

4.8. Capacidade de tráfego – capacidade de segmentar classes de tráfego em diferentes classes de dados.

4.9. Redundância e alta disponibilidade ava e passiva – tolerância ao aumento da exigência de recursos, mecanismos de tolerância a falhas.

4.10. Integridade e disponibilidade de serviços eletrônicos – assegurar a resiliência dos serviços eletrônicos do ministério, provendo uma camada interveniente de segurança.

4.11. A Solução de Firewall deverá permitir a filtragem de tráfego inbound/outbound, nas camadas TCP/IP 3 e 7, em conformidade com as regras estabelecidas na Política de Segurança da Informação e Comunicações.

4.12. Visando assegurar a disponibilidade da solução, os appliances deverão possuir capacidade de operar de forma redundante (failover), com sincronização em tempo-real de configuração e de estados das conexões. A redundância (failover) deverá permitir a operação nos modos Ativo-Ativo e Ativo-Passivo

4.13. Visando racionalizar o uso das soluções e serviços de Tecnologia da Informação, e considerando os benefícios e a efetiva necessidade de acesso remoto aos serviços internos, a solução de Firewall deverá suportar esquemas de VPN site-to-site e suportar VPN IPSec client-to-site.

4.14. A solução de firewall a ser adquirida deverá possuir interface de administração e monitoramento única e centralizada das políticas de firewall e VPN. Esta interface de administração e monitoramento única deverá possibilitar todas as definições e/ou alterações de regras e dispará-las para todos os dispositivos de segurança distribuídos ao longo da rede; de forma segura e com registro de logs das políticas instaladas.

4.15. O software de gerência deverá ser totalmente compatível com virtualização. A virtualização do software de gerência permitirá economia de custos com appliance dedicado e garantirá desempenho e disponibilidade à solução.

5. **ESTIMATIVA DA DEMANDA – QUANTIDADE DE BENS E SERVIÇOS**

5.1. Estudo para dimensionamento do equipamento, requisitos a serem atendidos:

- - Limite de utilização de carga de equipamento a ser adquirido: entre 20% e 30% de uso de processamento e memória (aproximadamente 1/3 do atual);
- - Taxa de crescimento do tráfego ao longo do contrato: 30%.
- - Capacidade de mínima de throughput para atender às demandas do MMFDH (conforme proporcionalidade de throughput /taxa de processamento e memória/crescimento do tráfego): 2.145 Mbps.

5.2. Conclui-se portanto que de acordo com os relatórios extraídos do firewall atual, com a expectativa de crescimento futura e a proporcionalidade entre throughput, taxa de processamento e memória, uma solução de NGFW ideal para atender o data center do MMFDH precisa ter no mínimo o suporte para no mínimo **2,1 Gbps de throughput** e que opere **OBRIGATORIAMENTE** com todas as funcionalidades de segurança habilitadas sem perda de desempenho ou indisponibilidade do sistema de proteção.

5.3. Os throughputs devem ser comprovados por documento de domínio público do fabricante. Caso o fabricante divulgue múltiplos números de desempenho para qualquer uma destas funcionalidades, somente o de menor valor será aceito.

5.4. A solução ideal também deverá suportar **IPsec VPN de pelo menos 2 Gbps, sem que haja perda de desempenho na solução.**

6. **ANÁLISE DE SOLUÇÕES**

6.1. Há várias soluções disponíveis no mercado que podem atender as necessidades deste ministério. No entanto, levaremos em conta aquelas soluções de mercado corporativas melhores pontuadas em testes de empresas especializadas tais como NSS LABS, Gartner, bem como casos de sucesso dentro do governo.

6.2. **É importante citar que como se trata de solução de hardware estão descartadas as possibilidades de soluções no Portal do Software Público Brasileiro, softwares livres ou públicos. As alternativas identificadas atendem aos padrões e-PING, e-ARQ, aplicáveis a esta contratação.**

6.3. Diante das possibilidades de implantação do projeto de expansão utilizamos como parâmetro para comparação a aquisição de um cluster com dois equipamentos com suas respectivas licenças, avaliações do produto e treinamento para os servidores do órgão.

6.4. **Existem duas alternativas disponíveis:**

6.5. **Renovação da garantia e suporte técnico da solução atual.**

6.5.1. Renovação da garantia e suporte técnico da solução atual foi descartada pelo motivo que o ciclo de vida do produto Fortinet 1000C encerrará em 2022. Esse prazo de dois anos de vida é muito inferior ao de 36 ou 60 meses que visa esta aquisição.

6.6. **Substituição de toda a solução atual por produtos de qualidade equivalentes às necessidades do MMFDH.**

6.7. I - Implica na aquisição de novos produtos, com foco em soluções de qualidade equivalente, ou seja, que sejam capazes de implementar todas as funcionalidades de segurança (controle de aplicações, controle de usuários, filtro web, IPS, Antivírus, AntiSpyware e anti malware Dia Zero) sem causar degradação de performance e que possam atender às demandas atuais e ao longo de 5 anos do MMFDH, conforme estudo abaixo:

I - **Cenário atual:**

a) Capacidade de throughput do equipamento atual com todas as funcionalidades habilitadas: 550 Mbps.

b) Taxa de utilização de carga do equipamento atual no ambiente de redes do MMFDH: entre 60% e 80% de uso de processamento e memória;

6.8. **Soluções disponíveis**

6.9. Há no mercado diversas soluções corporativas de **Next-Generation Firewall** (NGFW). Por essa razão, a análise de soluções é bastante complexa;

a) **Conceito Next-Generation Firewall:** Diferentemente de um modelo tradicional de firewall que faz controle somente por IP de origem, IP de destino, porta de origem, porta de destino e flags de protocolo, por exemplo a flag SYN do protocolo TCP. Um Next Generation Firewall vai além dessas capacidades mencionadas anteriormente, com análises profundas (Deep Inspection) do pacote que é trafegado por ele. Vamos a alguns exemplos práticos:

6.10. Em um NGFW, é possível analisar se um download que está sendo feito contém algum tipo de ameaça, por um ransomware, backdoor, minerador de bitcoin, ou outro malware qualquer, conhecido (que já tenha uma assinatura) ou

desconhecido (zero day), neste último a análise é feita através de uma sandbox local ou na nuvem, e que é extremamente importante possuir técnicas anti-evasivas e emulação.

6.11. Em uma outra situação o NGFW agrega função de IPS (Intrusion Prevenon System), ou seja, agrega funções que enxergam dentro dos pacotes de rede se existe alguém mal intencionado tentando explorar vulnerabilidades em algum serviço que rode na sua infraestrutura, por exemplo, apache, RDP, Oracle, Tomcat, JBoss, SSH, Nginx, SQL Server e muitos outros. Essa vulnerabilidade pode ser utilizada para derrubar algum serviço (Denial of Service - DOS), ganhar acesso indevido e roubar informações por exemplo (Data Loss - Vazamento de Dados).

6.12. Outra funcionalidade extremamente importante é a de URL Filtering, onde é possível controlar o acesso a milhares de sites não desejados, com base em políticas de segurança e evitar incidentes e uso indevido dos recursos de rede do órgão, por exemplo, uso de torrents, sites de Streaming (Nelix, Youtube, Vimeo, etc), Phishing, Pornografia, Spyware, de alto risco a segurança, Facebook (é possível dar acesso somente a parte do facebook, evitando acesso ao chat e a likes por exemplo), Whatsapp, Telegram e outras situações não desejadas. Importante é salientar também que esse tipo de firewall possibilita o bloqueio de ferramentas utilizadas normalmente para burlar proxies e firewalls, os anonymizers, como Ultra Surf, web proxy e técnicas de tunelamento por exemplo.

6.13. As features básicas de um Next Generation Firewall são as seguintes:

- · VPN
- · Identity and Computer Awareness
- · URL Filtering
- · Application Control
- · Intrusion and Threat Prevention
- · HTTPS / SSL Inspection
- · SandBox
- · Proteção de DNS

6.14. Um referencial de mercado amplamente utilizado, não apenas pela Administração Pública Federal, mas também por empresas privadas, mundialmente, é a análise independente e imparcial do Gartner;

6.15. Anualmente são publicados relatórios comparando as principais soluções do mercado em determinados nichos da tecnologia da informação. Em cada um desses relatórios, fabricantes são avaliados e posicionados em um gráfico (chamado de quadrante mágico) em que são pesados “habilidade de execução” e “completude de visão”. Isso representa uma visão do nível de maturidade e posicionamento no mercado das soluções disponíveis;

6.16. No contexto da presente contratação, existe o quadrante "Enterprise Network Firewall";

6.17. Segue o quadrante mágico mencionado:

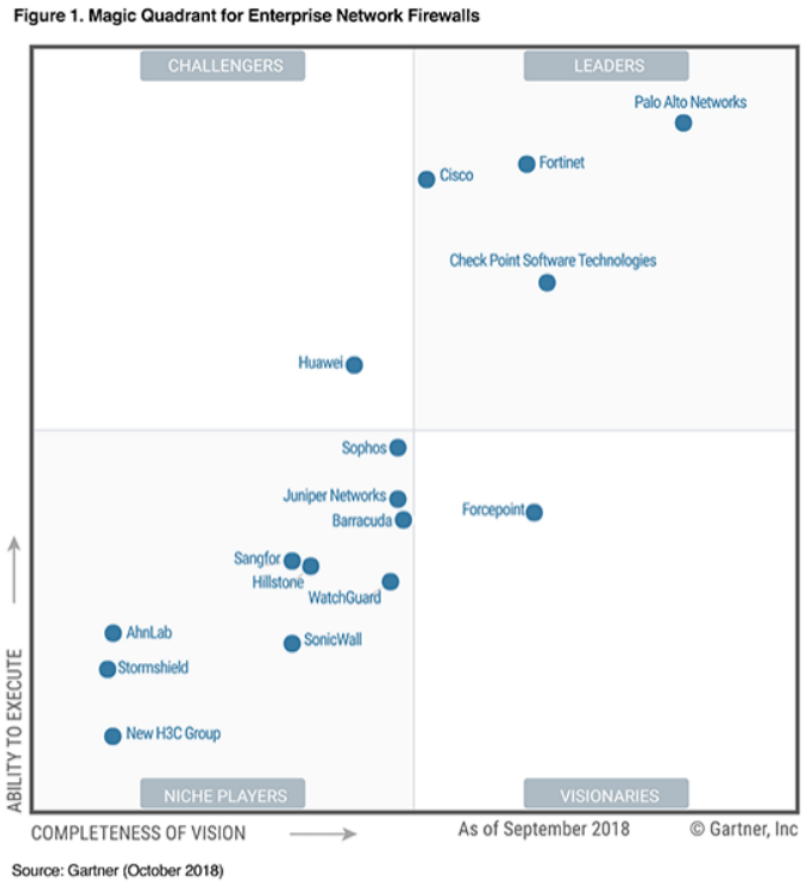

Imagem 3 - Quadrante magico do Gartner.

6.17.1. O estudo técnico observou as soluções que se encontram no quadrante mágico do Gartner como "Leaders", conforme tabela abaixo:

Comparativo de equipamentos de Firewall a partir da análise de líderes do Gartner					
Equipamento	**Threat Prevention Throughput (controle de aplicações, controle de usuários, Prevensão a Intrusos, Antivírus, AntiSpyware e anti malware Dia Zero habilitados)**	**IPSEC VPN Throughput**	**Portas 10Gbps (SFP+)**	**Armazenamento**	**Novas Conexões por segundo (com controle de aplicações, usuários, IPS e antimalware habilitados)**
FortiGate-1000C (Solução atualmente em uso)	550 Mbps	8 Gbps	2	128 GB	75.000
Check Point 5600	2,78 Gbps	6,5 Gbps	4	240 GB	185.000
Cisco firepower 4110	4,5 Gbps	8 Gbps	2 (opcionais)	200 GB	64.000
Palo Alto PA 3220	2,2 Gbps	2,5 Gbps	4	240 GB	58.000
Fortinet 1500D	5 Gbps	50 Gbps	8	2x240GB	300.000

7. REGISTRO DE SOLUÇÕES CONSIDERADAS INVIÁVEIS

7.1. Renovação da garantia e suporte técnico da solução atual.

7.1.1. Renovação da garantia e suporte técnico da solução atual foi descartada pelo motivo que o ciclo de vida do produto Fortinet 1000C encerrará em 2022. Esse prazo de dois anos de vida é muito inferior ao de 60 meses que visa esta aquisição.

7.2. Levando em consideração a possibilidade de renovar o suporte e garantia da solução atual existente no MMFDH, essa opção se tornou inviável visto que o end of life do produto está anunciado para 2022. Vide o item 2.7 e o documento Fortinet Product Life Cycle Information (0866429).

8. **ANÁLISE COMPARATIVA DE CUSTOS (TCO)**

8.1. Com base na conclusão da análise de aspecto técnico, foi realizada pesquisa sob o ponto de vista financeiro, em conformidade com a IN 03, da Secretaria de Gestão do Ministério do Planejamento, Orçamento e Gestão (de 24/04/2017);

8.2. Em 09 de setembro de 2019, ao realizar a pesquisa no referido portal utilizando a expressão "*Firewall*" como parâmetro de pesquisa para o campo "Descrição do Serviço", obteve êxito na pesquisa.

8.3. Em sequência, ao utilizar a mesma expressão no campo "Objeto da Compra" encontrou-se, a princípio, 82 processos de compra relacionados ao tema.

8.4. Deste universo de 82 contratações (SEI! 1167632), ao observar a quantidade ofertada de serviço, com o objetivo de tentar localizar algum contrato com a especificação **técnica similar** ao do MMFDH.

8.5. Em pesquisa de contratos semelhantes (por meio da planilha "Firewall" no site Compras Governamentais, consultada em 07/04/2020 como também pesquisas por outros contratos públicos realizados por meio da Internet), foram **consideradas 5 contratações**.

8.6. Tendo em vista a dificuldade de encontrar pregões com mesmo objeto, para complementar a análise de preços, fizemos pesquisa de mercado com empresas que fornecem equipamentos com o mesmo objeto pretendido. **Recebemos 4 propostas de mercado.**

8.7. Dos resultados filtrados que possuem semelhança com a necessidade do MMFDH, foram identificados os seguintes resultados:

Item	Fonte Consulta/Pesquisa		Valor	Resultado
Firewall 2 unidades, 12 meses	Agência Brasileira de Inteligência	R$	1.254.700,00	INEXEQUÍVEL
	Governo do Estado do Ceará	R$	1.851.400,00	EXEQUÍVEL
	Polícia Rodoviária Federal	R$	1.894.000,00	EXEQUÍVEL
	Instituto Nacional de Estudo e Pesquisa	R$	1.939.995,77	EXEQUÍVEL
	Tribunal Superior Federal	R$	3.874.000,00	EXCESSIVAMENTE ELEVADO
	Proposta de Fornecedor Fasthelp	R$	1.971.538,00	EXEQUÍVEL
	Proposta de Fornecedor Vtech	R$	2.154.000,00	EXEQUÍVEL
	Proposta de Fornecedor Compwire	R$	1.997.840,00	EXEQUÍVEL
	Proposta de Fornecedor Layertechnology	R$	2.113.684,00	EXEQUÍVEL
	Média dos Preços Exequíveis	**R$**	**1.988.922,54**	

Tabela 2 - Tabela referente aos contratos da APF de aquisição de solução de segurança.
As contratações acima são consideradas similares por vários parâmetros, devido a variação do cambio, motivo pelo qual a pesquisa de preço foi novamente realizada.

8.8. **Analisando os Editais dessas contratações similares é possível concluir que a realização de pregão eletrônico para contratação de nova solução de Next Generation Firewall é a única viável, que não há possibilidade adesão a ata de registro de preços vigentes e o pregão eletrônico permitirá maior competitividade entre os diferentes fabricantes.**

9. **DESCRIÇÃO DA SOLUÇÃO DE TIC A SER CONTRATADA**

9.1. **JUSTIFICATIVA DA SOLUÇÃO ESCOLHIDA**

9.1.1. Conforme demonstrado em estudo técnico e financeiro deste documento, o MMFDH tem a necessidade de trocar a solução existente para que haja aprimoramento da segurança de perímetro do órgão, tendo como principal enfoque a proteção da informação que permeia toda a estrutura tecnológica deste Ministério.

9.1.2. Foram observadas as especificações técnicas de funcionalidades, bem como de características de hardwares/software dos Termos de Referência dos processos mencionados na tabela de comparativos de preços deste estudo. A partir destes Termos de Referência citados foram definidas as Especificações Técnicas da solução pretendida pelo MMFDH.

9.1.3. As especificações técnicas definidas para este projeto foram baseadas nas especificações dos processos licitatórios já realizados e apontados na tabela abaixo. Processos estes que pudemos observar um considerável nível de competitividade entre diferentes fabricantes:

PROCESSO	DESCRIÇÃO	MODELO (FIREWALL)
CAPES - Nº 00005/2018 (SRP)	Solução de Proteção de Rede de Nova Geração contra ameaças avançadas, incluindo garantia e suporte técnico.	CHECK POINT 23500

ANAC - Nº 00015/2018 (SRP)	Equipamento de Firewall Tipo 1 instalado, implantado e operacional em cluster.	CHECK POINT 5900
ANAC - Nº 00015/2018 (SRP)	Equipamento de Firewall Tipo 2 instalado, implantado e operacional em cluster.	CHECK POINT 5600
UFOB - Nº 00012/2018 (SRP)	Firewall com filtro de conteúdo	FORTIGATE 2000E
DETRAN/RO - Nº 00067/2017 (SRP)	Aquisição de Solução de Appliance de Firewall do tipo UTM em cluster, suas respectivas licenças de uso com garantia para 60 meses.	CHECK POINT 15600
TCE/RJ - Nº 00068/2018 (SRP)	Aquisição de upgrade de firewall Palo Alto compatível com a solução atualmente implantada nas dependências deste Tribunal de Contas	PALO ALTO 5220
UFSJ - Nº 00046/2018 (SRP)	Aquisição de solução de segurança global (firewall) para os seis campi da UFSJ.	FORTIGATE 1500D

* É importante ressaltar que

9.1.4. O "*ANEXO A - ESPECIFICAÇÕES TÉCNICAS DA SOLUÇÃO*" foi resultado deste estudo com especificações mencionadas acima.

9.2. BENEFÍCIOS A SEREM ALCANÇADOS

- Maior proteção à informação.
- Mitigação de riscos inerentes a ataques maliciosos.
- Tornar usual as funcionalidades de segurança sem perda de desempenho ou indisponibilidade do sistema de proteção.
- Licenciamento e suporte para equipamentos da solução.
- Bloqueio de compartilhamento de informações sigilosas via cloud computing (SSL Inspection).
- Melhoria no gerenciamento das aplicações por parte da infraestrutura de TIC que poderá filtrar e observar quaisquer interações do usuário que foram realizadas.

9.3. NECESSIDADES DE ADEQUAÇÃO DO AMBIENTE PARA EXECUÇÃO CONTRATUAL

- Disponibilizar espaço físico para nova solução de segurança de perímetro;
- Disponibilizar instalações elétricas;
- Disponibilizar condicionamento do ar.

9.4. RECURSOS NECESSÁRIOS À CONTINUIDADE DO NEGÓCIO DURANTE E APÓS A EXECUÇÃO DO CONTRATO

- Os recursos humanos internos a serem alocados se referem aos fiscais técnico, administrativo e gestor do contrato que devem realizar suas atividades de acompanhamento e controle, conforme definido na IN nº 01/2019.
- Técnico da contratada de Sustentação de Ambiente de TIC.
- Servidores do Ministério serão alocados para realização de definições, acompanhamento e gerência da solução.

9.5. ESTRATÉGIA DE CONTINUIDADE CONTRATUAL - TRANSIÇÃO CONTRATUAL

- Qualquer interrupção referente à solução atual comprometerá a rede do ministério e poderá haver indisponibilidade da rede, gerando impactos diversos nas várias áreas do órgão.
- Por ter maior capacidade, a nova solução suportará todos os serviços da atual solução em situação emergencial. Portanto, haverá contingenciamento.
- A empresa contratada deverá prestar suporte proativo às duas soluções 24 (vinte e quatro) horas por dia e 7 (sete) dias por semana.
- Janelas de serviço para as mudanças de configuração e topologia deverão ocorrer em horários não comerciais, visando não afetar as atividades cotidianas do órgão.

10. ESTIMATIVA DE CUSTO TOTAL DA CONTRATAÇÃO

10.1. Para o cálculo do valor estimado, foram utilizados os valores médios encontrados nas tabela 2, na ordem de **R$1.988.922,54 (Um milhão, novecentos e oitenta e oito mil, novecentos e vinte e dois reais e cinquenta e quatro centavos).**

11. DECLARAÇÃO DE VIABILIDADE DA CONTRATAÇÃO

11.1. Assim, diante do exposto acima, declaramos ser **VIÁVEL** a contratação da solução demandada.

11.2. Em cumprimento ao disposto no Art. 11 da Instrução Normativa SGD/ME N° 1/2019, o presente documento segue assinado pelos Integrantes Requisitante e Técnico da Equipe de Planejamento da Contratação, designada pelo Documento de Oficialização da Demanda .

12. APROVAÇÃO E ASSINATURA

12.1. Conforme o § 2º do Art. 11 da IN SGD/ME nº 01, de 2019, o Estudo Técnico Preliminar segue aprovado e assinado pelos Integrantes Técnicos e Requisitantes, pela autoridade máxima da área de TIC, e pela autoridade superior, nos termos do § 3° do mesmo Art. 11.

EQUIPE DE PLANEJAMENTO DA CONTRATAÇÃO	
INTEGRANTE REQUISITANTE	*(Assinado eletronicamente)* **Helder Mota Gomes** Mat. 1584672
INTEGRANTE TÉCNICO	*(Assinado eletronicamente)* **Henrique Alcântara Veloso Mota** Mat. 1527028

AUTORIDADE SUPERIOR
Considerando a participação do Coordenador-Geral de TI na composição da Equipe de Planejamento da Contratação, e considerando o disposto no § 3° do Art. 11 da IN SGD/ME nº 01, de 2019, a **APROVO** o presente Estudo Técnico Preliminar, mediante competência contida no inciso II do art. 1º da Portaria Nº 431, de 28 de Fevereiro de 2020, conforme dispõe o inciso II do art. 9º do Decreto Nº 10.024, de 20 de setembro de 2019. (*Assinado Eletronicamente)* **LUCIANO BRAGAGNOLO** Subsecretário de Orçamento e Administração

Documento assinado eletronicamente por **Henrique Alcântara Veloso Mota**, **Coordenador(a) de Infraestrutura Tecnológica**, em 17/06/2020, às 15:42, conforme o § 1º do art. 6º e art. 10 do Decreto nº 8.539/2015.

Documento assinado eletronicamente por **Helder Mota Gomes**, **Coordenador(a) Geral de Tecnologia da Informação**, em 20/06/2020, às 21:03, conforme o § 1º do art. 6º e art. 10 do Decreto nº 8.539/2015.

Documento assinado eletronicamente por **Luciano Angelo Seffrin Bragagnolo**, **Subsecretário(a) de Orçamento e Administração**, em 22/06/2020, às 14:34, conforme o § 1º do art. 6º e art. 10 do Decreto nº 8.539/2015.

A autenticidade deste documento pode ser conferida no site https://sei.mdh.gov.br/autenticidade, informando o código verificador **1080218** e o código CRC **7EA9EB1D**.

Referência: Processo nº 00135.217382/2019-00 SEI nº 1080218

1338496 00135.217382/2019-00

MINISTÉRIO DA MULHER, DA FAMÍLIA E DOS DIREITOS HUMANOS
COORDENAÇÃO DE CONTRATOS E GESTÃO DE ATAS
SCS Quadra 09 - Lote C, Ed. Parque Cidade Corporate, Torre-A, 10º Andar
Brasília, DF. CEP 70308-200. - http://www.mdh.gov.br

MINUTA DE CONTRATO 02 - CCGA/CGL/SOAD/SE/MMFDH

	TERMO DE CONTRATO Nº XX/2020, QUE FAZEM ENTRE SI A UNIÃO, POR INTERMÉDIO DO MINISTÉRIO DA MULHER, DA FAMÍLIA E DOS DIREITOS HUMANOS E A EMPRESA XXX.

União, representada pelo **MINISTÉRIO DA MULHER, DA FAMÍLIA E DOS DIREITOS HUMANOS**, por intermédio da **SUBSECRETARIA DE ORÇAMENTO E ADMINISTRAÇÃO**, com sede no Setor Comercial Sul - B, Quadra 9, Lote C, Edifício Parque Cidade Corporate, 10º andar, Torre A, CEP 70308-200, na cidade de Brasília/DF, inscrito no CNPJ sob o n.º 27.136.980/0008-87, neste ato representado pelo Subsecretário de Orçamento e Administração, o Senhor **LUCIANO ANGELO SEFFRIN BRAGAGNOLO**, portador do RG nº 1.907.184 - SSP/DF e do CPF nº 902.177.801-72, designado por meio da Portaria n.º 1.036, de 6 de abril de 2020, publicada na Seção 2, do Diário Oficial da União – DOU, de 8 de abril de 2020, por subdelegação de competência fixada na Portaria n°1.256, de 22 de maio de 2020, publicado na Seção I do Diário Oficial da União-D.O.U de 25 de maio de 2020, doravante denominada **CONTRATANTE** e a **EMPRESA X,** com sede na XXXX**,** inscrita no CNPJ XXX, doravante designada **CONTRATADA**, neste ato representada pelo Sr. XXXX, portador da Carteira de Identidade nº RG nº XXX e CPF nº XXX, tendo em vista o que consta no Processo nº 00135.217382/2019-00, e em observância às disposições da Lei nº 8.666, de 21 de junho de 1993, da Lei nº 10.520, de 17 de julho de 2002, da Lei nº 8.248, de 22 de outubro de 1991, do Decreto nº 9.507, de 21 de setembro de 2018, do Decreto nº 7.174, de 12 de maio de 2010, da Instrução Normativa SGD/ME nº 1, de 4 de Abril de 2019 e da Instrução Normativa SEGES/MPDG nº 5, de 26 de maio de 2017 e suas alterações, resolvem celebrar o presente Termo de Contrato, decorrente do Pregão nº ...../20...., mediante as cláusulas e condições a seguir enunciadas.

1. **CLÁUSULA PRIMEIRA - OBJETO**

1.1. O objeto do presente instrumento é a aquisição de Solução Integrada de Segurança - Next Generation Firewall (NGFW) corporativo em alta disponibilidade para prover segurança e proteção da rede de computadores, contemplando gerência unificada com garantia de funcionamento pelo período de 60 (sessenta) meses, que serão prestados nas condições estabelecidas no Termo de Referência, anexo do Edital.

1.2. Este Termo de Contrato vincula-se ao Edital do Pregão, identificado no preâmbulo e à proposta vencedora, independentemente de transcrição.

1.3. Discriminação do objeto:

item	Descrição	CATMAT	Qtde	Valor Unitário (maximo)	Valor Considerando 12 meses (maximo)
1	Solução de Next Generation Firewall (hardware), incluindo IPS, prevenção contra ameaças de vírus, spywares, malwares "Zero Day", Filtro de URL com suporte técnico, licenciamento e garantia por 60 meses.	BR0150100	2	R$ 994.461,27	**R$ 1.988.922,54**

2. **CLÁUSULA SEGUNDA - VIGÊNCIA**

2.1. A vigência do contrato será de 12 meses prorrogáveis até 60 (sessenta) meses, contados a partir da data de sua assinatura.

2.2. A CONTRATADA não tem direito subjetivo à prorrogação contratual.

2.3. A prorrogação de contrato deverá ser promovida mediante celebração de termo aditivo.

3. **CLÁUSULA TERCEIRA - PREÇO**

3.1. O valor total da contratação é de R$..... (.....)

3.2. No valor acima estão incluídas todas as despesas ordinárias diretas e indiretas decorrentes da execução do objeto, inclusive tributos e/ou impostos, encargos sociais, trabalhistas, previdenciários, fiscais e comerciais incidentes, taxa de administração, frete, seguro e outros necessários ao cumprimento integral do objeto da contratação.

4. **CLÁUSULA QUARTA – DOTAÇÃO ORÇAMENTÁRIA**

4.1. As despesas decorrentes desta contratação estão programadas em dotação orçamentária própria, prevista no orçamento da União, para o exercício de 2020, na classificação abaixo:

Gestão/Unidade:

Fonte:

Programa de Trabalho:

Elemento de Despesa:

PI :

4.2. No(s) exercício(s) seguinte(s), as despesas correspondentes correrão à conta dos recursos próprios para atender às despesas da mesma natureza, cuja alocação será feita no início de cada exercício financeiro.

5. **CLÁUSULA QUINTA – PAGAMENTO**

5.1. O prazo para pagamento à CONTRATADA e demais condições a ele referentes encontram-se definidos no Termo de Referência e no Anexo XI da IN SEGES/MPDG n. 5/2017.

6. **CLÁUSULA SEXTA - DA LEI ANTICORRUPÇÃO**

6.1. As partes CONTRATANTES/CELEBRANTES DO CONTRATO comprometem-se a observar os preceitos legais instituídos pelo ordenamento jurídico brasileiro no que tange ao combate à corrupção, em especial a Lei nº 12.846, de 1º de Agosto de 2013, e, no que forem aplicáveis, os seguintes tratados internacionais: Convenção sobre o Combate da Corrupção de Funcionários Públicos Estrangeiros em Transações Comerciais Internacionais (Convenção da OCDE) - promulgada pelo Decreto nº 3.678, de 30 de novembro de 2000; a Convenção Interamericana Contra a Corrupção (Convenção da OEA) - promulgada pelo Decreto nº 4.410, de 7 de outubro de 2002; e a Convenção das Nações Unidas Contra a Corrupção (Convenção das Nações Unidas) - promulgada pelo Decreto nº 5.687, de 31 de janeiro de 2006.

6.2. A **CONTRATADA**, declara, por si e por seus administradores, funcionários, representantes e outras pessoas que agem em seu nome, direta ou indiretamente, estar ciente dos dispositivos contidos na Lei nº 12.846/2013; (ii) se obriga a tomar todas as providências para fazer com que seus administradores, funcionários e representantes tomem ciência quanto ao teor da mencionada Lei nº 12.846/2013.

6.3. **PARÁGRAFO PRIMEIRO** – A **CONTRATADA**, no desempenho das atividades objeto deste CONTRATO, compromete-se perante ao **CONTRATANTE** a abster-se de praticar ato(s) que possa(m) constituir violação à legislação aplicável ao presente instrumento pactual, incluindo aqueles descritos na Lei nº 12.846/2013, em especial no seu artigo 5º.

6.4. **PARÁGRAFO SEGUNDO** - Qualquer descumprimento das regras da Lei Anticorrupção e suas regulamentações, por parte da **CONTRATADA**, em qualquer um dos seus aspectos, poderá ensejar:

I - Instauração do Procedimento de Apuração da Responsabilidade Administrativa – PAR, nos termos do Decreto nº 8.420/2015 e Instrução Normativa CGU nº 13/2019, com aplicação das sanções administrativas porventura cabíveis;

II – Ajuizamento de ação com vistas à responsabilização na esfera judicial, nos termos dos artigos 18 e 19 da Lei nº 12.846/2013.

PARÁGRAFO TERCEIRO - A **CONTRATADA** obriga-se a conduzir os seus negócios e práticas comerciais de forma ética e íntegra em conformidade com os preceitos legais vigentes no país.

7. **CLÁUSULA SÉTIMA – REAJUSTAMENTO DE PREÇOS EM SENTIDO AMPLO.**

7.1. Os preços são fixos e irreajustáveis durante a vigência do contrato.

8. **CLÁUSULA OITAVA – GARANTIA DE EXECUÇÃO**

8.1. A CONTRATADA prestará garantia no valor de **R$ xxx** na modalidade a ser escolhida pela mesma, conforme disposto no § 1º do art. 56 da Lei n.º 8.666/93, correspondente a 5% (dois por cento) do valor total do contrato, no prazo de 30 (trinta) dias, cujo período de garantia deverá compreender o prazo de vigência do contrato com validade de 3 (três) meses após o término da vigência contratual, observadas as condições prevista no Termo de Referência.

9. **CLÁUSULA NONA – MODELO DE EXECUÇÃO DOS SERVIÇOS E FISCALIZAÇÃO**

9.1. O modelo de execução dos serviços a serem executados pela CONTRATADA, os materiais que serão empregados, a disciplina do recebimento do objeto e a fiscalização pela CONTRATANTE são aqueles previstos no Termo de Referência, anexo do Edital.

10. **CLÁUSULA DÉCIMA – OBRIGAÇÕES DA CONTRATANTE E DA CONTRATADA**

10.1. As obrigações da CONTRATANTE e da CONTRATADA são aquelas previstas no Termo de Referência, anexo do Edital.

11. **CLÁUSULA DÉCIMA PRIMEIRA - SANÇÕES ADMINISTRATIVAS**

11.1. As sanções relacionadas à execução do contrato são aquelas previstas no Termo de Referência, anexo do Edital.

12. **CLÁUSULA DÉCIMA SEGUNDA – RESCISÃO**

12.1. O presente Contrato poderá ser rescindido:

12.1.1. por ato unilateral e escrito da Administração, nas situações previstas nos incisos I a XII e XVII do art. 78 da Lei nº 8.666, de 1993, e com as consequências indicadas no art. 80 da mesma Lei, sem prejuízo da aplicação das sanções previstas no Termo de Referência, anexo ao Edital;

12.1.2. amigavelmente, nos termos do art. 79, inciso II, da Lei nº 8.666, de 1993.

12.2. Os casos de rescisão contratual serão formalmente motivados, assegurando-se à CONTRATADA o direito à prévia e ampla defesa.

12.3. A CONTRATADA reconhece os direitos da CONTRATANTE em caso de rescisão administrativa prevista no art. 77 da Lei nº 8.666, de 1993.

12.4. O termo de rescisão, sempre que possível, será precedido de Relatório indicativo dos seguintes aspectos, conforme o caso:

12.4.1. Balanço dos eventos contratuais já cumpridos ou parcialmente cumpridos;

12.4.2. Relação dos pagamentos já efetuados e ainda devidos;

12.4.3. Indenizações e multas.

13. **CLÁUSULA DÉCIMA TERCEIRA – VEDAÇÕES E PERMISSÕES**

13.1. É vedado à CONTRATADA interromper a execução dos serviços sob alegação de inadimplemento por parte da CONTRATANTE, salvo nos casos previstos em lei.

13.2. É permitido à CONTRATADA caucionar ou utilizar este Termo de Contrato para qualquer operação financeira, nos termos e de acordo com os procedimentos previstos na Instrução Normativa SEGES/ME nº 53, de 8 de Julho de 2020.

13.2.1. A cessão de crédito, a ser feita mediante celebração de termo aditivo, dependerá de comprovação da regularidade fiscal e trabalhista da cessionária, bem como da certificação de que a cessionária não se encontra impedida de licitar e contratar com o Poder Público, conforme a legislação em vigor, nos termos do Parecer JL-01, de 18 de maio de 2020.

13.2.2. O crédito a ser pago à cessionária é exatamente aquele que seria destinado à cedente (contratada) pela execução do objeto contratual, com o desconto de eventuais multas, glosas e prejuízos causados à Administração, sem prejuízo da utilização de institutos tais como os da conta vinculada e do pagamento direto

previstos na IN SEGES/ME nº 5, de 2017, caso aplicáveis.

14. **CLÁUSULA DÉCIMA QUARTA – ALTERAÇÕES**

14.1. Eventuais alterações contratuais reger-se-ão pela disciplina do art. 65 da Lei nº 8.666, de 1993, bem como do ANEXO X da IN/SEGES/MPDG nº 05, de 2017.

14.2. A CONTRATADA é obrigada a aceitar, nas mesmas condições contratuais, os acréscimos ou supressões que se fizerem necessários, até o limite de 25% (vinte e cinco por cento) do valor inicial atualizado do contrato.

14.3. As supressões resultantes de acordo celebrado entre as partes contratantes poderão exceder o limite de 25% (vinte e cinco por cento) do valor inicial atualizado do contrato.

15. **CLÁUSULA DÉCIMA QUINTA – DOS CASOS OMISSOS**

15.1. Os casos omissos serão decididos pela CONTRATANTE, segundo as disposições contidas na Lei nº 8.666, de 1993, na Lei nº 10.520, de 2002 e demais normas federais aplicáveis e, subsidiariamente, segundo as disposições contidas na Lei nº 8.078, de 1990 - Código de Defesa do Consumidor - e normas e princípios gerais dos contratos.

16. **CLÁUSULA DÉCIMA SEXTA – PUBLICAÇÃO**

16.1. Incumbirá à CONTRATANTE providenciar a publicação deste instrumento, por extrato, no Diário Oficial da União, no prazo previsto na Lei nº 8.666, de 1993.

17. **CLÁUSULA DÉCIMA SETIMA – FORO**

17.1. É eleito o Foro da Seção Judiciária do Distrito Federal - Justiça Federal para dirimir os litígios que decorrerem da execução deste Termo de Contrato que não possam ser compostos pela conciliação, conforme art. 55, §2º da Lei nº 8.666/93.

Para firmeza e validade do pactuado, o presente Termo de Contrato foi lavrado e disponibilizado, eletronicamente, por meio do Sistema Eletrônico de Informações – SEI, assinado pelos contraentes.

LUCIANO BRAGAGNOLO	**REPRESENTANTE**
Subsecretário de Orçamento e Administração	EMPRESA
Contratante	**Contratada**

Documento assinado eletronicamente por **Leandro de Castro Abelha**, **Coordenador(a) Substituto(a)**, em 21/09/2020, às 15:27, conforme o § 1º do art. 6º e art. 10 do Decreto nº 8.539/2015.

A autenticidade deste documento pode ser conferida no site https://sei.mdh.gov.br/autenticidade, informando o código verificador **1338496** e o código CRC **320F8454**.

Referência:

Comissão Permanente de Modelos de Licitações e Contratos da Consultoria-Geral da União

Termo de Contrato - Modelo para SERVIÇOS DE TECNOLOGIA DA INFORMAÇÃO E COMUNICAÇÃO

Atualização: 31/07/2020