PREGÃO ELETRÔNICO

INSTITUTO FEDERAL DO MATO GROSSO DO SUL

PREGÃO ELETRÔNICO Nº 20/2022
(Processo Administrativo n.° 23347.009360.2021-94)

Torna-se público que o(a) INSTITUTO FEDERAL DO MATO GROSSO DO SUL por meio do(a) Diretoria de Compras, Licitações e Contratos, sediado(a) na Rua Jornalista Belizário de Lima, 236 - Vila Gloria -, Campo Grande-MS, realizará licitação, *para registro de preços,* na modalidade PREGÃO, na forma ELETRÔNICA, sob a forma de execução indireta, 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, *do Decreto nº 7.892, de 23 de janeiro de 2013,* 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: 06/09/2022
Horário: 09:00 horas
Local: Portal de Compras do Governo Federal – **https://www.gov.br/compras/pt-br**
Critério de Julgamento: ***menor preço por grupo e item***
Regime de Execução: *Empreitada por Preço Unitário*

1 DO OBJETO

1.1 O objeto da presente licitação é a escolha da proposta mais vantajosa para a *contratação e aquisição* de solução de tecnologia da informação e comunicação de solução de segurança - firewall e backup - incluindo hardware, software, instalação, treinamento, suporte e garantia, pelo período de 60 (sessenta) meses com o objetivo de atender as demandas relacionadas à proteção da rede e dos dados, continuidade dos serviços da TI e recuperação de desastres**,** conforme condições, quantidades e exigências estabelecidas neste Edital e seus anexos.

1.2 *A licitação será dividida em grupo e itens, conforme tabela constante do Termo de Referência, facultando-se ao licitante a participação em quantos grupo/itens forem de seu interesse.*

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

2 *DO REGISTRO DE PREÇOS*

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

3 DO CREDENCIAMENTO

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

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

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

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

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

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

4 DA PARTICIPAÇÃO NO PREGÃO.

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

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

4.1.2 Será concedido tratamento favorecido para as microempresas e empresas de pequeno porte, para as sociedades cooperativas mencionadas no artigo 34 da Lei nº 11.488, de 2007, para o microempreendedor individual - MEI, nos limites previstos da Lei Complementar nº 123, de 2006, bem como para bens e serviços produzidos no país e bens produzidos de acordo com processo produtivo básico, na forma do art. 3º da Lei nº 8.248, de 1991 e art. 8º do Decreto nº 7.174, de 2010.

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 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 sociedades *cooperativas, considerando a vedação contida no art. 10 da Instrução Normativa SEGES/MP nº 5, de 2017.*

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.

c) 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:

4.6.1 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.

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

4.6.1.2 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.

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

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

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

4.6.5 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;

4.6.6 que a proposta foi elaborada de forma independente.

4.6.7 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;

4.6.8 que a solução é fornecida 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.

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

4.6.9.1 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.

4.7. 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 *valor unitário 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 no fornecimento da solução, 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 do quanto demandado e executado, 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.

6.3.3 O produto será entregue pelo preço fechado, não cabendo ao licitante demonstrar com planilha.

6.4 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.

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

6.6 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 fornecer a solução 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.

6.7 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.

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

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

6.9.1 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/grupo.*

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

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

7.8. O intervalo mínimo de diferença de valores ou percentuais entre os lances, que incidirá tanto em relação aos lances intermediários quanto em relação à proposta que cobrir a melhor oferta deverá ser de R$ 5,00 (cinco 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. 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.

7.26. 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.

7.26.1. 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, ao objeto executado:

7.26.1.1. por empresas brasileiras;

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

7.26.1.3. 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.

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

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

7.29. O pregoeiro solicitará ao licitante melhor classificado que, no prazo de 04 (quatro) horas [mínimo de 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.

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

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

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. 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:

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

8.2.2. contenha vício insanável ou ilegalidade;

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

8.2.4. 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.

8.2.4.1. 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:

8.2.4.1.1. 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.

8.3. 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 para que a empresa comprove a exequibilidade da proposta.

8.4. 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, não sendo possível a sua imediata desclassificação, será obrigatória a realização de diligências para aferir a legalidade e exequibilidade da proposta.

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

8.5.1. 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.

8.6. O Pregoeiro poderá convocar o licitante para enviar documento digital complementar, por meio de funcionalidade disponível no sistema, no prazo de 04 (quatro) horas, sob pena de não aceitação da proposta.

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

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

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

8.8. 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;

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

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

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

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

8.13. 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 mantida 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.

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

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

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

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

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

9.3. Havendo a necessidade de envio de documentos de habilitação complementares, necessários à confirmação daqueles exigidos neste Edital e já apresentados, o licitante será

convocado a encaminhá-los, em formato digital, via sistema, no prazo de 04 (quatro) 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 para atestados de capacidade técnica, e no caso daqueles 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 relacionada nos itens a seguir, para fins de habilitação.

9.8. **Habilitação jurídica:**

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

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

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

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

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

9.8.6. Empresas Estrangeiras:

9.8.6.1. As empresas estrangeiras que funcionem no País, autorizadas por decreto do Poder Executivo na forma do inciso V, do art. 28, da Lei nº 8.666, de 1993, devem se cadastrar no SICAF com a identificação do Cadastro Nacional de Pessoas Jurídicas.

9.8.6.2. As empresas estrangeiras que não funcionem no país para participarem de licitações, devem se cadastrar no Sicaf, acessando o sistema por meio do Portal de compras do Governo Federal (Comprasnet) pelo endereço eletrônico https://www.gov.br/compras/pt-br, e se registrar de acordo com o disposto no art. 20-A da Instrução Normativa nº 3, de 26 de abril de 2018, sendo que o registro cadastral compreende os níveis de:

9.8.6.2.1. Credenciamento;

9.8.6.2.2. Habilitação jurídica;

9.8.6.2.3. Regularidade fiscal federal e trabalhista;

9.8.6.2.4. Regularidade fiscal estadual e/ou municipal;

9.8.6.2.5. Qualificação técnica e;

9.8.6.2.6. Qualificação econômico-financeira

9.8.6.3. 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 *estadual* **e** *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 Estadual e 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 *estaduais* ou *municipais* relacionados ao objeto licitatório, deverá comprovar tal condição mediante a apresentação de declaração da Fazenda *Estadual* OU *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.

9.10.3. 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:

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

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

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

9.10.4. As empresas que apresentarem resultado inferior ou igual a 1(um) em qualquer dos índices de Liquidez Geral (LG), Solvência Geral (SG) e Liquidez Corrente (LC), deverão comprovar patrimônio líquido de 5% (cinco 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:

9.11.1.1.1. Devem ser da mesma natureza do objeto da licitação;

9.11.1.1.2. Poderão ser fornecidos por pessoas jurídicas de direito público ou privado, com correta identificação do emissor;

9.11.1.1.3. Devem ser emitidos sem rasuras, acréscimos ou entrelinhas;

9.11.1.1.4. Devem estar assinados por quem tenha competência para expedi-los, tais como representantes legais do órgão/empresa, diretores, gerentes e representantes formais das áreas técnica ou demandante (sem se limitar a esses);

9.11.1.1.5. Devem conter identificação clara e suficiente do Atestante; e

9.11.1.1.6. Devem apresentar redação clara, sucinta e objetiva que demonstre de forma inequívoca o atendimento ao objeto da requisição.

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. Os atestados de capacidade técnica podem ser apresentados em nome da matriz ou da filial da empresa licitante

9.11.4. 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.

9.11.5. Poderá ser admitida, para fins de comprovação de quantitativo mínimo do serviço, a apresentação de diferentes atestados de serviços executados de forma concomitante, pois essa situação se equivale, para fins de comprovação de capacidade técnico-operacional, a uma única contratação, nos termos do item 10.9 do Anexo VII-A da IN SEGES/MPDG n. 5/2017.

9.11.5.1. Deverá haver a comprovação da experiência mínima de 03 (três) anos na prestação dos serviços, sendo aceito o somatório de atestados de períodos diferentes, não havendo obrigatoriedade de os 03 (três) anos serem ininterruptos, conforme item 10.7.1 do Anexo VII-A da IN SEGES/MPDG n. 5/2017.

9.11.6. 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.

9.11.7. No caso de atestados emitidos por empresas privadas, não serão válidos aqueles emitidos por empresas pertencentes ao mesmo grupo empresarial da empresa proponente. São consideradas como pertencentes ao mesmo grupo empresarial as empresas controladas ou controladoras do licitante proponente, ou que tenha pelo menos uma mesma pessoa física ou jurídica que seja sócia ou possua vínculo com a empresa emitente ou empresa 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 da prova de inscrição nos cadastros de contribuintes estadual e municipal.

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 04 (quatro) horas, a contar da solicitação do Pregoeiro no sistema eletrônico e deverá:

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

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

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

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

10.4 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).

10.5 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.

10.6 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.

10.7 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.

10.8 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 Não haverá exigência de garantia de execução para a presente contratação.

15 *DA ATA DE REGISTRO DE PREÇOS*

15.1 *Homologado o resultado da licitação, terá o adjudicatário o prazo de 10 (dez) dias, contados a partir da data de sua convocação, para assinar a Ata de Registro de Preços, cujo prazo de*

validade encontra-se nela fixado, sob pena de decair do direito à contratação, sem prejuízo das sanções previstas neste Edital.

15.2 *Alternativamente à convocação para comparecer perante o órgão ou entidade para a assinatura da Ata de Registro de Preços, a Administração poderá encaminhá-la para assinatura, mediante correspondência postal com aviso de recebimento (AR) ou meio eletrônico, para que seja assinada e devolvida no prazo de 10 (dez) dias, a contar da data de seu recebimento.*

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

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

15.4.1 *Será incluído na ata, sob a forma de anexo, o registro dos licitantes que aceitarem fornecer a solução com preços iguais aos do licitante vencedor na sequência da classificação do certame, quando o objeto não atender aos requisitos previstos no art. 3º da Lei nº 8.666, de 1993;*

16 DO TERMO DE CONTRATO OU INSTRUMENTO EQUIVALENTE

16.1 Após a homologação da licitação, em sendo realizada a contratação, será firmado Termo de Contrato.

16.2 O adjudicatário terá o prazo de 10 (dez) dias úteis, contados a partir da data de sua convocação, para assinar o Termo de Contrato, sob pena de decair do direito à contratação, sem prejuízo das sanções previstas neste Edital.

16.2.1 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), disponibilização de acesso a sistema de processo eletrônico para esse fim ou outro meio eletrônico, para que seja assinado e devolvido no prazo de 10 (dez) dias, a contar da data de seu recebimento ou da disponibilização do acesso ao sistema de processo eletrônico.

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

16.3 O prazo de vigência da contratação é o previsto no instrumento contratual *em conformidade com item 10 do termo de referência.*

16.4 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.

16.4.1 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.

16.4.2 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.

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

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

17 DO REAJUSTAMENTO EM SENTIDO GERAL

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

18 DO MODELO DE GESTÃO DO CONTRATO

18.1 O modelo de gestão do contrato, contemplando os critérios de recebimento e aceitação do objeto, os procedimentos de testes e inspeção e os critérios de fiscalização, com base nos níveis mínimos de serviço/níveis de qualidade definidos, estão previstos no Termo de Referência.

19 DAS OBRIGAÇÕES DA CONTRATANTE E DA CONTRATADA

19.1 As obrigações (deveres e responsabilidades) da Contratante e da Contratada e do órgão gerenciadores da ata de registro de preços são as estabelecidas no Termo de Referência.

20 DO PAGAMENTO

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

20.1.1 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.

21 DAS SANÇÕES ADMINISTRATIVAS.

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

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

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

21.1.3 apresentar documentação falsa;

21.1.4 deixar de entregar os documentos exigidos no certame;

21.1.5 ensejar o retardamento da execução do objeto;

21.1.6 não mantiver a proposta;

21.1.7 cometer fraude fiscal;

21.1.8 comportar-se de modo inidôneo;

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

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

21.4 O licitante/adjudicatário que cometer qualquer das infrações discriminadas nos subitens anteriores ficará sujeito, sem prejuízo da responsabilidade civil e criminal, e quando não houver disposição específica no Termo de Referência, às seguintes sanções:

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

21.4.2 Multa de 5% (cinco por cento) sobre o valor estimado do(s) item(s) prejudicado(s) pela conduta do licitante;

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

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

21.4.4.1 A Sanção de impedimento de licitar e contratar prevista neste subitem também é aplicável em quaisquer das hipóteses previstas como infração administrativa neste Edital.

21.4.5 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;

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

21.6 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.

21.7 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.

21.8 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.

21.9 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.

21.10 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.

21.11 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.

21.12 As penalidades serão obrigatoriamente registradas no SICAF.

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

22 *DA FORMAÇÃO DO CADASTRO DE RESERVA*

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

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

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

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

23 DA IMPUGNAÇÃO AO EDITAL E DO PEDIDO DE ESCLARECIMENTO

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

23.2 A impugnação poderá ser realizada por forma eletrônica, pelo e-mail licit.02@ifms.edu.br, ou por petição dirigida ou protocolada no endereço Rua Jorn. Belizário Lima, 236, Vila Glória – Campo Grande/MS, seção PROAD/DIRLI

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

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

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

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

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

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

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

24 DAS DISPOSIÇÕES GERAIS

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

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

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

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

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

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

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

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

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

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

24.11 O Edital está disponibilizado, na íntegra, no endereço eletrônico https://www.gov.br/compras/pt-br/, e também poderá ser lido e/ou obtido no endereço Rua Jornalista Belizário Lima, 236 - Vila Glória Campo Grande/MS, nos dias úteis, no horário das 08:00 até 12:00 horas às 13:00 até 17:00 horas, mesmo endereço e período no qual os autos do processo administrativo permanecerão com vista franqueada aos interessados.

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

24.12.1 ANEXO I - Termo de Referência:

24.12.1.1 Apêndice A – Especificação técnica.

24.12.1.2 Anexo A - Endereço das unidades.

24.12.1.3 Anexo B – Modelo de Termo De Compromisso De Manutenção Do Sigilo E Segurança Da Informação.

24.12.1.4 Anexo C – Modelo de Termo De Ciência Individual De Sigilo E Segurança Da Informação.

24.12.1.5 Anexo D – Modelo De Ordem De Serviço.

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

24.12.3 ANEXO III – Minuta de Termo de Contrato;

24.12.4 ANEXO IV – Estudo Técnico Preliminar;

24.12.5 ANEXO V - Declaração de Inexistência de Registro de Oportunidade;

Campo Grande/MS , 15 de Agosto de 2022.

Assinatura da autoridade competente

ANEXO I - TERMO DE REFERÊNCIA

Aquisição de Solução de Segurança - Firewall e Backup.

Referência: Arts. 12 a 24 IN SGD/ME Nº 1/2019

1 – OBJETO DA CONTRATAÇÃO

1.1. Registro de preços para aquisição de solução de segurança - *firewall* e *backup* - incluindo *hardware*, *software*, instalação, treinamento, suporte e garantia, pelo período de 60 (sessenta) meses com o objetivo de atender as demandas relacionadas à proteção da rede e dos dados, continuidade dos serviços da TI e recuperação de desastres do Instituto Federal de Mato Grosso do Sul (IFMS), conforme condições, quantidades e exigências estabelecidas neste instrumento.

2 – DESCRIÇÃO DA SOLUÇÃO DE TIC

2.1. A solução de segurança de rede e de dados (Firewall e Backup) foi dividida em dois Grupos, conforme descrito abaixo:
2.1.1. Grupo 1 - Solução de segurança - *Firewall*, composto por:
2.1.1.1. Solução de Firewall em Appliance - Tipo 1 (Palo Alto Networks PA-460) para a Reitoria do IFMS, com garantia e suporte por 60 meses;
2.1.1.2. Solução de Firewall em Appliance - Tipo 2 (Palo Alto Networks PA-440) para os 10 *campi* do IFMS, com garantia e suporte por 60 meses;
2.1.1.3. Renovação de solução de Gerenciamento de Firewall Centralizado (Panorama) para 25 dispositivos, por 60 meses;
2.1.1.4. Serviço de Instalação e Configuração da Solução de Firewall Tipo 1 (item 1) - ONSITE em Campo Grande/MS;
2.1.1.5. Serviço de Projeto, Instalação e Configuração da Solução de Firewall Tipo 2 (item 2) - REMOTO.
2.1.2. Grupo 2 - Solução de segurança - *Backup*, composto por:
2.1.2.1. Solução de *software* de backup com licença perpétua baseada em *socket* com suporte por 60 meses;
2.1.2.2. Servidor de *backup* - *appliance* de *backup* com garantia e suporte por 60 meses para armazenamento das cópias de segurança;
2.1.2.3. Serviço de instalação e configuração da solução de *backup*;
2.1.2.4. Serviço de treinamento oficial do fabricante da solução de *backup*, que visa capacitar a equipe técnica do IFMS na operação e gestão da solução.
2.2. Os requisitos e funcionalidades estão detalhados no **APÊNDICE A - ESPECIFICAÇÃO TÉCNICA**.

2.3 Bens e serviços que compõem a solução

2.3.1. O objeto desta contratação, a solução de segurança de rede e de dados, configura-se como única solução de TIC, na forma do inciso I do art. 3º da Instrução Normativa n.º 1, de 4 de abril de 2019. Sendo composta pelos itens e serviços relacionados na tabela abaixo:

Grupo	Item	Descrição do Bem ou Serviço	Código CATMAT/ CATSER	Quantidade	Métrica ou Unidade
1	1	Solução de Firewall em Appliance - Tipo 1 (Palo Alto Networks PA-460)	150100	7	Unidade
	2	Solução de Firewall em Appliance - Tipo 2 (Palo Alto Networks PA-440)	150100	37	Unidade
	3	Renovação de solução de Gerenciamento de Firewall Centralizado (Panorama) para 25 dispositivos	27014	2	Unidade
	4	Serviço de Instalação e Configuração da Solução de Firewall Tipo 1 (item 1) - ONSITE em Campo Grande/MS	26972	5	Unidade
	5	Serviço de Projeto, Instalação e Configuração da Solução de Firewall Tipo 2 (item 2) - REMOTO	26972	38	Unidade
2	6	Software de backup com licenciamento por socket, conforme descrito na especificação técnica	27464	24	Licença por Socket
	7	Servidor de Backup	457720	2	Unidade
	8	Serviço de Instalação e Configuração da Solução de Backup	26972	1	Unidade
	9	Serviço de Treinamento Oficial do Fabricante da Solução de Backup	3840	4	Unidade

2.3.2. Os itens 3 e 6 se enquadram no conceito de Licenciamento de Software (ANEXO I da IN SGD/ME nº 01/2019);

2.3.3. A administração atendeu às normas específicas dispostas nos anexos, guias, manuais e modelos publicados pelo Órgão Central do SISP, conforme disposto no art. 8º, § 2, da IN SGD/ME nº 01/2019.

2.4 Especificação técnica dos itens que compõem a solução

2.5.1. As especificações técnicas dos itens que compõem a solução encontram-se detalhadas no **APÊNDICE A - ESPECIFICAÇÃO TÉCNICA**.

3 – JUSTIFICATIVA PARA A CONTRATAÇÃO

3.1. Contextualização e Justificativa da Contratação

3.1.1. O IFMS disponibiliza uma infraestrutura de TI para atender cerca de 25.000 (vinte e cinco mil) usuários da comunidade acadêmica, sendo composta por estudantes, docentes e técnicos administrativos. A equipe que cuida da segurança da informação na Reitoria, parte da Coordenação de Infraestrutura, Redes e Telecomunicações, é composta por um analista e quatro técnicos que são responsáveis por planejar, executar e manter políticas e medidas que garantam a segurança e a proteção da rede e dos sistemas computacionais do IFMS.
3.1.2. Além disso, nos *Campi* atuam um analista e pelo menos um técnico, que dão apoio a Reitoria e implementam soluções locais. Dessa forma, essa equipe atua diretamente na implementação e manutenção dos sistemas de proteção, como por exemplo, o firewall.
3.1.3. No momento, o IFMS conta com uma solução de *firewall* de próxima geração (Next Generation Firewall – NGFW), solução paga, da marca Palo Alto, adquirida no último processo de aquisição de equipamentos para segurança de rede (SRP 18/2014). Nesse período, foi feita uma tentativa de renovação das garantias dos equipamentos, que não foi possível devido à restrição orçamentária do IFMS à época.
3.1.4. A proteção da rede implementada é uma solução completa, porém está desatualizada. Devido ao vencimento da garantia não foi mais possível fazer as atualizações de software nos equipamentos, além disso, o hardware dos equipamentos de TIC são atualizados muito rapidamente, de modo a acompanhar a evolução dos softwares em geral. Com equipamentos de firewall não é diferente e esse tipo de solução necessita estar sempre atualizada por conta do constante surgimento de ameaças tecnológicas.
3.1.5. Alguns equipamentos apresentaram problemas físicos e não estão funcionando ou estão com o funcionamento comprometido, o que deixa a rede do IFMS em vulnerabilidade, já que as soluções alternativas (gratuitas) não atendem a todas as necessidades de proteção demandadas pela instituição.
3.1.6. Outro ponto importante a ser considerado é o backup, esse recurso de segurança de dados é fundamental para a manutenção das atividades da instituição. Os órgãos públicos vêm sofrendo uma crescente quantidade de ataques cibernéticos, essas ações, em grande parte, visam destruir as informações e inviabilizar o acesso aos sistemas da instituição alvo. Estar preparado para evitar essas invasões é muito importante, mas ser capaz de se recuperar de um evento que não foi possível evitar é fundamental. Nesse sentido, as cópias de segurança devem ter especial atenção na segurança de TIC de uma instituição.
3.1.7. O backup é o armazenamento seguro de cópias dos dados institucionais, esses dados podem ser informações de pessoas, sistemas e ações e a forma eficiente de fazer esses backups vai muito além de copiar os dados e dispor em outro local de armazenamento. É necessário criar rotinas de backup, automatizar ações, verificar e testar as cópias, utilizar recursos de compressão para poupar espaço de armazenamento, entre outros procedimentos.
3.1.8. Todas essas ações são muito complexas para serem realizadas manualmente e sem conhecimento profundo das tecnologias atuais, ainda mais considerando o tamanho atual da equipe técnica de TIC da instituição. Dessa forma, faz-se necessária a aquisição de soluções especializadas e atualizadas, com equipamento e softwares modernos, juntamente com

suporte, manutenção e a capacitação, com o objetivo de garantir o atendimento à demanda de segurança institucional e da sua comunidade.

3.2. Alinhamento aos Instrumentos de Planejamento Institucionais

Alinhamento ao PDI 2019-2023	
ID	**Objetivos Estratégicos**
4.3	Propiciar a infraestrutura física e tecnológica adequadas para atividades acadêmicas, administrativas e culturais.

Estratégia de Governo Digital 2020-2022	
OE	**Descrição**
16	Otimização das infraestruturas de tecnologia da informação

Alinhamento ao PDTIC 2021-2023			
ID	**Necessidade do PDTIC**		
N01	Dotar a área de TI de infraestrutura adequada		
ID	**Ação do PDTIC**	**ID**	**Meta do PDTIC associada**

A002	Adquirir e atualizar ativos de hardware e/ou instalações (obras) necessárias.	**M01**	Manter atualizado o parque de equipamentos e softwares de tecnologia da informação do IFMS.
A003	Adquirir/Contratar/Atualizar softwares ou licenças de softwares para área administrativa e acadêmica.		

Alinhamento ao PAC 2022	
Item	**Descrição**
761	Solução perpétua de Software de backup/recovery para Máquinas Virtuais com Suporte técnico e direito de atualização por 60 meses.
762	Suporte técnico e direito de atualização de Software de backup/recovery para Máquinas Virtuais por 48 meses.
763	Solução de firewall para a Reitoria
764	Solução de firewall para os *Campi*
765	Solução de gerenciamento de firewall centralizado

3.3. Estimativa da demanda

As estimativas aqui especificadas contemplam os Órgãos Gerenciador e Participantes:

Grupo	Item	Descrição do Bem ou Serviço	Quantidade
1	1	Solução de Firewall em Appliance - Tipo 1 (Palo Alto Networks PA-460)	7
	2	Solução de Firewall em Appliance - Tipo 2 (Palo Alto Networks PA-440)	37

	3	Renovação de solução de Gerenciamento de Firewall Centralizado (Panorama) para 25 dispositivos	2
	4	Serviço de Instalação e Configuração da Solução de Firewall Tipo 1 (item 1) - ONSITE em Campo Grande/MS	5
	5	Serviço de Projeto, Instalação e Configuração da Solução de Firewall Tipo 2 (item 2) - REMOTO	38
2	6	Software de backup com licenciamento por socket, conforme descrito na especificação técnica	24
	7	Servidor de Backup	2
	8	Serviço de Instalação e Configuração da Solução de Backup	1
	9	Serviço de Treinamento Oficial do Fabricante da Solução de Backup	4

3.4. Parcelamento da Solução de TIC

3.4.1. A solução proposta neste documento foi dividida em dois grupos compostos por itens de natureza similar e que se complementam para atender o objetivo dessa aquisição. Os equipamentos, as licenças, os serviços e até o treinamento de cada grupo interagem entre si, de maneira que um componente interfere no funcionamento correto do outro componente, dessa forma o parcelamento dos itens pode ser prejudicial e até mesmo inviabilizar a implementação da solução.
3.4.2. Esta condição de agrupamento visa eliminar possíveis falhas surgidas após a implantação do projeto. Habitualmente, observa-se que após a solução instalada, em contratações desmembradas com este escopo de fornecimento por itens, caso ocorra alguma indisponibilidade ou mau funcionamento de um elemento do sistema, os diferentes fornecedores passam a debater quanto à responsabilidade pela solução, seja pela falta de diagnóstico preciso em termos de “causa da falha”, seja por alegações quanto à competência contratual em intervenções nos produtos de diferentes fornecedores que integram a solução. Por outro lado, o fornecedor único por lote, é responsável pela integração de todos os componentes e pela manutenção da estabilidade e operacionalidade de todo o lote. A Administração ganha em capacidade de gestão do contrato, com instrumentos de cobrança efetiva e fiscalização dos contratos e procedimento padronizado de suporte técnico durante o período de garantia, propiciando agilidade na resolução dos problemas advindos de falhas das soluções ou outros eventos relacionados ao contrato de fornecimento e prestação de serviço.
3.4.3. O agrupamento e adjudicação em Grupo é lícito, “desde que os lotes sejam integrados por itens de uma mesma natureza e que guardem relação entre si" (Acórdão TCU 5.260/2011-1ª Câmara). Também nessa linha, é certo que, conforme disserta o Acórdão TCU n° 861/2013, o “aumento da eficiência administrativa do setor público passa pela otimização do gerenciamento de seus contratos de fornecimento. Essa eficiência administrativa também é de estatura constitucional e deve ser buscada pela administração pública”.

3.4.4. É vedada a aquisição individual de itens registrados para os quais a licitante vencedora não apresentar o menor preço, conforme dispõe os Acórdãos 588/2016 e 343/2014, do Plenário, reiterados pelo Acórdão nº 17180/2021 da 1ª Câmara.
3.4.5. Portanto, a estruturação proposta agrupa de forma segura (técnica e economicamente viável) serviços de uma mesma natureza, que guardam correlação entre si, seja por similaridade técnica ou de tecnologia, bem como de aplicabilidade em busca de uma única solução, sem causar qualquer prejuízo à ampla competitividade. Portanto, pelos motivos elencados, se faz necessário o agrupamento dos itens.

3.5. Resultados e Benefícios a Serem Alcançados

3.5.1. Proteger a rede do IFMS e garantir a confidencialidade, integridade e disponibilidade dos dados e informações, gerenciando os riscos e ameaças que possam interferir na infraestrutura da rede.
3.5.2. Proporcionar a continuidade dos serviços do IFMS através da manutenção de cópias de segurança, permitindo a restauração de dados e serviços em caso de perdas e desastres tecnológicos.

4 – ESPECIFICAÇÃO DOS REQUISITOS DA CONTRATAÇÃO

4.1. Requisitos de Negócio

4.1.1. A presente contratação orienta-se pelos seguintes requisitos de negócio:
4.1.1.1. Atender as demandas registradas no PAC 2022 da Diretoria de Gestão de Tecnologia da Informação, juntamente aos demais dez *Campi* do IFMS;
4.1.1.2. Prover recursos computacionais necessários ao perfeito desenvolvimento das atividades laborais dos setores envolvidos. Tratam-se de recursos de hardware que forneçam apoio à execução de tarefas como: controle e registro de acesso a internet, filtro de conteúdo, configuração de rede virtual privada (VPN), automatização das rotinas de backup, cópia e armazenamentos das principais informações da Instituição;
4.1.1.3. Padronizar as especificações e configurações dos equipamentos de firewall das unidades do IFMS, que decidiram pela aquisição desses objetos, após o devido estudo técnico preliminar;
4.1.1.4. Assegurar que os equipamentos tenham garantia e suporte ao longo de sua vida útil.

4.2. Requisitos de Capacitação

4.2.1. A CONTRATADA deve repassar qualquer conhecimento relacionado às tecnologias utilizadas na prestação de serviços necessários para a continuidade dos serviços pelo órgão ou empresa por esta designada.
4.2.2. O repasse de conhecimento visa a realização da transferência de tecnologia e deve ser executada por profissional com experiência.
4.2.3. Para a solução de backup será necessário capacitação, pois a equipe de TI do IFMS não possui conhecimento da tecnologia e pode ter dificuldades para operacionalizar as ferramentas. Por isso, faz parte da aquisição treinamento específico que deverá ser

conduzido pelo próprio fabricante ou por um parceiro nacional, capacitado, certificado e autorizado pelo fabricante a ministrar treinamentos oficiais.
4.2.4. O treinamento poderá ser ministrado *in loco* ou remotamente.

4.3. Requisitos Legais

4.3.1. O presente processo de contratação deve estar aderente à Constituição Federal, ao Decreto-Lei nº 200/1967, à Lei nº 8.666/93, (Lei de Licitações), à Lei nº10.520/01, (Lei do Pregão), ao Decreto nº 10.024/2019 (Pregão Eletrônico), ao Decreto nº 7.892/2013 (Registro de Preços), à IN SGD/ME nº 01/2019 (Contratação de Soluções de TIC) e a outras legislações aplicáveis.
4.3.2. Os bens e serviços que constituem o objeto deste Termo de Referência enquadram-se no conceito de comuns, nos termos da Lei nº 10.520/2022, em que os requisitos técnicos são suficientes para determinar o conjunto da solução escolhida, constatando-se, ainda, que a solução é fornecida por mais de uma empresa no mercado.
4.3.3. Os bens e serviços que constituem o objeto deste Termo de Referência não incide nas hipóteses vedadas pelos artigos 3º e 4º da IN SGD/ME nº 01/2019.
4.3.4. O presente Termo de Referência, ainda, foi elaborado, respeitando as vedações constantes no artigo 5º da IN SGD/ME nº 01/2019, bem como atendido ao disposto no artigo 8º, §2, da IN SGD/ME nº 01/2019.

4.4. Requisitos de Manutenção

4.4.1. Os itens adquiridos nesse processo deverão possuir garantia do fabricante, ou autorizada no Brasil, com validade mínima de 60 (sessenta) meses, contados a partir do recebimento da solução.
4.4.2. Especificações para manutenção preventiva:
4.4.2.1. Durante o prazo de garantia, deverá ser possível realizar a atualização de sistema operacional dos equipamentos para obter novas funcionalidades e correções.
4.4.2.2. Durante o prazo de garantia, deverá ser possível realizar a atualização das assinaturas de proteção da solução.
4.4.2.3. A CONTRATADA deverá disponibilizar, na vigência da garantia, todas as atualizações dos softwares e *firmwares* dos equipamentos, concebidas em data posterior ao seu fornecimento, pelo período especificado no Termo de Referência, sem qualquer ônus adicional para a CONTRATANTE;
4.4.2.4. As atualizações incluídas devem ser do tipo "*minor release*" e "*major release*", permitindo manter os equipamentos atualizados em sua última versão de software/firmware;
4.4.2.5. A implementação de novas versões de softwares deverá ser realizada de tal forma que as interrupções no ambiente de produção sejam as mínimas possíveis e estritamente necessárias, e, ainda, não causem transtornos aos usuários finais do órgão.
4.4.3. Especificações para suporte e comunicação:
4.4.3.1. Durante o prazo de garantia, os chamados poderão ser abertos diretamente com a CONTRATADA ou autorizada oficial do fabricante através de ligação telefônica (preferencialmente em português), website ou e-mail. O suporte deverá estar disponível na modalidade de 24x7 (24 horas por dia, 7 dias por semana).

4.4.3.2. Poderão ser realizadas consultas técnicas ou questionamentos da equipe técnica da CONTRATANTE para sanar dúvidas, repassar conhecimentos, ou ainda obter melhores práticas. Estas consultas deverão ser realizadas através de e-mail, chat, ou outro meio acordado com a CONTRATANTE.
4.4.3.3. Todas as solicitações feitas pela CONTRATANTE deverão ser registradas pela CONTRATADA em sistema informatizado para acompanhamento e controle da execução dos serviços.
4.4.3.4 O acompanhamento da prestação de serviço deverá ser por meio de um número de protocolo fornecido pela CONTRATADA, no momento da abertura da solicitação.

4.5. Requisitos Temporais

4.5.1. A entrega dos equipamentos deverá ser efetivada no prazo máximo de 45 dias corridos a contar do recebimento da Ordem de Fornecimento de Bens (OFB), emitida pela CONTRATANTE, podendo ser prorrogada, excepcionalmente, por até igual período, desde que justificado previamente pela CONTRATADA e autorizado pela CONTRATANTE;
4.5.2. O suporte técnico e direito de atualização dos softwares deverão ser de no mínimo 60 (sessenta) meses, contados a partir da data de recebimento do equipamento ou da ativação da licença;
4.5.3. A entrega deve ser agendada com antecedência mínima de 24 horas, sob o risco de não ser autorizada.

4.6. Requisitos de Segurança e Privacidade

4.6.1. A CONTRATADA deverá obedecer aos procedimentos operacionais adotados pela CONTRATANTE, no tocante à segurança da informação;
4.6.2. Os serviços contratados deverão ser prestados em conformidade com leis, normas e diretrizes vigentes no âmbito da Administração Pública Federal relacionadas à Segurança da Informação e Comunicações (SIC), em especial atenção à Lei de Geral de Proteção de Dados nº 13.709 de 14 de agosto de 2018, ao Decreto Federal nº 9.637, de 26 de dezembro de 2018, à Instrução Normativa GSI/PR nº 01, de 13 de junho de 2008 (e suas normas complementares) e à Política de Segurança da Informação e Comunicação do IFMS.
4.6.3. Manter sigilo, sob pena de responsabilidades civis, penais e administrativas, sobre todo e qualquer assunto de interesse da CONTRATANTE ou de terceiros, de que tomar conhecimento, em razão da execução do objeto do futuro Contrato, devendo orientar seus empregados nesse sentido também - conforme termo de compromisso e termo de ciência, previstos no art. 18° da IN SGD/ME nº 01 de 2019.
4.6.4. Os conhecimentos, dados e informações de propriedade do IFMS repassados à CONTRATADA por força do objeto do contrato, constituem informação privilegiada e possuem caráter de confidencialidade.
4.6.5. A CONTRATADA deverá comunicar à CONTRATANTE qualquer ocorrência de transferência, remanejamento ou demissão de funcionário, para que seja providenciada a revogação de todos os privilégios de acessos aos sistemas, informações e recursos da CONTRATANTE, porventura colocados à disposição para realização dos serviços contratados.

4.6.6. Promover o afastamento em relação ao objeto da contratação, no prazo máximo de 24 (vinte e quatro) horas após o recebimento da notificação, de qualquer dos seus recursos técnicos que não correspondam aos critérios de confiança ou que perturbe a ação da equipe de fiscalização da CONTRATANTE.

4.7. Requisitos Sociais, Ambientais e Culturais

4.7.1. Os equipamentos devem estar aderentes à Lei nº 12.305, de 2 de agosto de 2010, que institui a Política Nacional de Resíduos Sólidos.
4.7.2. No que couber, visando a atender ao disposto na legislação aplicável – em destaque às Instruções Normativas nº 05/2017/SEGES e nº 01/2019/SGD – a CONTRATADA deverá priorizar, para o fornecimento do objeto, a utilização de bens que sejam no todo ou em parte compostos por materiais recicláveis, atóxicos e biodegradáveis.

4.8. Requisitos de Arquitetura Tecnológica

4.8.1. Na ocorrência de atualização dos softwares, estes deverão estar em sua versão estável mais atual do produto, não serão aceitos produtos obsoletos ou fora de linha de produção do Fabricante.
4.8.2. Além dos requisitos expostos acima, outros, de forma mais detalhada, encontram-se apresentados no **APÊNDICE A – ESPECIFICAÇÃO TÉCNICA** deste Termo de Referência.

4.9. Requisitos de Projeto e de Implementação

4.9.1. A implantação da solução deverá ser realizada por profissionais especializados da contratada, que possuam certificação do fabricante da solução adquirida, ou pelo próprio fabricante.
4.9.2. A implantação da solução deverá ocorrer com participação direta dos técnicos do IFMS que atuarão na solução.
4.9.3. A implantação deverá abranger:
4.9.3.1. Integração da solução com a infraestrutura atual do IFMS;
4.9.3.2. Migração das regras de firewall existentes;
4.9.3.3. Configuração das funcionalidades suportadas pela solução e descritas no presente Termo de Referência;
4.9.3.4. Demais requisitos apresentados no item 4.8 no referente ao serviço de instalação da solução de firewall e de backup.
4.9.4. As informações referentes à implantação deverão estar presentes no projeto de instalação.
4.9.5. A Contratada deverá fornecer documentação completa da solução, incluindo especificação do equipamento, características, funcionalidades, comentários e configurações executadas.
4.9.6. O processo de implantação deverá ser devidamente documentado pela Contratada, que deverá apresentar relatório com o detalhamento do processo realizado ao final da implantação como requisito para o aceite definitivo.
4.9.7. A instalação/configuração deverá ser realizada de tal forma que as interrupções no ambiente de produção do IFMS sejam as mínimas possíveis e estritamente necessárias.

4.9.7.1. Os serviços que eventualmente acarretem risco para os sistemas em produção ou requeiram parada de serviços e/ou equipamentos somente poderão ser executados fora de expediente, em horários previamente acordados com a CONTRATANTE.
4.9.8. A CONTRATADA deverá efetuar a instalação/configuração dos softwares para a última versão homologada pelo fabricante, atendendo integralmente às características e às necessidades da CONTRATANTE e responsabilizando-se por todas as conexões, materiais, acessórios e mão de obra necessária para sua operacionalização.

4.10. Requisitos de Implantação

4.10.1. O processo de entrega dos equipamentos deverá ser realizado pela CONTRATADA sob a supervisão do preposto, que dará conhecimento do andamento do fornecimento aos diversos locais ao gestor do contrato.
4.10.2. A CONTRATADA deverá apresentar as declarações/certificados do FABRICANTE, comprovando que o produto possui a garantia solicitada neste termo de referência.
4.10.3. O Termo de Recebimento Definitivo só será emitido após finalização dos testes do ambiente tecnológico do IFMS.
4.10.4. A implantação deverá abranger:
4.10.4.1. Integração da solução com a infraestrutura atual do IFMS;
4.10.4.2. Migração das regras de *firewall* e backups existentes;
4.10.4.3. Configuração das funcionalidades suportadas pela solução e descritas no presente Termo de Referência;
4.10.4.4. Demais requisitos apresentados no item 4.8 referentes aos serviços de instalação e configuração.
4.10.5. A instalação/configuração deverá ser realizada de tal forma que as interrupções no ambiente de produção do IFMS sejam as mínimas possíveis e estritamente necessárias.

4.11. Requisitos de Garantia

4.11.1. Os equipamentos fornecidos deverão estar cobertos por garantia do fabricante no Brasil pelo período especificado em cada item, conforme APÊNDICE A;
4.11.2. A garantia deve incluir substituição de peças decorrente de vícios de projeto, fabricação, construção e montagem, pelo período especificado no termo de referência, a contar da data de aceite provisório dos equipamentos;
4.11.3. Os softwares fornecidos deverão estar cobertos por garantia que ofereça atualizações necessárias para a correção de vícios, pelo período especificado neste Termo de Referência;
4.11.4. A garantia deve incluir também envio de peças/equipamentos de reposição, que deverão ser entregues nos locais especificados neste Termo de Referência, ou na sua ausência, na sede da contratante, abrangendo-se todos os custos de deslocamento (envio e retorno) das peças/equipamentos de substituição. Obrigatoriamente o envio de peças/equipamentos de reposição deve ser realizado pelo fabricante dos equipamentos, sendo este responsável pelo controle e logística de peças de reposição;
4.11.5. Devem ser descritos, no momento da proposta, qual o tipo de garantia fornecida. Os equipamentos devem ter seus números seriais atrelados ao sistema de suporte do fabricante dos equipamentos com data específica de início e fim do suporte.

4.11.6. O serviço de assistência técnica em GARANTIA deve cobrir todos os procedimentos técnicos destinados ao reparo de eventuais falhas apresentadas nos equipamentos, de modo a restabelecer seu normal estado de uso e dentre os quais se incluem a substituição de peças de hardware, ajustes e reparos técnicos em conformidade com manuais e normas técnicas especificadas pelo FABRICANTE ou a troca técnica (substituição) de equipamento avariado por outro novo (sem uso), no mesmo modelo e padrão apresentado na PROPOSTA ou superior.
4.11.7. O acionamento do serviço de assistência técnica em GARANTIA deverá estar disponível preferencialmente através de central telefônica ou diretamente via website, para operacionalização da abertura de chamados e fornecimento de número de protocolo a fim de realizar o acompanhamento e monitoramento das solicitações.
4.11.8. O FABRICANTE deverá possuir site na internet com a disponibilização de manuais, drivers, firmwares e todas as atualizações existentes relativas ao equipamento ofertado. Durante toda vigência do CONTRATO e da GARANTIA, deverá ser mantida base de conhecimento de problemas, bem como o histórico dos reparos ou substituições para os equipamentos fornecidos.
4.11.9. Sempre que solicitado pelo CONTRATANTE, a CONTRATADA deverá emitir relatório(s), preferencialmente em formato digital, com informações analíticas e sintéticas dos chamados técnicos abertos e atendimentos realizados no período estipulado na solicitação, contendo informações de todas as intervenções realizadas com os registros completos das ocorrências, incluindo, no mínimo, informações do chamado como: identificação do órgão, nome do solicitante, data, hora, modelo do equipamento, falha relatada, problema identificado pelo fabricante, ação corretiva realizada e data de fechamento do chamado com equipamento prontamente restabelecido.
4.11.10. O serviço de assistência técnica pode ser realizado mediante aplicação de ferramentas de diagnóstico remoto, não podendo a CONTRATADA se eximir de prestar o suporte diante da impossibilidade técnica e/ou incompatibilidade de eventuais acessos remotos em virtude de restrições tecnológicas do ambiente do CONTRATANTE.
4.11.11. A movimentação dos equipamentos entre localidades NÃO exclui a garantia.
4.11.12. A garantia não será afetada caso a CONTRATANTE necessite instalar placas de rede locais, interfaces específicas para acionamento de outros equipamentos, adicionar unidade de disco rígido bem como alterar a capacidade de memória, ressaltando que a garantia desses opcionais adicionados será de total responsabilidade da CONTRATANTE.

4.12. Requisitos de Experiência Profissional

4.12.1. A CONTRATADA deverá dimensionar adequadamente a sua equipe de profissionais de forma a atingir os níveis de serviço estabelecidos neste Termo de Referência.
4.11.2. Os profissionais que atuaram na execução dos serviços de implantação da solução deverão possuir qualificação plena e conhecimento técnico compatível com a complexidade das demandas a serem atendidas, conforme **APÊNDICE A – ESPECIFICAÇÃO TÉCNICA** deste Termo de Referência.
4.11.3. A formação da equipe de profissionais é de exclusiva responsabilidade da CONTRATADA e serão gerenciados exclusivamente pelo preposto da empresa.

4.11.4. A prestação de serviços dessa contratação não gera vínculo empregatício entre os empregados da contratada e o IFMS, vedando-se qualquer relação entre estes que caracterize pessoalidade e subordinação.

4.13. Requisitos de Formação da Equipe

4.13.1. A CONTRATADA deverá apresentar um representante legal para atuar como preposto do contrato.
4.13.2. A CONTRATADA deverá encaminhar expediente ao IFMS, informando os nomes dos técnicos que estão autorizados a executar as atividades contratadas.
4.13.3. Deve ser executado por profissional(ais) com as seguintes qualificações:

PERFIL - PREPOSTO	
Responsável por representar a empresa sempre que for necessário, devendo este possuir a seguinte qualificação:	
Experiência/Qualificação	**Modo de Comprovação**
Em atividades de gestão de contratos ou de recursos humanos.	Registro em Carteira de Trabalho ou contrato(s) executado(s) pelo funcionário.
Formação	**Modo de Comprovação**
Nível Superior completo na área de Tecnologia da Informação, Recursos Humanos, Administração de Empresas ou outro curso superior com especialização mínima de 360h (trezentas e sessenta horas) em Tecnologia da Informação.	Diploma ou Certificado de conclusão de curso de graduação deverá ser, devidamente registrado e fornecido por instituição de ensino superior reconhecida pelo Ministério da Educação – MEC.

4.14. Requisitos de Metodologia de Trabalho

4.14.1. O fornecimento dos equipamentos está condicionado ao recebimento pela CONTRATADA da OFB emitida pela CONTRATANTE.
4.14.2. A OFB indicará o tipo de equipamento, a quantidade e a localidade na qual os equipamentos deverão ser entregues.
4.14.3. A CONTRATADA deve prestar serviço de assistência técnica para os equipamentos objeto desta contratação no local original de fornecimento do equipamento constante da OFB, conforme condições previstas na sessão específica de assistência técnica deste Termo de Referência.
4.14.4. O andamento do fornecimento dos equipamentos deve ser acompanhado pela CONTRATADA, que dará ciência de eventuais acontecimentos à CONTRATANTE.

4.15. Requisitos de Segurança da Informação

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

4.15.2. A solução CONTRATADA deverá observar a Norma Brasileira ABNT NBR ISO/IEC 27002.
4.15.3. A CONTRATADA deverá manter a integridade da rede de dados e das informações do IFMS durante a prestação dos serviços.
4.15.4. A CONTRATADA deverá respeitar a Política de Segurança da Informação e Comunicação do IFMS, bem como demais políticas e normas internas que poderão ser instituídas durante a vigência do contrato.
4.15.5. A CONTRATADA deverá guardar sigilo absoluto sobre quaisquer dados e informações contidos em quaisquer documentos e mídias, incluindo os equipamentos e seus meios de armazenamento, de que venha a ter conhecimento durante a execução dos serviços, não podendo, sob qualquer pretexto, divulgar, reproduzir ou utilizar, sob pena de lei, independentemente da classificação de sigilo conferida pelo CONTRATANTE a tais documentos.
4.15.6. O Termo de Compromisso, contendo declaração de manutenção de sigilo e respeito às normas de segurança vigentes na entidade, deverá ser assinado por um representante da CONTRATADA e encontra-se no **ANEXO B**. A CONTRATADA deverá providenciar a assinatura do Termo de Ciência, disponível no **ANEXO C**, por todos os seus colaboradores que estejam relacionados com a execução do projeto. O Termo de Compromisso e o Termo de Ciência deverão ser entregues assinados durante a reunião inicial.
4.15.7. Qualquer unidade de armazenamento, tais como SSDs, HDDs e memórias, utilizadas deverão permanecer em posse da CONTRATANTE mesmo após o uso, após dano à unidade ou após o término do contrato. Caso seja necessária a remoção de alguma unidade de armazenamento, esta ação deverá ser realizada no prédio do IFMS (reitoria ou campus) e imediatamente entregue à CONTRATANTE.
4.15.8. Caso haja necessidade de manutenção fora das dependências do IFMS as unidades de armazenamento deverão ser removidas dentro das dependências do IFMS e deverão ficar sob responsabilidade da CONTRATANTE enquanto perdurar o conserto.

4.16. Outros Requisitos Aplicáveis

4.16.1. Nos termos do Capítulo IV (arts. 41 e 42) do Decreto n° 8.420, de 18 de março de 2015, é fortemente recomendável que a CONTRATADA possua ou desenvolva PROGRAMA DE INTEGRIDADE, que consiste num conjunto de “mecanismos e procedimentos internos de integridade, auditoria e incentivo à denúncia de irregularidades e na aplicação efetiva de códigos de ética e de conduta, políticas e diretrizes com objetivo de detectar e sanar desvios, fraudes, irregularidades e atos ilícitos praticados contra a administração pública, nacional ou estrangeira”.

5 – RESPONSABILIDADES

5.1. Deveres e responsabilidades da CONTRATANTE

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

5.1.2. Encaminhar formalmente a demanda por meio de Ordem de Serviço ou de Fornecimento de Bens, de acordo com os critérios estabelecidos no Termo de Referência ou Projeto Básico;
5.1.3. Receber o objeto fornecido pela CONTRATADA que esteja em conformidade com a proposta aceita, conforme inspeções realizadas;
5.1.4. Aplicar à CONTRATADA as sanções administrativas regulamentares e contratuais cabíveis, comunicando ao órgão gerenciador da Ata de Registro de Preços, quando aplicável;
5.1.5. Liquidar o empenho e efetuar o pagamento à CONTRATADA, dentro dos prazos preestabelecidos em contrato;
5.1.6. Comunicar à CONTRATADA todas e quaisquer ocorrências relacionadas com o fornecimento da solução de TIC;
5.1.7. Definir produtividade ou capacidade mínima de fornecimento da solução de TIC por parte da CONTRATADA, com base em pesquisas de mercado, quando aplicável; e
5.1.8. Prever que os direitos de propriedade intelectual e direitos autorais da solução de TIC sobre os diversos artefatos e produtos produzidos em decorrência da relação contratual, incluindo a documentação, o código-fonte de aplicações, os modelos de dados e as bases de dados, pertençam à Administração;
5.1.9. Exigir o cumprimento de todas as obrigações assumidas pela CONTRATADA, de acordo com as cláusulas contratuais e os termos de sua proposta.
5.1.10. Exercer o acompanhamento e a fiscalização dos serviços, por servidor especialmente designado para esse fim, independentemente do acompanhamento e controle exercido pela CONTRATADA, o que inclui:
5.1.10.1. Receber os objetos no prazo e condições estabelecidas no Edital e seus anexos.
5.1.10.2. Verificar minuciosamente, no prazo fixado, a conformidade dos bens recebidos provisoriamente com as especificações constantes do Edital e da proposta, para fins de aceitação e recebimento definitivo.
5.1.10.3. Comunicar à CONTRATADA, por escrito, sobre imperfeições, falhas ou irregularidades verificadas no objeto fornecido, para que seja substituído, reparado ou corrigido.
5.1.10.4. Notificar à CONTRATADA, por escrito, da ocorrência de eventuais imperfeições no curso da execução dos serviços, fixando prazo para a sua correção, caso já não haja prazo estabelecido por este documento.
5.1.11. Efetuar o pagamento à CONTRATADA no valor correspondente ao fornecimento do objeto, no prazo e forma estabelecidos no Edital e seus anexos.
5.1.12. Efetuar as retenções tributárias devidas sobre o valor da Nota Fiscal/Fatura fornecida pela CONTRATADA, no que couber, em conformidade com o item 6 do Anexo XI da IN SEGES/MP n. 5/2017 e com o art. 36, §8º da IN SLTI/MPOG N. 02/2008.
5.1.13. 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.
5.1.14. Não praticar atos de ingerência na administração da CONTRATADA, tais como:
5.1.14.1. 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.

5.1.14.2. Direcionar a contratação de pessoas para trabalhar nas empresas CONTRATADAS.
5.1.14.3. 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.
5.1.15. Fornecer por escrito as informações necessárias para o desenvolvimento dos serviços objeto do contrato.
5.1.16. Realizar avaliações periódicas da qualidade dos serviços, após seu recebimento.
5.1.17. 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.
5.1.18. 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.

5.2. Deveres e responsabilidades da CONTRATADA

5.2.1. 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;
5.2.2. Reparar, corrigir, remover ou substituir, às suas expensas, no total ou em parte, no prazo fixado pelo GESTOR DO CONTRATO, os serviços efetuados em que se verificarem vícios, defeitos ou incorreções resultantes da execução ou dos materiais empregados;
5.2.3. 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;
5.2.4. Quando especificado, manter durante a execução do CONTRATO equipe técnica composta por profissionais devidamente habilitados, treinados e qualificados para fornecimento da Solução de Tecnologia da Informação de acordo com os requisitos contratados, em conformidade com as normas e determinações em vigor;
5.2.5. 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° 7.203/2010;
5.2.6. 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;
5.2.7. Arcar com todos os custos administrativos de sua responsabilidade relacionados ao OBJETO e à execução do CONTRATO – responsabilizando-se inclusive por todas as

obrigações trabalhistas, sociais, previdenciárias, tributárias e as demais previstas em legislação específica, cuja inadimplência não transfere responsabilidade ao CONTRATANTE;
5.2.8. 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;
5.2.9. Informar prontamente ao CONTRATANTE sobre fatos e/ou situações relacionadas à prestação dos serviços contratados que representem risco ao êxito da contratação ou o cumprimento de prazos exigidos, além de responsabilizar-se pelo conteúdo e veracidade das informações prestadas - sob pena de incorrer em situações de dolo ou omissão e comunicar ao GESTOR/FISCAL DO CONTRATO, no prazo de 24 (vinte e quatro) horas, qualquer ocorrência anormal ou acidente que se verifique no local dos serviços;
5.2.10. 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;
5.2.11. 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;
5.2.12. Promover a guarda, manutenção e vigilância de materiais, ferramentas, e tudo o que for necessário à execução dos serviços, durante a vigência do CONTRATO;
5.2.13. 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;
5.2.14. Submeter previamente, por escrito, à CONTRATANTE, para análise e aprovação, quaisquer mudanças nos métodos executivos que fujam às especificações do memorial descritivo e/ou modelo de execução;
5.2.15. 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;
5.2.16. Manter durante toda a vigência do CONTRATO, em compatibilidade com as obrigações assumidas, todas as condições de habilitação e qualificação exigidas na licitação;
5.2.17. 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;
5.2.18. 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;
5.2.19. 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;

5.2.20. Atender prontamente quaisquer orientações e exigências do GESTOR DO CONTRATO, inerentes à execução do objeto contratual e propiciar todos os meios e facilidades necessárias à fiscalização da Solução de Tecnologia da Informação pelo CONTRATANTE, cujo representante terá poderes para sustar o fornecimento, total ou parcialmente, em qualquer tempo, sempre que considerar a medida necessária;
5.2.21. Manter a produtividade ou a capacidade mínima de fornecimento da Solução de Tecnologia da Informação durante a execução do contrato, conforme art. 18, inciso I, alínea "g" da IN SLTI.MP n° 04, de 11/09/2014;
5.2.22. Ceder os direitos de propriedade intelectual e direitos autorais da Solução de Tecnologia da Informação sobre os diversos artefatos e produtos produzidos ao longo do CONTRATO, incluindo a documentação, os modelos de dados e as bases de dados ao CONTRATANTE, nos termos da legislação vigente;
5.2.23. Zelar pelo cumprimento de leis e normas relativas à segurança e medicina do trabalho durante a execução de quaisquer serviços de sua responsabilidade nas instalações do CONTRATANTE. Assim como cumprir as normas do CONTRATANTE aplicáveis em suas instalações funcionais, inclusive regras de acesso e controles de segurança; e
5.2.24. Manter o mais rigoroso sigilo sobre quaisquer dados, informações, documentos e especificações que a ela venham a ser confiados ou que venha a ter acesso em razão da execução dos serviços, não podendo, sob qualquer pretexto, revelá-los, divulgá-los, reproduzi-los ou deles dar conhecimento a quaisquer terceiros.

5.3. Deveres e responsabilidades do órgão gerenciador da ata de registro de preços

5.3.1. Efetuar o registro do licitante fornecedor e firmar a correspondente Ata de Registro de Preços;
5.3.2. Conduzir os procedimentos relativos a eventuais renegociações de condições, produtos ou preços registrados;
5.3.3. Definir mecanismos de comunicação com os órgãos participantes e não participantes, contendo:
5.3.1.1. as formas de comunicação entre os envolvidos, a exemplo de ofício, telefone, e-mail, ou sistema informatizado, quando disponível; e
5.3.2.1. definição dos eventos a serem reportados ao órgão gerenciador, com a indicação de prazo e responsável;
5.3.4. Definir mecanismos de controle de fornecimento da solução de TIC, observando, dentre outros:
5.3.4.1 a definição da produtividade ou da capacidade mínima de fornecimento da solução de TIC;
5.3.4.2. as regras para gerenciamento da fila de fornecimento da solução de TIC aos órgãos participantes e não participantes, contendo prazos e formas de negociação e redistribuição da demanda, quando esta ultrapassar a produtividade definida ou a capacidade mínima de fornecimento e for requerida pela CONTRATADA; e
5.3.5. as regras para a substituição da solução registrada na Ata de Registro de Preços, garantida a realização de Prova de Conceito, em função de fatores supervenientes que tornem necessária e imperativa a substituição da solução tecnológica;

6 – MODELO DE EXECUÇÃO DO CONTRATO

6.1. Rotinas de Execução

6.1.1. DA INICIALIZAÇÃO DO CONTRATO

6.1.1.1. Após a assinatura do Contrato e a nomeação do Gestor e Fiscais do Contrato, será realizada a Reunião Inicial de alinhamento com o objetivo de nivelar os entendimentos acerca das condições estabelecidas no Contrato, Edital e seus anexos, e esclarecer possíveis dúvidas acerca da execução dos serviços.
6.1.1.2. A reunião inicial poderá ser realizada de forma presencial ou remota.
6.1.1.3. A reunião será realizada em conformidade com o previsto no inciso I do Art. 31 da IN SGD-ME nº 01/2019 e ocorrerá em até 10 (dez) dias úteis da assinatura do Contrato, podendo ser prorrogada a critério da CONTRATANTE.
6.1.1.4. A pauta desta reunião observará, pelo menos:

a) Apresentação do Preposto da empresa pelo representante legal da Contratada. A Carta de apresentação do Preposto deverá conter no mínimo o nome completo e CPF do funcionário da empresa designado para acompanhar a execução do contrato e atuar como interlocutor principal junto à CONTRATANTE, incumbido de receber, diligenciar, encaminhar e responder as principais questões técnicas, legais e administrativas referentes ao andamento contratual.
b) Apresentação das declarações/certificados do fabricante, comprovando que o produto ofertado possui a garantia solicitada neste termo de referência.
c) O representante legal da CONTRATADA deverá entregar o Termo de Compromisso e o Termo de Ciência, contendo declaração de manutenção de sigilo e respeito às normas de segurança vigentes na entidade;
d) O representante legal da CONTRATADA deverá apresentar o cronograma de execução do projeto;
e) Serão feitos esclarecimentos relativos a questões operacionais, administrativas e de gestão do contrato.

6.1.2. DA EXECUÇÃO DO CONTRATO

6.1.2.1. O gestor do contrato emitirá a Ordem de Fornecimento de Bens (OFB) para a entrega dos bens desejados.
6.1.2.2. A CONTRATADA fornecerá um equipamento com as mesmas configurações do tipo indicado na OFB para geração da imagem, quando for solicitado o fornecimento com imagem "ISO".
6.1.2.3. A remessa (única ou parcelada) deve ser feita no endereço constante da OFB compatível com a relação de endereços constantes do ANEXO A - ENDEREÇOS DAS UNIDADES.
6.1.2.4. Os bens serão recebidos provisoriamente, quando da entrega do objeto integral do objeto (incluindo todas as parcelas), pelo(a) responsável pelo acompanhamento e fiscalização do contrato, para efeito de posterior verificação de sua conformidade com as especificações constantes neste Termo de Referência e na proposta.
6.1.2.4.1. Os bens poderão ser rejeitados, no todo ou em parte, quando em desacordo com as especificações constantes neste Termo de Referência e na proposta, devendo ser

substituídos no prazo de 10 (dez) dias corridos, a contar da notificação da contratada, às suas custas, sem prejuízo da aplicação das penalidades.

6.1.2.5. O recebimento provisório será realizado pelo FISCAL TÉCNICO do CONTRATO quando da entrega do OBJETO resultante de cada ORDEM DE FORNECIMENTO DE BENS e consiste na emissão do documento "TERMO DE RECEBIMENTO PROVISÓRIO" que, por sua vez, consiste na declaração formal de que os bens foram entregues e os serviços foram prestados, para posterior análise das conformidades e qualidades baseadas nos requisitos e nos critérios de aceitação previstos na 7.1 deste Termo de Referência.

6.1.2.5.1. O recebimento provisório ou definitivo não modifica, restringe ou elide a plena responsabilidade da CONTRATADA de fornecer os bens de acordo com as especificações, quantidades e condições estabelecidas, inclusive na proposta de preços, nem invalida qualquer reclamação que o CONTRATANTE venha a fazer em virtude de posterior constatação da entrega de bens fora de especificação, garantido o devido reparo, sem custo adicional.

6.1.2.6. Após o recebimento provisório, os fiscais TÉCNICO, REQUISITANTE e ADMINISTRATIVO realizarão análise do(s) bem(ns) entregue(s), considerando:

a) A avaliação da qualidade realizada a partir da aplicação de listas de verificação e de acordo com os critérios de aceitação definidos em CONTRATO;
b) Verificação de aderências aos requisitos e especificações técnicas;
c) Identificação de eventuais não conformidade com os termos contratuais;
d) Verificação de aderência aos termos contratuais, a cargo do Fiscal Administrativo do CONTRATO;
e) Verificação da manutenção das condições classificatórias referentes à pontuação obtida e à habilitação técnica, a cargo dos Fiscais Administrativo e Técnico do CONTRATO;
f) Encaminhamento à CONTRATADA das eventuais demandas de correção, a cargo do GESTOR do CONTRATO ou, por delegação de competência, do Fiscal Técnico do CONTRATO;
g) Cálculo e encaminhamento à CONTRATADA de indicação de eventuais glosas por descumprimento de níveis mínimos de serviço exigidos por parte do Gestor do CONTRATO, quando for o caso.

6.1.2.7. Os bens serão recebidos definitivamente no prazo de 15 (quinze) dias úteis, contados do recebimento provisório, após a verificação da qualidade e quantidade do material e consequente aceitação mediante termo circunstanciado, desde que estejam de acordo com os critérios de aceitação constante da seção 7.1 deste Termo de Referência.

6.1.2.8. Concluída a avaliação da qualidade e da conformidade dos bens entregues e provisoriamente recebidos, a CONTRATANTE confeccionará o documento "TERMO DE RECEBIMENTO DEFINITIVO", com base nas informações da etapa de avaliação da qualidade e contendo a autorização para emissão e posterior pagamento da(s) NOTA(S) FISCAL(IS).

6.1.2.9. Nos casos aplicáveis, observando de forma complementar o disposto na alínea “c” do inciso II do art. 50 da IN n° 05/SEGES/MPDG, de 26/05/2017, quando houver glosa parcial das faturas, o GESTOR deverá comunicar a empresa para que emita a(s) NOTA(S) FISCAL(IS) com o valor exato dimensionado, evitando, assim, efeitos tributários sobre valor glosado pela Administração.

6.1.2.10. A(s) Nota(s) Fiscal(is) apresentadas pela CONTRATADA devem estar aderentes aos requisitos legais e tributários firmados pelos órgãos competentes, sendo que o pagamento somente será autorizado após ATESTE pelo(s) servidor(es) competente(s), condicionado este ato à verificação da conformidade e da adequação em relação aos bens efetivamente entregues.
6.1.2.11. O pagamento observará o disposto na seção 7.5 deste Termo de Referência.
6.1.2.11.1. Caso sejam verificadas irregularidades que impeçam a liquidação e o pagamento da despesa, o GESTOR DO CONTRATO deve indicar as cláusulas contratuais pertinentes, solicitando à contratada, por escrito, as respectivas medidas de correção.
6.1.3. DAS ROTINAS DE EXECUÇÃO:
6.1.3.1. Prazos, horários de fornecimento de bens ou prestação dos serviços:
6.1.3.1.1. A entrega de todos os produtos deverá ocorrer em até no máximo 90 (noventa) dias corridos a contar do recebimento da Ordem de Fornecimento de Bens (OFB).
6.1.3.1.2. A implantação completa da solução deverá ser concluída em até 30 (trinta) dias corridos após a entrega do objeto.
6.1.3.1.3. Os equipamentos deverão ser entregues e instalados no endereço constante da OFB compatível com a relação de endereços constantes do **ANEXO A - ENDEREÇOS DAS UNIDADES**.
6.1.3.1.4. A entrega e a instalação deverão ser realizadas em dias úteis no horário das 08:00 às 12:00 e das 14:00 às 18:00. Excepcionalmente, a instalação poderá ocorrer em dia ou horário diferente destes, mediante pedido ou autorização da CONTRATANTE.
6.1.3.1.5. A entrega deverá ser agendada com antecedência mínima de 24 horas, sob o risco de não ser autorizada.
6.1.3.1.6. O suporte técnico deverá ser de, no mínimo, 60 meses.
6.1.3.2. Documentação mínima exigida:
6.1.3.2.1. A CONTRATADA deverá fornecer:
6.1.3.2.1.1. Manuais técnicos do usuário e de referência contendo todas as informações sobre os produtos com as instruções para instalação, configuração, operação e administração;
6.1.3.2.1.2. Documentação completa da solução, incluindo especificação do equipamento, características e funcionalidades implementadas, desenho lógico da implantação, comentários e configurações executadas.
6.1.3.2.1.3. Relatório com o detalhamento do processo realizado ao final da implantação como requisito para o aceite definitivo.
6.1.3.3. Formas de transferência de conhecimento:
6.1.3.3.1. A fim de promover a transferência de conhecimento, a implantação da solução deverá ocorrer com participação direta da equipe de TI da reitoria do IFMS que atuarão na solução. Durante a implantação da solução a equipe da CONTRATADA deverá repassar as informações para a equipe do IFMS apresentando as configurações realizadas nos equipamentos, a topologia final e procedimentos executados.

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

6.2.1. Não se aplica.

6.3. Mecanismos formais de comunicação

6.3.1. São definidos como mecanismos de comunicação, entre a CONTRATANTE, e a CONTRATADA, os seguintes:
6.3.1.1. Ordem de Fornecimento de bens / Ordem de Serviço (conforme modelo genérico apresentado no **ANEXO D**);
6.3.1.2. Ata de Reunião;
6.3.1.3. Ofício;
6.3.1.4. Sistema de abertura de chamados.

6.4. Manutenção de Sigilo e Normas de Segurança

6.4.1. A CONTRATADA deverá manter sigilo absoluto sobre quaisquer dados e informações contidos em quaisquer documentos e mídias, incluindo os equipamentos e seus meios de armazenamento, de que venha a ter conhecimento durante a execução dos serviços, não podendo, sob qualquer pretexto, divulgar, reproduzir ou utilizar, sob pena de lei, independentemente da classificação de sigilo conferida pelo CONTRATANTE a tais documentos.
6.4.2. O **Termo de Compromisso**, contendo declaração de manutenção de sigilo e respeito às normas de segurança vigentes na entidade, a ser assinado pelo representante legal da CONTRATADA e Termo de Ciência, a ser assinado por todos os empregados da CONTRATADA diretamente envolvidos na contratação, encontram-se nos **ANEXOS B** e **C**.

7 – MODELO DE GESTÃO DO CONTRATO

7.1. Critérios de Aceitação

7.1.1. Os itens (bens e serviços) fornecidos deverão atender aos critérios de aceitação a seguir definidos:

Critérios de aceitação dos bens e serviços	
CRITÉRIO	**DESCRIÇÃO DO CRITÉRIO**
Forma	Os bens e serviços deverão ser entregues da forma especificada no item 4 - ESPECIFICAÇÃO DOS REQUISITOS DA CONTRATAÇÃO.
Completude	Os bens e serviços entregues serão avaliados com base em sua conformidade com requisitos de conteúdo mínimo e etapas de construção pré-estabelecidas.
Consistência	Os bens e serviços entregues serão avaliados com base em sua conformidade com requisitos de amplitude técnica, fidedignidade, fundamentação e fiabilidade do conteúdo.

Qualidade	Os bens e serviços entregues serão avaliados com base em sua conformidade a níveis de serviço pré-estabelecidos.

7.1.2. Resultados e/ou produtos entregues que não atendam aos níveis mínimos de qualidade e/ou serviços, sejam inconsistentes e/ou incompletos serão rejeitados. Entregas desformatadas poderão ser aceitas com restrição, implicando compromisso do provedor de serviços em solucionar as restrições impreterivelmente no tempo determinado pelo tomador de serviços, sob pena de não recebimento (rejeição) – não exclusas outras cumulações previstas em CONTRATO.
7.1.3. Será REJEITADO, no todo ou em parte, o serviço ou entregável fornecido em desacordo com as especificações constantes deste TERMO DE REFERÊNCIA e seus APÊNDICES e ANEXOS. Ainda, conforme o art. 69 da Lei 8.666/1993, a CONTRATADA é obrigada a reparar, corrigir, remover, reconstruir ou substituir, às suas expensas, no total ou em parte, o objeto do CONTRATO em que se verificarem vícios, defeitos ou incorreções resultantes da execução ou de materiais empregados.
7.1.4. Só haverá o RECEBIMENTO DEFINITIVO (HOMOLOGAÇÃO), após a análise da qualidade dos serviços, em face da aplicação dos critérios de qualidade e da verificação dos níveis mínimos de serviço, resguardando-se ao CONTRATANTE o direito de não receber o objeto cuja qualidade seja comprovadamente baixa – situação em que poderão ser aplicadas à CONTRATADA as penalidades previstas em lei, neste TERMO DE REFERÊNCIA e no CONTRATO. Quando for caso, a empresa será convocada a refazer todos os serviços rejeitados, sem custo adicional.
7.1.5. Nos termos do Anexo V da IN SEGES/MP n. 5/2017, será efetuada a retenção ou glosa no pagamento, proporcional à irregularidade verificada, sem prejuízo das sanções cabíveis, caso se constate que a CONTRATADA:
7.1.5.1. Não produziu os resultados acordados;
7.1.5.2. Deixou de executar as atividades contratadas, ou não as executou com a qualidade mínima exigida;
7.1.5.3. Deixou de utilizar os materiais e/ou recursos humanos exigidos para a execução do serviço e/ou utilizou-os com qualidade ou quantidade inferior à demandada.
7.1.6. A aplicação de descontos/glosas em função do descumprimento de critérios de qualidade, avaliação de resultados e/ou níveis mínimos de serviço exigidos não concorre com a aplicação (concomitante ou não) das sanções administrativas previstas em CONTRATO, inclusive daquelas previstas em função do reiterado descumprimento dos critérios de qualidade do serviço, sendo essa uma prerrogativa da Administração.

7.2. Procedimentos de Teste e Inspeção

7.2.1. O CONTRATANTE reserva-se ao direito de promover avaliações, inspeções e diligências visando esclarecer quaisquer situações relacionadas à prestação dos serviços contratados, sendo obrigação da CONTRATADA acolhê-las.

7.3. Níveis Mínimos de Serviço Exigidos

7.3.1. Os NÍVEIS MÍNIMOS DE SERVIÇO (ou NÍVEIS DE SERVIÇO) definem critérios objetivos e mensuráveis cuja finalidade é aferir e avaliar os resultados dos serviços contratados e o desempenho da CONTRATADA, conforme apresentado mais adiante. Neles encontram-se definidos: a maneira pela qual estes fatores serão avaliados; o nível mínimo aceitável; e os descontos a serem aplicados na fatura, quando o serviço prestado não alcançar o nível esperado.
7.3.2. Os NÍVEIS DE SERVIÇOS devem ser considerados e entendidos pela CONTRATADA como um compromisso e comprometimento de qualidade que está assumindo para a prestação dos serviços. Portanto, no decorrer da execução contratual a CONTRATADA deverá monitorar continuamente seus indicadores, zelando pela qualidade dos serviços e pela efetiva entrega de resultados.
7.3.3. Eventualmente poderão existir impedimentos técnicos para o atendimento dos prazos previamente estabelecidos para uma demanda ou indicador. Nesses casos, a CONTRATADA deverá notificar formalmente o CONTRATANTE – ficando a critério exclusivo deste último avaliar os impedimentos, assim como acatar ou rejeitar as justificativas apresentadas.
7.3.4. Indicadores de níveis de serviços (INS):

IAE – INDICADOR DE ATRASO DE ENTREGA DE OFB	
Tópico	**Descrição**
Finalidade	Medir o tempo de atraso na entrega dos produtos e serviços constantes na Ordem de Fornecimento de Bens.
Meta a cumprir	IAE < = 0 A meta definida visa garantir a entrega dos produtos e serviços constantes nas Ordens de Fornecimento de Bens dentro do prazo previsto.
Instrumento de medição	Ordem de Fornecimento de Bens e Termos de Recebimento Provisório e Definitivo emitidos.
Forma de acompanhamento	A avaliação será feita conforme linha de base do cronograma registrada na OFB. Será subtraída a data de entrega dos produtos da OFB (desde que o fiscal técnico reconheça aquela data, com registro em Termo de Recebimento Provisório) pela data do recebimento da OFB pela contratada.
Periodicidade	Para cada OFB encerrada mediante Termo de Recebimento Definitivo.
Mecanismo de Cálculo (métrica)	IAE = (TEX – TEST) / TEST Onde: IAE – Indicador de Atraso de Entrega da OFB;

	TEX – Tempo de Execução – corresponde ao período de execução da OFB, da sua data de início até a data de entrega dos produtos da OFB. A data de início será aquela contante na OFB; caso não esteja explícita, será o primeiro dia útil após a emissão da OFB. A data de entrega da OFB deverá ser aquela reconhecida pelo fiscal técnico, conforme critérios constantes no Termo de Referência. Para os casos em que o fiscal técnico rejeita a entrega, o prazo de execução da OFB continua a correr, findando-se apenas quanto a CONTRATADA entrega os produtos da OS e haja aceitação por parte do fiscal técnico. TEST – Tempo Estimado para a execução da OFB – constante na OFB, conforme estipulado no Termo de Referência.
Observações	1. Serão utilizados dias úteis na medição. 2. Os dias com expediente parcial no órgão/entidade serão considerados como dias úteis no cômputo do indicador. 3. Não se aplicará este indicador para as OFB de Manutenções Corretivas do tipo Garantia e aquelas com execução interrompida ou cancelada por solicitação da CONTRATANTE.
Início de Vigência	A partir da emissão da OFB.
Faixas de ajuste no pagamento e Sanções	Para valores do indicador IAE: De 0 a 0,10 – Pagamento integral da OFB; De 0,11 a 0,20 – Glosa de 0,1% sobre o valor da OFB; De 0,21 a 0,30 – Glosa de 0,2% sobre o valor da OFB; De 0,31 a 0,50 – Glosa de 0,3% sobre o valor da OS; De 0,51 a 1,00 – Glosa de 0,5% sobre o valor da OFB; Acima de 1 – Será aplicada Glosa de 1% sobre o valor da OFB e multa de 0,5% sobre o valor do Contrato.

IAAC - INDICADOR DE ATRASO NO ATENDIMENTO A CHAMADOS	
Tópico	**Descrição**
Finalidade	Medir o tempo de atraso no atendimento de chamados.
Meta a cumprir	IAAC 0% A meta definida visa garantir que o atendimento dos chamados ocorra dentro do prazo considerado razoável.
Instrumento de medição	Documento utilizado para abertura de chamado junto à CONTRATADA.
Forma de acompanhamento	Contagem de tempo entre a abertura do chamado pela CONTRATANTE e a conclusão satisfatória do atendimento pela CONTRATADA.
Periodicidade	Por chamado aberto ao longo de todo o período contratual.
Mecanismo de Cálculo (métrica)	IAAC = PE - PPPP100 Onde: IAAC = Indicador de Atraso no Atendimento a Chamados PE = Prazo Efetivo de conclusão PP = Prazo Previsto de conclusão

Observações	1 - A contagem de tempo para regularização de inconformidades levará em consideração apenas as horas transcorridas durante o horário de funcionamento da sede do IFMS (das 08h00 às 17h00) em dias úteis (segunda a sexta-feira, excluídos os feriados). 2 - Prazo Previsto para chamados de criticidade urgente = até 20 horas corridas. O chamado será urgente quando o problema identificado gerar indisponibilidade total da solução. 4 - Prazo Previsto para chamados de criticidade alta = até 48 horas corridas. O chamado terá alta criticidade quando o problema identificado gerar indisponibilidade da solução repetidas vezes no intervalo de um turno de trabalho (manhã ou tarde). 5 - Prazo Previsto para chamados de criticidade média = até 120 horas corridas. O chamado terá média criticidade quando o problema identificado gerar indisponibilidades esporádicas ao longo de uma semana de trabalho. 6 - Prazo Previsto para chamados de criticidade baixa = até 240 horas corridas. O chamado terá baixa criticidade quando o problema identificado não gerar indisponibilidade da solução.
Início de Vigência	A partir da emissão da Ordem de Fornecimento de Bens.
Faixas de ajuste no pagamento e Sanções	IAAC Razoável <= 20% - Glosa de 0,5% (meio por cento) para cada rejeição até o limite de 5 ocorrências; 1% (um por cento) para cada rejeição superior a 5 ocorrências (quaisquer cujo IAAC seja superior à meta). IAAC Indesejável > 20% e <= 40% - Glosa de 1% (um por cento) para cada rejeição até o limite de 5 ocorrências; 2% (um por cento) para cada rejeição superior a 5 ocorrências (quaisquer cujo IAAC seja superior à meta). IAAC Inaceitável > 40% - Glosa de 2% (dois por cento) para cada rejeição até o limite de 5 ocorrências; 4% (quatro por cento) para cada rejeição superior a 5 ocorrências (quaisquer cujo IAAC seja superior à meta).

7.4. Sanções Administrativas e Procedimentos para retenção ou glosa no pagamento

7.4.1. A finalidade das sanções administrativas em licitações e contratos públicos é responder à prática de infração administrativa cometida pelo sancionado – podendo ter caráter preventivo, educativo, repressivo e/ou reparativo (quando se busca a reparação de danos ao erário público).

7.4.2. Nos termos da LEI Nº 10.520/2002 comete infração administrativa a CONTRATADA que:
7.4.2.1. Inexecutar total ou parcialmente qualquer das obrigações assumidas em decorrência da contratação;
7.4.2.2. ensejar o retardamento da execução do objeto;
7.4.2.3. falhar ou fraudar a execução do contrato;
7.4.2.4. comportar-se de modo inidôneo; ou
7.4.2.5. cometer fraude fiscal.
7.4.3. As sanções administrativas fixadas nas normas, aplicadas aos LICITANTES e CONTRATADOS, são as seguintes:
7.4.3.1. Advertência;
7.4.3.2. Multa;
7.4.3.3. Suspensão temporária de participação em licitação e impedimento de contratar com a Administração, por prazo não superior a 02 (dois) anos;
7.4.3.4. Declaração de inidoneidade para licitar ou contratar com a Administração Pública;
7.4.3.5. Impedimento de licitar e contratar com a União, Estados, Distrito Federal ou Municípios e o descredenciamento no Sistema de Cadastramento de Fornecedores - SICAF pelo prazo de até 5 (cinco) anos, sem prejuízo das multas previstas em edital e no contrato e das demais cominações legais.
7.4.4. A aplicação de qualquer das penalidades previstas realizar-se-á em processo administrativo que assegurará o contraditório e a ampla defesa à CONTRATADA, observando-se o procedimento previsto na Lei nº 8.666/1993, e, subsidiariamente, na Lei nº 9.784, de 29/01/1999.
7.4.5. Conforme previsto no art. 40 da Instrução Normativa n° 03, de 26 de abril de 2018, que estabelece normas para o funcionamento do Sistema de Cadastramento Unificado de Fornecedores - SICAF no âmbito dos órgãos e entidades integrantes do Sistema de Serviços Gerais – SISG, as sanções descritas são passíveis de registro no SICAF.
7.4.6. A sanção de advertência consiste em uma comunicação formal à CONTRATADA, após a instauração do processo administrativo sancionador, sendo aplicada quando do não cumprimento de quaisquer das obrigações contratuais consideradas faltas leves – assim entendidas aquelas que não acarretam prejuízos significativos para o serviço contratado.
7.4.7. A advertência deve conter o apontamento do fato gerador, determinando que seja sanada a impropriedade e notificando que, em caso de reincidência, sanção mais elevada poderá ser aplicada.
7.4.8. A sanção pecuniária será aplicada em caso de atraso injustificado no cumprimento de obrigação contratual e/ou em decorrência da inexecução parcial ou total do objeto da contratação, nos termos do art. 86 e 87 da Lei nº 8.666/1993, e/ou na reincidência de faltas punidas por advertência, e demais vedações que não tipifiquem infração sujeita à suspensão temporária de participação em licitação, declaração de inidoneidade e impedimento de licitar e contratar com a Administração Federal, e será aplicada nos seguintes percentuais:
I - 0,33% (trinta e três centésimos por cento) por dia de atraso, na entrega de material ou execução de serviços, calculado sobre o valor correspondente à parte inadimplente, até o limite de 9,9%, que corresponde a até trinta dias de atraso;
II - 0,66 % (sessenta e seis centésimos por cento) por dia de atraso, na entrega de material ou execução de serviços, calculado, desde o primeiro dia de atraso, sobre o valor

correspondente à parte inadimplente, em caráter excepcional, e a critério do órgão contratante, quando o atraso ultrapassar trinta dias;
III - 5% (cinco por cento) sobre o valor total do contrato/nota de empenho, por descumprimento do prazo de entrega;
IV - 15% (quinze por cento) em caso de recusa injustificada do adjudicatário em assinar o contrato ou retirar o instrumento equivalente, dentro do prazo estabelecido pela Administração, recusa parcial ou total na entrega do material, recusa na conclusão do serviço, ou rescisão do contrato/nota de empenho, calculado sobre a parte inadimplente; e
V - 20% (vinte por cento) sobre o valor do contrato/nota de empenho, pela inexecução total do contrato.
7.4.9. A multa (de mora) será formalizada por simples apostilamento contratual, na forma do art. 65, § 8° , da Lei n° 8.666, de 1993, e será executada após regular processo administrativo, observada a seguinte ordem:
I - Mediante desconto no valor da garantia depositada do respectivo contrato, caso exigida no EDITAL;
II - Mediante desconto no valor das parcelas devidas à contratada; e
III - Mediante procedimento administrativo ou judicial de execução.
7.4.10. Se a multa aplicada for superior ao valor da garantia prestada, além da perda desta, responderá à contratada pela sua diferença, devidamente atualizada pelo Índice Geral de Preços – Mercado (IGP-M) ou equivalente, que será descontada dos pagamentos eventualmente devidos pela Administração ou cobrados judicialmente.
7.4.11. O atraso, para efeito de cálculo de multa, será contado em dias corridos, a partir do dia seguinte ao do vencimento do prazo de entrega ou execução do contrato, se dia de expediente normal na repartição interessada, ou no primeiro dia útil seguinte. As sanções de advertência, suspensão e inidoneidade poderão ser aplicadas juntamente com a multa, conforme § 2º do art. 87 de Lei nº 8.666, de 1993.
7.4.12. No caso de multa, cuja apuração ainda esteja em processamento, ou seja, na fase da defesa prévia e/ou prazo recursal, a Contratante poderá fazer a retenção do valor correspondente à multa, até a decisão, caso não obtenha sucesso na execução da garantia ofertada. Caso a defesa prévia e/ou recurso seja aceito, ou aceito parcialmente, pela Contratante, o valor retido correspondente será depositado em favor da Contratada, em até 5 (cinco) dias úteis a contar da data da decisão final. Ao exceder o limite máximo admitido de infrações durante a vigência contratual OU mediante o reiterado descumprimento de critérios de qualidade e/ou níveis mínimos de serviço exigidos OU diante da reiterada aplicação de sanções contratuais, a ADMINISTRAÇÃO CONTRATANTE deverá avaliar a possibilidade de promover a rescisão do CONTRATO em função da INEXECUÇÃO TOTAL ou PARCIAL do OBJETO, da perda de suas funcionalidades e da comprovada desconformidade com os critérios mínimos de qualidade exigidos – ressalvada a aplicação adicional de outras sanções administrativas cabíveis, respeitados os princípios da razoabilidade, da proporcionalidade, da ampla defesa e do contraditório.
7.4.13. A sanção de suspensão de participar em licitações e contratar com o órgão sancionador suspende o direito do sancionado de participar dos procedimentos licitatórios promovidos no âmbito do órgão responsável pela aplicação da sanção por prazo não superior a 02 (dois) anos. A previsão legal está inserida no inciso III do art. 87 da Lei nº 8.666, de 21 de junho de 1993.

7.4.14. A aplicação da sanção de impedimento de licitar e contratar com os órgãos e entidades da União, prevista no art. 7º da Lei 10.520/2002, impossibilitará o sancionado de participar de licitações e formalizar contrato no âmbito interno do ente federativo que aplicar a sanção – no presente caso, a União.
7.4.15. Com fundamento no artigo 7º da Lei nº 10.520/2002 e no art. 49 do Decreto nº 10.024/2019, ficará(ão) impedida(s) de licitar e contratar com a União e será descredenciada no SICAF e no cadastro de fornecedores do CONTRATANTE, pelo prazo de até 5 (cinco) anos, garantida a ampla defesa, sem prejuízo das multas previstas neste Termo/Contrato e demais cominações legais a(s) CONTRATADA(S) que:
7.4.15.1. Apresentar documentação falsa;
7.4.15.2. Ensejar o retardamento da execução do objeto;
7.4.15.3. Falhar ou fraudar na execução do contrato;
7.4.15.4. Deixar de entregar a documentação exigida no edital;
7.4.15.5. Não assinar o termo de contrato e/ou ata de registro de preços ou aceitar/retirar o instrumento equivalente, quando convocado dentro do prazo de validade da proposta;
7.4.15.6. Não mantiver proposta;
7.4.15.7. Comportar- se de modo inidôneo;
7.4.15.8. Fizer declaração falsa;
7.4.15.9. Cometer fraude fiscal.
7.4.16. Ainda, nos termos do art. 49 do Decreto n° 10.024, de 20 de setembro de 2019, que "regulamenta a licitação, na modalidade pregão, na forma eletrônica, para a aquisição de bens e a contratação de serviços comuns, incluídos os serviços comuns de engenharia, e dispõe sobre o uso da dispensa eletrônica, no âmbito da administração pública federal", temos que:

> *Art. 49. Ficará impedido de licitar e de contratar com a União e será descredenciado no Sicaf, pelo prazo de até cinco anos, sem prejuízo das multas previstas em edital e no contrato e das demais cominações legais, garantido o direito à ampla defesa, o licitante que, convocado dentro do prazo de validade de sua proposta:*
> *I - não assinar o contrato ou a ata de registro de preços;*
> *II - não entregar a documentação exigida no edital;*
> *III - apresentar documentação falsa;*
> *IV - causar o atraso na execução do objeto;*
> *V - não mantiver a proposta;*
> *VI - falhar na execução do contrato;*
> *VII - fraudar a execução do contrato;*
> *VIII - comportar-se de modo inidôneo;*
> *IX - declarar informações falsas; e*
> *X - cometer fraude fiscal.*
> *§ 1º As sanções descritas no caput também se aplicam aos integrantes do cadastro de reserva, em pregão para registro de preços que, convocados, não honrarem o compromisso assumido sem justificativa ou com justificativa recusada pela administração pública.*
> *§ 2º As sanções serão registradas e publicadas no Sicaf.*

7.4.17. O descredenciamento no Sistema de Cadastramento de Fornecedores do Governo Federal (SICAF) se dará com a aposição da situação "inativo" sobre os dados do fornecedor

no sistema, em consequência da aplicação da sanção de impedimento de licitar e contratar com a União, em conformidade com o art. 7º da Lei nº 10.520/2002.

7.4.18. 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.

7.4.19. A sanção de declaração de inidoneidade impossibilitará o sancionado de participar de licitações e formalizar contratos com todos os órgãos e entidades da Administração Pública direta e indireta da União, dos Estados, do Distrito Federal e dos Municípios e vigerá 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 ADMINISTRAÇÃO CONTRATANTE pelos prejuízos causados.

7.4.20. Também ficam sujeitas às penalidades do art. 87, III e IV da Lei nº 8.666, de 1993, as empresas ou profissionais que:

7.4.20.1. tenham sofrido condenação definitiva por praticar, por meio dolosos, fraude fiscal no recolhimento de quaisquer tributos;

7.4.20.2. tenham praticado atos ilícitos visando a frustrar os objetivos da licitação; e/ou

7.4.20.3. demonstrem não possuir idoneidade para contratar com a Administração em virtude de atos ilícitos praticados.

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

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

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

7.4.24. 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.

7.4.25. 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.

7.4.26. Se, durante o processo de aplicação de penalidade, se houver indícios de prática de infração administrativa tipificada pela Lei nº 12.846/2013, 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.

7.4.27. 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 12.846/2013, seguirão seu rito normal na unidade administrativa.

7.4.28. 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.

7.5. Do Pagamento

7.5.1. O CONTRATANTE demandará os volumes de licenças contratadas de forma gradual, de acordo com sua efetiva necessidade e seguindo cronograma de implantação, cabendo o pagamento apenas sobre os quantitativos demandados, fornecidos e efetivamente implantados.

Faturamento = [(Ordem de FornecimentoExecutada)-AjusteNMS]
Faturamento: Remuneração devida à CONTRATADA pelo fornecimento de licenças/subscrições demandadas em uma Ordem de Fornecimento, considerando as quantidades efetivamente entregues/prestadas e os valores estabelecidos em contrato. Ajuste: Ajuste (redução/glosa) em função dos resultados dos indicadores de Níveis Mínimos de Serviço e da aplicação dos critérios de reduções à remuneração.

7.5.2. O valor unitário individual de cada licença deverá ser calculado da seguinte forma:

A solução de firewall e de backup deve ser faturada de uma única vez, de acordo com a quantidade efetivamente demandada pelo CONTRATANTE e entregue pela CONTRATADA.

7.5.3. Para fins de cálculo do faturamento, o valor unitário de cada solução de segurança será aquele verificado no ato de emissão da respectiva ORDEM DE FORNECIMENTO.

7.5.4. Sobre o faturamento da CONTRATADA incidirão eventuais descontos/glosas resultantes dos resultados e de acordo com a aplicação dos critérios de reduções ao faturamento, conforme recomendado nas normas aplicáveis às contratações públicas de Tecnologia da Informação por órgãos e entidades da Administração Pública Federal, considerando a análise de alternativas realizada no ESTUDO TÉCNICO PRELIMINAR e o disposto na Súmula TCU n° 269, in verbis:

> *"Nas contratações para a prestação de serviços de tecnologia da informação, a remuneração deve estar vinculada a resultados ou ao atendimento de níveis de serviço, admitindo-se o pagamento por hora trabalhada ou por posto de serviço somente quando as características do objeto não o permitirem, hipótese em que a excepcionalidade deve estar prévia e adequadamente justificada nos respectivos processos administrativos". [Súmula TCU n° 269]*

7.5.5. Ainda, em atenção ao disposto na Instrução Normativa 01/2019/SGD/ME, todas as atividades inerentes ao ciclo de vida dos serviços contratados estão incluídas na métrica de pagamento em função dos resultados e/ou produtos entregues, de forma que o CONTRATANTE não efetuará pagamentos adicionais por quaisquer atividades já incluídas no escopo desses serviços.
7.5.6. Na medição dos valores para faturamento será apurado o afastamento dos indicadores de medição de resultado em relação às metas estabelecidas. Nos casos em que o afastamento apontar o desempenho abaixo da meta exigida será calculado o valor do ajuste (desconto/glosa) a ser aplicado sobre o faturamento – de acordo com os critérios fixados para cada INDICADOR. Não há previsão de pagamentos adicionais para superação de metas.
7.5.7. Em conformidade com o disposto no ANEXO I da Instrução Normativa SGD n° 01/2019, não é admitida a cobrança retroativa de valores referentes a serviços de suporte técnico e de atualização de versões relativa ao período em que o órgão ou entidade tenha eventualmente ficado sem cobertura contratual, assim como não será admitida cobrança de valores para reativação de serviços agregados.
7.5.8. Também não será admitida a cobrança de valores relativos a serviço de correção de erros, inclusive retroativos, que devem ser corrigidos sem ônus ao(s) CONTRATANTE(S), durante o prazo de validade técnica das subscrições de uso. Caso os erros venham a ser corrigidos em versão posterior do software, essa versão deverá ser fornecida sem ônus para o CONTRATANTE.
7.5.9. O CONTRATANTE demandará os serviços de segurança de forma gradual, seguindo cronogramas de implantação, cabendo o pagamento apenas sobre os quantitativos demandados, fornecidos e efetivamente implantados/entregues.
7.5.10. Na medição dos valores para faturamento serão apurados os resultados apresentados pela CONTRATADA na execução das Ordens de Fornecimento, considerando os critérios e as metas estabelecidas. Nos casos em que essa medição apontar o desempenho abaixo da meta exigida será calculado o valor do ajuste (desconto/glosa) a ser aplicado sobre o faturamento – de acordo com os critérios fixados para cada INDICADOR de NÍVEL MÍNIMO DE SERVIÇO. Não há previsão de pagamentos adicionais para superação de metas.
7.5.11. O pagamento será efetuado mediante a apresentação da Nota Fiscal, devidamente certificada, acusando o recebimento, por parte do responsável pelo órgão solicitante.
7.5.12. O documento fiscal somente será atestado e encaminhado para pagamento após o

aceite formal da conclusão da entrega de toda a solução, o que contempla a entrega dos equipamentos e realização dos serviços de instalação, configuração, atualização e capacitação.

7.5.13. O prazo para pagamento será de no máximo 30 (trinta) dias a partir da data de sua entrega no órgão, desde que não haja impedimento legal.

8 – ESTIMATIVA DE PREÇOS DA CONTRATAÇÃO

8.1. A estimativa de preço da contratação foi realizada pela EQUIPE DE PLANEJAMENTO DA CONTRATAÇÃO para elaboração do orçamento detalhado, composta por preços unitários e fundamentada em PESQUISA DE PREÇOS realizada em conformidade com os procedimentos administrativos estabelecidos na Instrução Normativa 01/2019/SGD/ME e na Instrução Normativa nº 73/2020/SEGES/ME e suas atualizações, obtendo-se o seguinte resultado:

Solução de segurança - Backup e Firewall					
Grupo 1 - Solução de segurança - *firewall*					
Item	**Descrição do Bem ou Serviço**	**Unidade de medida**	**Quantidade**	**Valor Unitário Máximo**	**Valor Total Máximo**
1	Solução de Firewall em Appliance - Tipo 1 (Palo Alto Networks PA-460)	unidade	7	R$ 183.780,05	R$ 1.286.460,35
2	Solução de Firewall em Appliance - Tipo 2 (Palo Alto Networks PA-440)	unidade	37	R$ 55.014,76	R$ 2.035.546,12
3	Renovação de solução de Gerenciamento de Firewall Centralizado (Panorama) para 25 dispositivos	unidade	2	R$ 108.864,45	R$ 217.728,90
4	Serviço de Instalação e Configuração da Solução de Firewall Tipo 1 (item 1) - ONSITE em Campo Grande/MS	unidade	5	R$ 37.500,00	R$ 187.500,00
5	Serviço de Projeto, Instalação e Configuração da Solução de Firewall Tipo 2 (item 2) - REMOTO	unidade	38	R$ 15.350,00	R$ 583.300,00
Valor Total Estimado do Grupo 1				**R$ 4.310.535,37**	
Grupo 2 - Solução de segurança - *backup*					
Item	**Descrição do Bem ou Serviço**	**Unidade de medida**	**Quantidade**	**Valor Unitário Máximo**	**Valor Total Máximo**
6	Software de backup com licenciamento por socket, conforme descrito na especificação técnica	Licença por Socket	24	R$ 51.348,34	R$ 1.232.360,16
7	Servidor de Backup	Unidade	2	R$ 200.265,13	R$ 400.530,26
8	Serviço de Instalação e Configuração da Solução de Backup	Unidade	1	R$ 101.000,00	R$ 101.000,00

9	Serviço de Treinamento Oficial do Fabricante da Solução de Backup	Unidade	4	R$ 8.832,50	R$ 35.330,00
Valor Total Estimado do Grupo 2				**R$ 1.769.220,42**	
Valor Total Estimado (Grupo 1 + Grupo 2)				**R$ 6.079.755,79**	

8.2. Os quantitativos contemplam as estimativas dos Órgãos Gerenciador e Participantes, sendo sua distribuição e locais de entrega:

Solução de segurança - Backup e Firewall					
Grupo 1 - Solução de segurança - *firewall*					
Item	**Descrição do Bem ou Serviço**	**Unidade de medida**	**Quantidade**	**UASG**	**Município/UF de entrega**
1	Solução de Firewall em Appliance - Tipo 1 (Palo Alto Networks PA-460)	unidade	2	158132 – IFMS	Campo Grande/MS
			2	155016 – Hospital Universitário Grande Dourados	Dourados/MS
			1	158144 - IFMT	Cuiabá/MT
			2	158156 - IFAC	Rio Branco/AC
2	Solução de Firewall em Appliance - Tipo 2 (Palo Alto Networks PA-440)	unidade	10	158132 – IFMS	Campo Grande/MS
			18	158144 - IFMT	Cuiabá/MT
			7	158156 - IFAC	Rio Branco/AC

			2	158127 –IFFAR	Santa Maria/RS
3	Renovação de solução de Gerenciamento de Firewall Centralizado (Panorama) para 25 dispositivos	Unidade	1	158132 – IFMS	Campo Grande/MS
			1	158144 - IFMT	Cuiabá/MT
4	Serviço de Instalação e Configuração da Solução de Firewall Tipo 1 (item 1) - ONSITE em Campo Grande/MS	unidade	1	158132 – IFMS	Campo Grande/MS
			2	155016 – Hospital Universitário Grande Dourados	Dourados/MS
			2	158156 - IFAC	Rio Branco/AC
5	Serviço de Projeto, Instalação e Configuração da Solução de Firewall Tipo 2 (item 2) - REMOTO	unidade	10	158132 – IFMS	Campo Grande/MS
			19	158144 - IFMT	Cuiabá/MT
			7	158156 - IFAC	Rio Branco/AC
			2	158127 –IFFAR	Santa Maria/RS
Grupo 2 - Solução de segurança - *backup*					
Item	**Descrição do Bem ou Serviço**	**Unidade de medida**	**Quantidade**	**UASG**	**Município/UF de entrega**

6	Software de backup com licenciamento por socket, conforme descrito na especificação técnica	Licença por Socket	24	158132 – IFMS	Campo Grande/MS
7	Servidor de Backup	Unidade	2	158132 – IFMS	Campo Grande/MS
8	Serviço de Instalação e Configuração da Solução de Backup	Unidade	1	158132 – IFMS	Campo Grande/MS
9	Serviço de Treinamento Oficial do Fabricante da Solução de Backup	Unidade	4	158132 – IFMS	Campo Grande/MS

8.3. Os endereços de entrega e prestação dos serviços serão os seguintes:

- IFMS – Instituto Federal do Mato Grosso do Sul – Av. Ceará, 972 – Santa Fé. CEP 79021-000, Campo Grande/MS.
- Hospital Universitário da Grande Dourados – Rua Ivo Alves da Rocha, 558 – Altos do Indaiá. CEP 79823-501, Dourados/MS.
- IFMT – Instituto Federal do Mato Grosso – Av. Sen. Filinto Müller, 953 – Quilombo. CEP 78043-409, Cuiabá/MT.
- IFAC – Instituto Federal do Acre – Rua Cel. José Galdino, n° 495 – Bosque. CEP 69900-640, Rio Branco/AC.
- IFFAR – Instituto Federal Farroupilha – Alameda Santiago do Chile, 195 – nossa Sra. Das Dores. CEP 97050-685, Santa Maria/RS.

9 – ADEQUAÇÃO ORÇAMENTÁRIA E CRONOGRAMA FÍSICO-FINANCEIRO

9.1. Considerando o disposto no §2° do art. 7° do Decreto n° 7.892, de 23/01/2013, que regulamenta o Sistema de Registro de Preços, “na licitação para registro de preços não é necessário indicar a dotação orçamentária, que somente será exigida para a formalização do contrato ou outro instrumento hábil”.

10 – DA VIGÊNCIA DO CONTRATO

10.1. O CONTRATO terá vigência de 12 (doze) meses, a contar de sua assinatura.
10.2. O encerramento da vigência contratual, não interrompe a obrigação de prestação da GARANTIA TÉCNICA, por 60 meses, devendo a CONTRATADA honrá-la durante todo o período estipulado.

11 – DO REAJUSTE DE PREÇOS (quando aplicável)

11.1. Dentro do prazo de vigência do CONTRATO – mediante solicitação da CONTRATADA e por intermédio de APOSTILAMENTO – os preços contratados poderão sofrer REAJUSTE após o interregno de 01 (UM) ANO, exclusivamente para as obrigações iniciadas e concluídas após a ocorrência da anualidade, mediante aplicação do Índice de Custos de Tecnologia da Informação – ICTI, mantido pela Fundação Instituto de Pesquisa Econômica Aplicada – IPEA (http://www.ipea.gov.br/cartadeconjuntura/index.php/tag/icti/).
11.2. Nos reajustes subsequentes ao primeiro, o interregno mínimo de um ano será contado a partir dos efeitos financeiros do último reajuste.
11.3. No caso de atraso ou não divulgação do índice de reajustamento, o CONTRATANTE pagará à CONTRATADA a importância calculada pela última variação conhecida, liquidando a diferença correspondente tão logo seja divulgado o índice definitivo. Fica a CONTRATADA obrigada a apresentar memória de cálculo referente ao reajustamento de preços do valor remanescente, sempre que este ocorrer.
11.4. Nas aferições finais, o índice utilizado para reajuste será, obrigatoriamente, o definitivo. Caso o índice estabelecido para reajustamento venha a ser extinto ou de qualquer forma não possa mais ser utilizado, será adotado, em substituição, o que vier a ser determinado pela legislação então em vigor. Na ausência de previsão legal quanto ao índice substituto, as partes elegerão novo índice oficial, para reajustamento do preço do valor remanescente, por meio de TERMO ADITIVO.

12 – DOS CRITÉRIOS DE SELEÇÃO DO FORNECEDOR

12.1. Regime, Tipo e Modalidade da Licitação

12.1.1. O regime da execução dos contratos é empreitada por preço global, sendo constituída por 2 (dois) grupos e o tipo e critério de julgamento da licitação é o menor preço para a seleção da proposta mais vantajosa, utilizado para compras e serviços de modo geral e para contratação de bens e serviços de informática. De acordo com o Art. 4º do Decreto nº 5.450/2005, esta licitação deve ser realizada na modalidade de Pregão, na sua forma eletrônica, com julgamento pelo critério de menor preço.
12.1.2. A fundamentação pauta-se na premissa que a contratação de serviços baseia-se em padrões de desempenho e qualidade claramente definidos no Termo de Referência, havendo diversos fornecedores capazes de prestá-los. Caracterizando-se como “serviço comum” conforme Art. 9º, §2º do Decreto 7.174/2010 e legislação específica art.1º da Lei 10520 e§1º do art. 1° do Decreto n° 10.024/2019.
12.1.3. A prestação de serviços não envolve “dedicação exclusiva de mão de obra” - nos termos do art. 17 da IN 05/SEGES/MPDG de 26/05/2017 - uma vez que a CONTRATADA poderá compartilhar os recursos humanos e materiais disponíveis para execução simultânea de outros contratos. A prestação dos serviços também 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.

12.2 Justificativa para a Aplicação do Direito de Preferência e Margens de Preferência

12.2.1. Nos termos da legislação vigente, conforme previsão em Edital, nas aquisições de bens e serviços de informática e automação definidos pela Lei n° 8.248, de 1991, será assegurado o direito de preferência conforme procedimento estabelecido nos artigos 5° e 8° do Decreto n° 7.174, de 2010. Sendo que as licitantes qualificadas como microempresas ou empresas de pequeno porte que fizerem jus ao direito de preferência terão prioridade no exercício desse benefício em relação às médias e às grandes empresas na mesma situação.
12.2.2. Não se aplica o tratamento diferenciado e simplificado para as microempresas e empresas de pequeno porte quando não for vantajoso para administração pública ou representar prejuízo ao objeto, conforme preconiza o inciso II, Art. 10, do Decreto nº 8.538 de 6 de outubro de 2015. Assim, tal tratamento não será aplicado a este processo licitatório, uma vez que a reserva de uma fração da quantidade dos itens poderá ocasionar falhas durante ou após a implantação da solução, conforme mencionado no tópico 3.4 referente ao parcelamento da solução.

12.3 Critérios de Qualificação Técnica para a Habilitação

12.3.1. As exigências de habilitação jurídica e de regularidade fiscal e trabalhista são as usuais para a generalidade dos objetos, conforme disciplinado no edital.
12.3.2. Os critérios de qualificação econômica a serem atendidos pelo fornecedor estão previstos no edital.
12.3.3. O critério de qualificação técnica a ser atendido pelo fornecedor será a comprovação de capacidade técnica, que ocorrerá mediante a apresentação de um ou mais Atestado(s) de Capacidade Técnica que comprove(m) sua aptidão para prover produtos de igual natureza ou compatível ao objeto especificado neste Termo de Referência, emitido ou firmado com pessoa jurídica de direito público ou privado, que comprove o fornecimento dos itens especificado.
12.3.4 A critério da contratante, nas situações em que julgar necessário, poderão ser realizadas inspeções e diligências com a finalidade de apoiar/comprovar as informações contidas em Atestado de Capacidade Técnica entregues pelos licitantes – nos termos do §3°, do art. 43, da Lei nº 8.666, de 21 de junho de 1993. Assim como poderão ser solicitadas cópias de documentos complementares como contratos, notas fiscais e notas de empenho.
12.3.5. A recusa do emitente do ATESTADO em prestar esclarecimentos e/ou fornecer documentos comprobatórios, ou sofrer diligências, ou a constatada inexatidão das informações atestadas, desconstituirá o documento – o que poderá, inclusive, configurar prática criminosa – ensejando comunicação ao Ministério Público Federal e abertura de Processo Administrativo Disciplinar, conforme o caso, para fins de apuração de responsabilidades.
12.3.6. No caso de atestados emitidos por empresas privadas, não serão válidos aqueles emitidos por empresas pertencentes ao mesmo grupo empresarial da empresa proponente. São consideradas como pertencentes ao mesmo grupo empresarial as empresas controladas ou controladoras do licitante proponente, ou que tenha pelo menos uma mesma pessoa física ou jurídica que seja sócia ou possua vínculo com a empresa emitente ou empresa licitante.
12.3.7 Ainda, com respeito aos ATESTADOS DE CAPACIDADE TÉCNICA:
a) Devem ser da mesma natureza do objeto da licitação;

b) Poderão ser fornecidos por pessoas jurídicas de direito público ou privado, com correta identificação do emissor;
c) Devem ser emitidos sem rasuras, acréscimos ou entrelinhas;
d) Devem estar assinados por quem tenha competência para expedi-los, tais como representantes legais do órgão/empresa, diretores, gerentes e representantes formais das áreas técnica ou demandante (sem se limitar a esses);
e) Devem conter identificação clara e suficiente do Atestante; e
f) Devem apresentar redação clara, sucinta e objetiva que demonstre de forma inequívoca o atendimento ao objeto da requisição.

13 – DA EQUIPE DE PLANEJAMENTO DA CONTRATAÇÃO E DA APROVAÇÃO

13.1. A Equipe de Planejamento da Contratação foi instituída pela Portaria nº 582, de 30 de maio de 2022.
13.2. Conforme o §6º do art. 12 da IN SGD/ME nº 01, de 2019, o Termo de Referência ou Projeto Básico será assinado pela Equipe de Planejamento da Contratação e pela autoridade máxima da Área de TIC e aprovado pela autoridade competente.

Matheus Jardim Guerreiro da Silva - Integrante Requisitante
Helder Coelho Silva - Integrante Técnico
Thassiany Cuellar do Nascimento - Integrante Administrativo
Carlitos Fioravante Vieira de Oliveira - Autoridade Máxima da Área de TIC

Campo Grande/MS, 15 de agosto de 2022.

Aprovo,

Elaine Borges Monteiro Cassiano

Campo Grande/MS, 17 de agosto de 2022.

APÊNDICE A – ESPECIFICAÇÃO TÉCNICA

A solução ofertada deve atender a todos os requisitos técnicos descritos abaixo:

I. Especificações básicas comuns para os Firewalls Tipo 1 e Tipo 2 (Grupo 1 - item 1 e item 2):

1. Descrição:

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

1.2. A solução de Next Generation Firewall (NGFW) deverá ser compatível com a Solução de Gerenciamento Centralizado Panorama Virtual Palo Alto Networks existente no órgão;

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

2. Características Gerais:

2.1. A solução deve consistir em appliance de proteção de rede com funcionalidades de Next Generation Firewall (NGFW);

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

2.3. 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;

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

2.5. 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;

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

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

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

2.8.1. Suporte a 4094 VLAN Tags 802;1q;

2.8.2. Agregação de links 802;3ad e LACP;

2.8.3. Policy based routing ou policy based forwarding;

2.8.4. Roteamento multicast (PIM-SM);

2.8.5. DHCP Relay;

2.8.6. DHCP Server;

2.8.7. Jumbo Frames;

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

2.9. Suportar sub-interfaces ethernet lógicas;

2.9.1. Suporte a, no mínimo, 2 (dois) roteadores virtuais na mesma instância de firewall;

2.10. O firewall deve ter a capacidade de testar o funcionamento de rotas estáticas e rota default com a definição de um endereço IP de destino que deve estar comunicável

através de uma rota. Caso haja falha na comunicação o firewall deve ter a capacidade de usar rota alternativa para estabelecer a comunicação;

2.11. Deve suportar os seguintes tipos de NAT:
- 2.11.1. Nat dinâmico (Many-to-1);
- 2.11.2. Nat dinâmico (Many-to-Many);
- 2.11.3. Nat estático (1-to-1);
- 2.11.4. NAT estático (Many-to-Many);
- 2.11.5. Nat estático bidirecional 1-to-1;
- 2.11.6. Tradução de porta (PAT);
- 2.11.7. NAT de Origem;
- 2.11.8. NAT de Destino;
- 2.11.9. Suportar NAT de Origem e NAT de Destino simultaneamente;
- 2.11.10. Deve implementar Network Prefix Translation (NPTv6), prevenindo problemas de roteamento assimétrico;

2.12. Deve implementar o protocolo ECMP;
- 2.12.1. Deve implementar balanceamento de link por hash do IP de origem;
- 2.12.2. Deve implementar balanceamento de link por hash do IP de origem e destino;
- 2.12.3. Deve implementar balanceamento de link através do método round-robin;
- 2.12.4. Deve implementar balanceamento de link por peso. Nesta opção deve ser possível definir o percentual de tráfego que será escoado por cada um dos links. Deve suportar o balanceamento de, no mínimo, quatro links;
- 2.12.5. Deve implementar balanceamento de link através de políticas por usuário e grupos de usuários do LDAP/AD;
- 2.12.6. Deve implementar balanceamento de link através de políticas por aplicação e porta de destino;
- 2.12.7. Deve implementar o protocolo Link Layer Dicovery (LLDP), permitindo que o appliance e outros ativos da rede se comuniquem para identificação da topologia da rede em que estão conectados e a função dos mesmos facilitando o processo de throubleshooting. As informações aprendidas e armazenadas pelo appliance devem ser acessíveis via SNMP;
- 2.12.8. Enviar log para sistemas de monitoração externos, simultaneamente;
- 2.12.9. Deve haver a opção de enviar logs para os sistemas de monitoração externos via protocolo TCP e SSL;
- 2.12.10. Deve permitir configurar certificado caso necessário para autenticação no sistema de monitoração externo de logs;
- 2.12.11. Proteção contra anti-spoofing;
- 2.12.12. Deve permitir bloquear sessões TCP que usarem variações do 3-way hand-shake, como 4 way e 5 way split hand-shake, prevenindo desta forma possíveis tráfegos maliciosos;
- 2.12.13. Deve permitir bloquear conexões que contenham dados no payload de pacotes TCP-SYN e SYN-ACK durante o three-way handshake;
- 2.12.14. Deve exibir nos logs de tráfego o motivo para o término da sessão no firewall, incluindo sessões finalizadas onde houver de-criptografia de SSL e SSH;
- 2.12.15. Para IPv4, deve suportar roteamento estático e dinâmico (RIPv2, BGP e OSPFv2);
- 2.12.16. Para IPv6, deve suportar roteamento estático e dinâmico (OSPFv3);
- 2.12.17. Suportar a OSPF *graceful restart*;
- 2.12.18. Deve suportar o protocolo MP-BGP (Multiprotocol BGP) permitindo que o firewall possa anunciar rotas multicast para IPv4 e rotas unicast para IPv6;
- 2.12.19. Suportar no mínimo as seguintes funcionalidades em IPv6: SLAAC (address auto configuration), NAT64, Identificação de usuários a partir do LDAP/AD, Captive Portal, IPv6 over IPv4 IPSec, Regras de proteção contra DoS (Denial of Service), De-criptografia SSL e SSH, PBF (Policy Based Forwarding), QoS, DHCPv6 Relay, IPSEc, VPN SSL, Ativo/Ativo, Ativo/Passivo, SNMP, NTP,

SYSLOG, DNS, Neighbor Discovery (ND), Recursive DNS Server (RDNSS), DNS Search List (DNSSL) e controle de aplicação;

2.12.20. Os dispositivos de proteção devem ter a capacidade de operar de forma simultânea em uma única instância de firewall, mediante o uso de suas interfaces físicas nos seguintes modos: Modo sniffer (monitoramento e análise do tráfego de rede), camada 2 (l2) e camada 3 (l3);

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

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

2.12.20.3. Modo Camada – 3 (L3), para inspeção de dados em linha e ter visibilidade e controle do tráfego em nível de aplicação operando como default gateway das redes protegidas.

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

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

2.13.1. Em modo transparente;

2.13.2. Em layer 3.

2.14. A configuração em alta disponibilidade deve sincronizar:

2.14.1. Sessões;

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

2.14.3. Certificados de-criptografados;

2.14.4. Associações de Segurança das VPNs;

2.14.5. Tabelas FIB;

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

2.15. As funcionalidades de controle de aplicações, VPN IPSec e SSL, QOS, SSL e SSH Decryption e protocolos de roteamento dinâmico devem operar em caráter permanente, podendo ser utilizadas por tempo indeterminado, mesmo que não subsista o direito de receber atualizações ou que não haja contrato de garantia de software com o fabricante.

3. CONTROLE POR POLÍTICA DE FIREWALL:

3.1. Deverá suportar controles por zona de segurança;

3.2. Controles de políticas por porta e protocolo;

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

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

3.5. Deve suportar a consulta a fontes externas de endereços IP, domínios e URLs podendo ser adicionados nas políticas de firewall para bloqueio ou permissão do tráfego;

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

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

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

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

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

3.9. Deve de-criptografar tráfego Inbound e Outbound em conexões negociadas com TLS 1.2 e 1.3;

3.10. Deve de-criptografar sites e aplicações que utilizam certificados ECC, incluindo Elliptical Curve Digital Signature Algorithm (ECDSA);
3.11. Controle de inspeção e de-criptografia de SSH por política;
3.12. 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;
3.13. 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);
3.13.1. É permitido uso de appliance externo, específico para a de-criptografia de (SSL e TLS), com espelhamento de cópia do tráfego de-criptografado tanto para o firewall, quanto para as soluções de análise;
3.14. Bloqueios dos seguintes tipos de arquivos: APK, BAT, CAB, CLASS, CHM, CPL, DLL, EXE, JAR, JOB, JSE, HLP, HTA, MSI, MSP, OCX, PIF, PRG, RAR, REG, SHB, SHSVB, VBE, VBS, WSF, WSH, TORRENT, 7Z;
3.15. Traffic shaping QoS baseado em Políticas (Prioridade, Garantia e Máximo)
3.16. QoS baseado em políticas para marcação de pacotes (diffserv marking), inclusive por aplicações;
3.17. Suporte a objetos e regras IPV6;
3.18. Suporte a objetos e regras multicast;
3.19. Deve suportar no mínimo três tipos de negação de tráfego nas políticas de firewall: Drop sem notificação do bloqueio ao usuário, Drop com opção de envio de ICMP Unreachable para máquina de origem do tráfego, TCP-Reset para o client, TCP-Reset para o server ou para os dois lados da conexão;
3.20. Suportar a atribuição de agendamento das políticas com o objetivo de habilitar e desabilitar políticas em horários pré-definidos automaticamente.

4. CONTROLE DE APLICAÇÕES

4.1. Os dispositivos de proteção de rede deverão possuir a capacidade de reconhecer aplicações, independente de porta e protocolo, com as seguintes funcionalidades:
4.1.1. Deve ser possível a liberação e bloqueio somente de aplicações sem a necessidade de liberação de portas e protocolos;
4.1.2. Reconhecer pelo menos 3.500 aplicações diferentes, incluindo, mas não limitado: a tráfego relacionado a peer-to-peer, redes sociais, acesso remoto, update de software, protocolos de rede, voip, áudio, vídeo, proxy, mensageiros instantâneos, compartilhamento de arquivos, e-mail;
4.1.3. Reconhecer pelo menos as seguintes aplicações: bittorrent, gnutella, skype, facebook, linked-in, twitter, citrix, logmein, teamviewer, ms-rdp, vnc, gmail, youtube, http-proxy, http-tunnel, facebook chat, gmail chat, whatsapp, whatsapp-file-transfer, whatsapp-voice, 4shared, dropbox, dropbox-sharing, dropbox-upload, dropbox-download, google drive, skydrive, db2, mysql, oracle, active directory, kerberos, ldap, radius, itunes, dhcp, ftp, dns, wins, msrpc, ntp, snmp, rpc over http, gotomeeting, webex, webex-file-sharing, webex-uploading, webex-downloading, evernote, google-docs, ms-office365, ms-office365-teams, ms-office365-sharepoint, etc;
4.1.4. 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;
4.1.5. Deve aplicar heurística a fim de detectar aplicações através de análise comportamental do tráfego observado, incluindo, mas não limitado a Encrypted Bittorrent e aplicações VOIP que utilizam criptografia proprietária;

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

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

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

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

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

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

4.1.12. Atualizar a base de assinaturas de aplicações automaticamente;

4.1.13. Reconhecer aplicações em IPv6;

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

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

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

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

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

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

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

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

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

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

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

4.1.24. Deve permitir criar filtro na tabela de regras de segurança para exibir somente:
- 4.1.24.1. Regras que permitem passagem de tráfego baseado na porta e não por aplicação, exibindo quais aplicações estão trafegando nas mesmas, o volume em bytes trafegado por cada a aplicação por, pelo menos, os últimos 30 dias e o primeiro e último registro de log de cada aplicação trafegada por esta determinada regra;
- 4.1.24.2. Aplicações permitidas em regras de forma desnecessária, pois não há tráfego da mesma na determinada regra;
- 4.1.24.3. Regras de segurança onde não houve passagem de tráfego nos últimos 90 dias;

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

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

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

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

4.1.29. Deve ser possível a criação de grupos estáticos de aplicações e grupos dinâmicos de aplicações baseados em características das aplicações como:
- 4.1.29.1. Tecnologia utilizada nas aplicações (Client-Server, Browse Based, Network Protocol, etc);
- 4.1.29.2. Nível de risco da aplicação;
- 4.1.29.3. Categoria e sub-categoria de aplicações;
- 4.1.29.4. Aplicações que usem técnicas evasivas, utilizadas por malwares, como transferência de arquivos e/ou uso excessivo de banda, etc.

5. PREVENÇÃO DE AMEAÇAS

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

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

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

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

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

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

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

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

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

5.10. Deve permitir o bloqueio de vulnerabilidades;

5.11. Deve permitir o bloqueio de exploits conhecidos;

5.12. Deve incluir proteção contra ataques de negação de serviços;
5.13. Deve suportar a inspeção e criação de regras de proteção de DOS e QOS para o conteúdo de tráfego tunelado pelo protocolo GRE;
5.14. Deverá possuir os seguintes mecanismos de inspeção de IPS:
  5.14.1. Análise de padrões de estado de conexões;
  5.14.2. Análise de decodificação de protocolo;
  5.14.3. Análise para detecção de anomalias de protocolo;
  5.14.4. Análise heurística;
  5.14.5. IP Defragmentation;
  5.14.6. Remontagem de pacotes de TCP;
  5.14.7. Bloqueio de pacotes malformados;
5.15. Ser imune e capaz de impedir ataques básicos como: Synflood, ICMPflood, UDPfloof, etc;
5.16. Detectar e bloquear a origem de portscans com possibilidade de criar exceções para endereços IPs de ferramentas de monitoramento da organização;
5.17. Bloquear ataques efetuados por worms conhecidos, permitindo ao administrador acrescentar novos padrões;
5.18. Suportar os seguintes mecanismos de inspeção contra ameaças de rede: análise de padrões de estado de conexões, análise de decodificação de protocolo, análise para detecção de anomalias de protocolo, análise heurística, IP Defragmentation, remontagem de pacotes de TCP e bloqueio de pacotes malformados;
5.19. Possuir assinaturas específicas para a mitigação de ataques DoS e DDoS;
5.20. Possuir assinaturas para bloqueio de ataques de buffer overflow;
5.21. Deverá possibilitar a criação de assinaturas customizadas pela interface gráfica do produto;
5.22. Deve permitir usar operadores de negação na criação de assinaturas customizadas de IPS e anti-spyware, permitindo a criação de exceções com granularidade nas configurações;
5.23. Permitir o bloqueio de vírus e spywares em, pelo menos, os seguintes protocolos: HTTP, FTP, SMB, SMTP e POP3;
  5.23.1. É permitido uso de appliance externo (antivírus de rede), para o bloqueio de vírus e spywares em protocolo SMB de forma a conter malwares se espalhando horizontalmente pela rede;
5.24. Suportar bloqueio de arquivos por tipo;
5.25. Identificar e bloquear comunicação com botnets;
5.26. Deve suportar várias técnicas de prevenção, incluindo Drop e tcp-rst (Cliente, Servidor e ambos);
5.27. Deve suportar referência cruzada com CVE;
5.28. Registrar na console de monitoração as seguintes informações sobre ameaças identificadas:
  5.28.1. O nome da assinatura ou do ataque, aplicação, usuário, origem e o destino da comunicação, além da ação tomada pelo dispositivo;
5.29. Deve suportar a captura de pacotes (PCAP), por assinatura de IPS e Antispyware;
5.30. Deve permitir que na captura de pacotes por assinaturas de IPS e Antispyware seja definido o número de pacotes a serem capturados. Esta captura deve permitir selecionar, no mínimo, 50 pacotes;
5.31. Deve possuir a função resolução de endereços via DNS, para que conexões com destino a domínios maliciosos sejam resolvidas pelo Firewall com endereços (IPv4 e IPv6), previamente definidos;
5.32. Permitir o bloqueio de vírus, pelo menos, nos seguintes protocolos: HTTP, FTP, SMB, SMTP e POP3;
5.33. Os eventos devem identificar o país de onde partiu a ameaça;
5.34. Deve incluir proteção contra vírus em conteúdo HTML e Java script, software espião (spyware) e worms;

5.35. Proteção contra downloads involuntários usando HTTP de arquivos executáveis; maliciosos;
5.36. Rastreamento de vírus em pdf;
5.37. Deve permitir a inspeção em arquivos comprimidos que utilizam o algoritmo deflate (zip, gzip, etc;);
5.38. Deve ser possível a configuração de diferentes políticas de controle de ameaças e ataques baseado em políticas do firewall considerando Usuários, Grupos de usuários, origem, destino, zonas de segurança, etc, ou seja, cada regra de firewall poderá ter uma configuração diferentes de IPS, sendo essas políticas por Usuários, Grupos de usuário, origem, destino, zonas de segurança;
5.39. 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);
5.40. A solução deve mostrar nos logs as seguintes informações sobre domínios DGA:
5.40.1. Domínio suspeito identificado;
5.40.2. ID de assinatura de detecção;
5.40.3. Usuário logado na estação/servidor que originou o tráfego;
5.40.4. Aplicação;
5.40.5. Porta de destino;
5.40.6. IP de origem;
5.40.7. IP de destino;
5.40.8. Horário;
5.40.9. Ação do firewall;
5.40.10. Severidade;
5.41. 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;
5.42. A análise automática deve incluir, no mínimo, as seguintes características:
5.42.1. Padrões de consulta;
5.42.2. Entropia;
5.42.3. Análise de frequência n-gram de domínios;
5.42.4. Taxa de consultas.

6. ANÁLISE DE MALWARES MODERNOS

6.1. Devido aos Malwares hoje em dia serem muito dinâmicos e um antivírus comum reativo não ser capaz de detectar os mesmos com a mesma velocidade que suas variações são criadas, a solução ofertada dever possuir funcionalidades para análise de Malwares não conhecidos incluídas na própria ferramenta ou entregue com composição com outro fabricante;
6.2. O dispositivo de proteção deve ser capaz de enviar arquivos trafegados de forma automática para análise "In Cloud" ou local, onde o arquivo será executado e simulado em ambiente controlado;
6.3. Selecionar através de políticas granulares quais tipos de arquivos sofrerão esta análise incluindo, mas não limitado a: endereço IP de origem/destino, usuário/grupo do AD/LDAP, aplicação, porta, URL/categoria de URL de destino, tipo de arquivo e todas estas opções simultaneamente;
6.4. Deve possuir a capacidade de diferenciar arquivos analisados em pelo menos três categorias: malicioso, não malicioso e arquivos não maliciosos, mas com características indesejáveis como softwares que deixa o sistema operacional lento, que alteram parâmetros do sistema, etc;
6.5. Suportar a análise com pelo menos 100 (cem) tipos de comportamentos maliciosos para a análise da ameaça não conhecida;
6.6. Suportar a análise de arquivos maliciosos em ambiente controlado com, no mínimo, sistema operacional Windows 10;

6.7. Deve suportar a monitoração de arquivos trafegados na internet (HTTPs, FTP, HTTP, SMTP) como também arquivos trafegados internamente entre servidores de arquivos usando SMB em todos os modos de implementação: sniffer, transparente e L3;

6.8. A solução deve possuir a capacidade de analisar em sand-box links (http e https) presentes no corpo de e-mails trafegados em SMTP e POP3. Deve ser gerado um relatório caso a abertura do link pela sand-box o identifique como site hospedeiro de exploits;

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

6.10. Para ameaças trafegadas em protocolo SMTP e POP3, a solução deve ter a capacidade de mostrar nos relatórios o remetente, destinatário e assunto dos e-mails permitindo identificação ágil do usuário vítima do ataque;

6.11. O sistema de análise “In Cloud” ou local deve prover informações sobre as ações do Malware na máquina infectada, informações sobre quais aplicações são utilizadas para causar/propagar a infecção, detectar aplicações não confiáveis utilizadas pelo Malware, gerar assinaturas de Antivírus e Anti-spyware automaticamente, definir URLs não confiáveis utilizadas pelo novo Malware e prover informações sobre o usuário infectado (seu endereço ip e seu login de rede);

6.12. O sistema automático de análise "In Cloud" ou local deve emitir relatório com identificação de quais soluções de antivírus existentes no mercado possuem assinaturas para bloquear o malware;

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

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

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

6.16. Deve permitir informar ao fabricante quanto a suspeita de ocorrências de falso-positivo e falso-negativo na análise de malwares de dia Zero a partir da própria interface de gerência;

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

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

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

6.20. 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;

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

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

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

7. FILTRO DE URL

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

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

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

7.1.3. Deverá incluir a capacidade de criação de políticas baseadas na visibilidade e controle de quem está utilizando quais URLs através da integração com serviços de diretório, autenticação via ldap, Active Directory, E-directory e base de dados local;
7.1.4. Permite popular todos os logs de URL com as informações dos usuários conforme descrito na integração com serviços de diretório;
7.1.5. Suporta a capacidade de criação de políticas baseadas no controle por URL e Categoria de URL;
7.1.6. 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;
7.1.7. Suporta base ou cache de URLs local no appliance, evitando delay de comunicação/validação das URLs;
7.1.8. Possui pelo menos 60 categorias de URLs;
7.1.9. Deve classificar o nível de risco de URLs em, pelo menos, três níveis: baixo, médio e alto;
7.1.10. Deve possuir categoria específica para classificar domínios recém registrados (com menos de 32 dias);
7.1.11. A solução deve ter a capacidade de classificar sites em mais de uma categoria, de acordo com a necessidade;
7.1.12. Suporta a criação categorias de URLs customizadas;
7.1.13. Suporta a exclusão de URLs do bloqueio, por categoria;
7.1.14. Permite a customização de página de bloqueio;
7.1.15. 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;
7.1.16. Deve permitir bloquear o acesso do usuário caso o mesmo tente fazer o envio de suas credenciais em sites classificados como phishing pelo filtro de URL da solução;
7.1.17. 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);
7.1.18. Suporta a inclusão nos logs do produto de informações das atividades dos usuários;
7.1.19. Deve salvar nos logs as informações dos seguintes campos do cabeçalho HTTP nos acessos a URLs: UserAgent, Referer, e X-Forwarded For.
7.1.20. A solução deverá implementar uma análise avançada de URL em tempo real enviando a URL para um serviço de análise em cloud e não somente fazer a consulta em base local;
7.1.21. A filtragem de URL em tempo real deverá ser ativada por meio do perfil de filtragem de URL;
7.1.22. Deverá ser exibido nos logs as URLs analisadas por meio da categoria detecção em tempo real com como o tipo de ameaça.

8. IDENTIFICAÇÃO DE USUÁRIOS

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

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

8.4. Deve implementar a criação de políticas de segurança baseada em atributos específicos do Radius, incluindo, mas não limitado a: baseado no sistema operacional do usuário remoto exigir autenticação padrão Windows e on-time password (OTP) para usuários Android;

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

8.5.1. Deve suportar o recebimento eventos de autenticação de controladoras wireless, dispositivos 802;1x e soluções NAC via syslog, para a identificação de endereços IP e usuários;

8.6. Deve permitir o controle, sem instalação de cliente de software, em equipamentos que solicitem saída a internet para que antes de iniciar a navegação, expanda-se um portal de autenticação residente no firewall (Captive Portal);

8.7. Suporte a autenticação Kerberos;

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

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

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

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

8.12. O firewall deve operar/suportar Security Assertion Markup Language (SAML) 2;0, com single sign-on e single logout para as funcionalidades de Captive Portal e VPN SSL (client to server), permitindo login único e interativo para fornecer acesso automático a serviços autenticados, internos e externos à organização;

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

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

9. QOS

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

9.2. Suportar a criação de políticas de QoS por:

9.2.1. Endereço de origem

9.2.2. Endereço de destino

9.2.3. Por usuário e grupo do LDAP/AD;

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

9.2.5. Por porta;

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

9.3.1. Banda Garantida

9.3.2. Banda Máxima

9.3.3. Fila de Prioridade;

9.4. Suportar priorização RealTime de protocolos de voz (VOIP) como H;323, SIP, SCCP, MGCP e aplicações como Skype;
9.5. Suportar marcação de pacotes Diffserv, inclusive por aplicação;
9.6. Deve implementar QOS (traffic-shapping), para pacotes marcados por outros ativos na rede (DSCP); A priorização e limitação do tráfego deve ser efetuada nos dois sentidos da conexão (inboud e outbound);
9.7. Disponibilizar estatísticas RealTime para classes de QoS;
9.8. Deve suportar QOS (traffic-shapping), em interface agregadas;
9.9. Deverá permitir o monitoramento do uso que as aplicações fazem por bytes, sessões e por usuário.

10. FILTRO DE DADOS

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

11. Geolocalização

11.1. Suportar a criação de políticas por Geolocalização, permitindo o tráfego de determinado País/Países sejam bloqueados;
11.2. Deve possibilitar a visualização dos países de origem e destino nos logs dos acessos;
11.3. Deve permitir visualizar nos logs e criar políticas para liberar e bloquear tráfego de países por: tipo de arquivo, aplicação e categoria de URL;
11.4. Deve possibilitar a criação de regiões geográficas pela interface gráfica e criar políticas utilizando as mesmas.

12. VPN

12.1. Suportar VPN Site-to-Site e Cliente-To-Site;
12.2. Suportar IPSec VPN;
12.3. Suportar SSL VPN;
12.4. A VPN IPSEc deve suportar:
  12.4.1. 3DES;
  12.4.2. Autenticação MD5 e SHA-1;
  12.4.3. Diffie-Hellman Group 1, Group 2, Group 5 e Group 14;
  12.4.4. Algoritmo Internet Key Exchange (IKEv1 e v2);
  12.4.5. AES 128, 192 e 256 (Advanced Encryption Standard)
  12.4.6. Autenticação via certificado IKE PKI;
12.5. Deve possuir interoperabilidade com os seguintes fabricantes:
  12.5.1. Cisco;
  12.5.2. Checkpoint;
  12.5.3. Juniper;
  12.5.4. Palo Alto Networks;
  12.5.5. Fortinet;
  12.5.6. Sonic Wall;

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

12.7. A VPN SSL deve suportar:

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

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

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

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

12.7.5. Deve permitir a criação de rotas de acesso e faixas de endereços IP atribuídas a clientes remotos de VPN de forma customizada por usuário AD/LDAP e grupo de usuário AD/LDAP;

12.7.6. Deve permitir que todo o tráfego dos usuários remotos de VPN seja escoado para dentro do túnel de VPN, impedindo comunicação direta com dispositivos locais como proxies;

12.7.7. Atribuição de DNS nos clientes remotos de VPN;

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

12.7.9. 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;

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

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

12.7.12. Deve exibir mensagens de notificação customizada toda vez que um usuário remoto se conectar a VPN. Deve permitir que o usuário desabilite a exibição da mensagem nas conexões seguintes;

12.7.13. Deve avisar ao usuário remoto de VPN quanto a proximidade da expiração de senha LDAP. Deve permitir também a customização da mensagem com informações relevantes para o usuário;

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

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

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

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

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

12.7.19. Permite estabelecer um túnel VPN client-to-site do cliente a plataforma de segurança, fornecendo uma solução de single-sign-on aos usuários, integrando-se com as ferramentas de Windows-logon;

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

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

12.7.22. 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;

12.7.23. O agente deverá comunicar-se com o portal para determinar as políticas de segurança do usuário,
12.7.24. Deve permitir que a conexão com a VPN SSL seja estabelecida das seguintes formas:
12.7.24.1. Antes do usuário autenticar na estação;
12.7.24.2. Após autenticação do usuário na estação;
12.7.24.3. Sob demanda do usuário;
12.7.25. Deve manter uma conexão segura com o portal durante a sessão;
12.7.26. O agente de VPN SSL client-to-site deve ser compatível com pelo menos: Vista Windows 7, Windows 8, Mac OSx e Chrome OS;
12.7.27. O portal de VPN deve enviar ao cliente remoto, a lista de gateways de VPN ativos para estabelecimento da conexão, os quais devem poder ser administrados centralmente;
12.7.28. Deve haver a opção do cliente remoto escolher manualmente o gateway de VPN e de forma automática através da melhor rota entre os gateways disponíveis com base no tempo de resposta mais rápido;
12.7.29. Deve possuir a capacidade de identificar se a origem da conexão de VPN é externa ou interna.

13. AVALIAÇÃO DE BOAS PRÁTICAS

13.1. A solução deverá possuir relatório de avaliação de boas práticas por meio de análise das configurações atuais;
13.2. O relatório de boas práticas deverá mostrar o estado atual da solução e a adoção de práticas recomendadas de segurança com sugestões de adequações específicas alinhadas com práticas recomendadas;
13.3. Deverá mostrar onde melhorar a postura de segurança e definir uma linha de base para comparação posterior, fornecendo links para documentação técnica que mostra como fazer o ajuste das configurações das recomendações;
13.4. Além de mostrar um comparativo de boas práticas das configurações atuais e posteriores o relatório deverá incluir na comparação como está o grau de boas práticas adotado por instituições do mesmo setor de atuação;
13.5. O relatório deverá possuir avaliação de melhores práticas recomendadas com base no CIS (Critical Security Controls) e do NIST Security Controls (National Institute of Standards and Technology) sobre as configurações atuais da solução, identificando os riscos e fornecendo recomendações. Exemplo: A solução deverá apontar quais são as configurações que deverão ser ajustadas e indicar local com exemplo de configuração a ser realizada para melhorar a adoção e elevar o grau de segurança;
13.6. A avaliação de práticas recomendadas deverá mostrar a adoção de recursos de segurança como por exemplo a porcentagem de adoção de regras por usuários e por aplicações;
13.7. Deverá mostrar informações de adoção da solução, apontando configurações individuais para verificar como os recursos de segurança estão sendo aproveitados. Exemplo: Análise da base de regras para identificar se as mesmas estão sendo aproveitadas e se são relevantes;
13.8. O relatório poderá ser emitido diretamente na solução ou por meio de portal WEB do fabricante da solução.

14. OTIMIZAÇÃO DE POLÍTICAS DE FIREWALL

14.1. Deverá ser fornecido junto na solução ou em conjunto com a mesma a funcionalidade de otimização de políticas de firewall para possibilitar visibilidade, controle e habilitar aplicações em regras com políticas de segurança;
14.2. Deverá ser possível identificar regras baseadas em portas para que o administrador possa convertê-las em regras baseadas em aplicações que permita o tráfego e a

inclusão de aplicações em regras existentes sem comprometer a disponibilidade, bem como identificar regras configuradas com aplicações não utilizadas.

14.3. A conversão de regras baseadas em portas em regras baseadas em aplicações deverá permitir a inclusão de aplicações que se deseja permitir em uma lista de permissões e negar acesso a todos as outras aplicações;

15. GARANTIA

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

15.2. Garantia e suporte de 60 (sessenta) meses com envio de peças/equipamentos de reposição em até 3 dias úteis.

15.3. Garantia e suporte 24x7 do fabricante para a solução de software ofertada pelo período mínimo de 60 (sessenta) meses, incluindo a evolução para novas versões.

II. Especificações específicas para a solução de Firewall em Appliance - Tipo 1 (Grupo 1 - item 1):

1. A plataforma de segurança deve possuir a capacidade e as características abaixo, por equipamento:
   1.1. Throughput de 4Gbps com a funcionalidade de controle de aplicação habilitada para todas as assinaturas que o fabricante possuir;
   1.2. Throughput de 2Gbps com as seguintes funcionalidades habilitadas simultaneamente para todas as assinaturas que a plataforma de segurança possuir devidamente ativadas e atuantes: Controle de Aplicação, IPS, Antivírus, Antispyware e Anti-malware;
   1.3. Os throughputs devem ser comprovados por documento de domínio público do fabricante. A ausência de tais documentos comprobatórios reservará ao órgão o direito de aferir a performance dos equipamentos em bancada, assim como atendimento de todas as funcionalidades especificadas neste edital. Caso seja comprovado o não atendimento das especificações mínimas nos testes de bancada, serão considerados inabilitados e sujeitos às sanções previstas em lei;
   1.4. Os documentos públicos devem comprovar os throughputs aferidos com tráfego HTTP ou blend de protocolos definidos pelo fabricante como misto de aplicações;
   1.5. Suporte a, no mínimo, 300.000 de conexões simultâneas;
   1.6. Suporte a, no mínimo, 60.000 novas conexões HTTP por segundo;
   1.7. Deve ser entregue com 01 (uma) fonte de alimentação e permitir uso de fonte redundante futura interna ou externa ao equipamento 120/240 AC ou DC;
   1.8. No mínimo, 08 (oito) interfaces de rede 1 Gbps em portas cobre RJ45;
   1.9. 1 (uma) interface de rede 1 Gbps dedicada para gerenciamento;
   1.10. 1 (uma) interface do tipo console ou similar;
   1.11. Suporte a, no mínimo, 30 (trinta) zonas de segurança;
   1.12. Estar licenciada para suportar sem o uso de licença, 1.000 (mil) clientes de VPN SSL simultâneos;
   1.13. Estar licenciada para ou suportar sem o uso de licença, 200 (duzentos) túneis de VPN IPSEC simultâneos;
2. 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;

III. Especificações específicas para a solução de Firewall em Appliance - Tipo 2 (Grupo 1 - item 2):

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

1.1. Throughput de 2Gbps com a funcionalidade de controle de aplicação habilitada para todas as assinaturas que o fabricante possuir;
1.2. Throughput de 1Gbps com as seguintes funcionalidades habilitadas simultaneamente para todas as assinaturas que a plataforma de segurança possuir devidamente ativadas e atuantes: Controle de Aplicação, IPS, Antivírus, Antispyware e Anti-malware;
1.3. 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;
1.4. Os documentos públicos devem comprovar os throughputs aferidos com tráfego HTTP ou blend de protocolos definidos pelo fabricante como misto de aplicações;
1.5. Suporte a, no mínimo, 150.000 de conexões simultâneas;
1.6. Suporte a, no mínimo, 30.000 novas conexões HTTP por segundo;
1.7. Deve ser entregue com 01 (uma) fonte de alimentação e permitir uso de fonte redundante futura interna ou externa ao equipamento 120/240 AC ou DC;
1.8. No mínimo, 08 (oito) interfaces de rede 1 Gbps em portas cobre RJ45;
1.9. 1 (uma) interface de rede 1 Gbps dedicada para gerenciamento;
1.10. 1 (uma) interface do tipo console ou similar;
1.11. Suporte a, no mínimo, 30 (trinta) zonas de segurança;
1.12. Estar licenciada para suportar sem o uso de licença, 1.000 (mil) clientes de VPN SSL simultâneos;
1.13. Estar licenciada para ou suportar sem o uso de licença, 200 (duzentos) túneis de VPN IPSEC simultâneos;

2. 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;

IV - Renovação de solução de Gerenciamento de Firewall Centralizado (Panorama) para 25 dispositivos (Grupo 1 - item 3)

1. Renovação da Solução de Gerenciamento Centralizado Panorama Virtual Palo Alto Networks existente no órgão;
2. Deverá ser considerado premium support para 25 dispositivos (devices);
3. Serial number da solução atual: 000702699866;
4. Deverá ser compatível com os itens 1 e 2 do Grupo 1;
5. Deverá estar disponível durante, no mínimo, 60 (sessenta) meses.
6. Deverá possuir o mesmo nível de suporte e tempo de garantia do item 1 e item 2 do Grupo 1, incluindo a evolução para novas versões.

V - Serviço de Instalação e Configuração da solução de Firewall Tipo 1 - ONSITE em Campo Grande/MS (Grupo 1 - item 4)

1. Serviço de instalação onsite a ser realizado em horário comercial com programação de janela de virada fora do horário em Campo Grande/MS;
2. Os serviços devem ser executados e planejados por técnicos certificados em gerenciamento de projetos. Fica a cargo deste órgão a solicitação da comprovação das certificações dos técnicos responsáveis pela realização dos serviços;
3. Será de responsabilidade da contratada todo o planejamento e implementação da topologia de rede e de recursos de segurança;

4. Deverá ser realizado inicialmente uma implementação AS-IS onde os equipamentos novos deverão receber as configurações dos equipamentos Palo Alto Networks existentes no órgão, devendo a contratada fazer os ajustes necessários;
5. Ao final da implementação a contratada deverá emitir e apresentar um relatório de segurança com dados obtidos a partir da solução contendo:
    1. Informações de adoção da solução, apontando configurações individuais para verificar como os recursos de segurança estão sendo aproveitados. Exemplo: Análise da base de regras para identificar se as mesmas estão sendo aproveitadas e se são relevantes;
    2. Informações de avaliação de melhores práticas sobre as configurações da solução, identificando os riscos e fornecendo recomendações. Exemplo: A avaliação deverá comparar as configurações atuais às práticas recomendadas devendo apontar qual das práticas recomendadas estão ou não sendo utilizadas;
    3. Informações referente as aplicações e as ameaças detectados no ambiente mostrando as aplicações em uso e quais introduzem ameaças na rede, utilização de aplicações SaaS, total de ameaças (malwares conhecidos, malwares desconhecidos e detecções de comando e controle) bem como a movimentações de arquivos (tipos e riscos);
    4. Após a emissão e análise dos relatórios a contratada deverá fazer as melhorias de configurações de adoção da solução e de melhores práticas;
6. A contratada deve ainda, após a instalação e configuração, monitorar presencialmente a solução pelo prazo mínimo de 1 (um) dia útil, sendo possível o *troubleshooting* em caso de problemas ou não conformidades na operação. Durante este período deve ser observado e realizado também o ajuste e configurações que porventura não estarão de acordo com a operação desejada por este órgão;
7. A realização dos serviços deve ser planejada de acordo com disponibilidade de ambas as partes, em prazo máximo de 30 dias após a entrega definitiva dos bens ou oficialização da ordem de empenho. O planejamento anterior ao serviço pode ser realizado remotamente através de webconferência e videoconferência;
8. O planejamento dos serviços de instalação deve resultar em um documento tipo SOW (em tradução livre, escopo de trabalho). Neste documento devem conter a relação de produtos; descrição e quantidades de equipamentos e serviços; descrição da infraestrutura atual e desejada; detalhamento dos serviços que serão executados; premissas do projeto; local, horários e condições de execução dos serviços; pontos de contato da contratante e contratada; cronograma faseado do projeto, dividido em etapas, com responsáveis e data e início e fim (se aplicável); relação da documentação a ser entregue ao final da execução dos serviços; responsabilidade da contratante e contratada; plano de gerenciamento de mudanças; itens excluídos no projeto; e termo de aceite. Os serviços não poderão ser iniciados antes da apresentação e assinatura de concordância de ambas as partes;
9. Ao término dos serviços deve ser criado um relatório detalhado contendo todos os itens configurados no projeto (as-built), etapas de execução e toda informação pertinente a posterior continuidade e manutenção da solução instalada;
10. Deve ser entregue relatório contendo todo o serviço realizado executado;
11. Deverá ser feita por profissionais devidamente qualificados e certificados pelo fabricante e acompanhada pelos técnicos da contratante.

VII - Serviço de Projeto, Instalação e Configuração da Solução de Firewall Tipo 2 - REMOTO (Grupo 1 - item 5)

1. Serviço de instalação remoto a ser realizado em horário comercial;
2. Os serviços devem ser executados e planejados por técnicos certificados em gerenciamento de projetos. Fica a cargo deste órgão a solicitação da comprovação das certificações dos técnicos responsáveis pela realização dos serviços;
3. Será de responsabilidade da contratada todo o planejamento e implementação da topologia de rede e de recursos de segurança;

4. Deverá ser realizado inicialmente uma implementação AS-IS onde os equipamentos novos deverão receber as configurações dos equipamentos Palo Alto Networks existentes no órgão, devendo a contratada fazer os ajustes necessários;
5. A realização dos serviços deve ser planejada de acordo com disponibilidade de ambas as partes, em prazo máximo de 30 dias após a entrega definitiva dos bens ou oficialização da ordem de empenho. O planejamento anterior ao serviço pode ser realizado remotamente através de webconferência e videoconferência;
6. O planejamento dos serviços de instalação deve resultar em um documento tipo SOW (em tradução livre, escopo de trabalho). Neste documento devem conter a relação de produtos; descrição e quantidades de equipamentos e serviços; descrição da infraestrutura atual e desejada; detalhamento dos serviços que serão executados; premissas do projeto; local, horários e condições de execução dos serviços; pontos de contato da contratante e contratada; cronograma faseado do projeto, dividido em etapas, com responsáveis e data e início e fim (se aplicável); relação da documentação a ser entregue ao final da execução dos serviços; responsabilidade da contratante e contratada; plano de gerenciamento de mudanças; itens excluídos no projeto; e termo de aceite. Os serviços não poderão ser iniciados antes da apresentação e assinatura de concordância de ambas as partes;
7. Ao término dos serviços deve ser criado um relatório detalhado contendo todos os itens configurados no projeto (as-built), etapas de execução e toda informação pertinente a posterior continuidade e manutenção da solução instalada;
8. Deve ser entregue relatório contendo todo o serviço realizado executado;
9. Deverá ser feita por profissionais devidamente qualificados e certificados pelo fabricante e acompanhada pelos técnicos da contratante.

VIII - Software de backup com licenciamento por socket (Grupo 2 - item 6)

1. A solução ofertada deverá pertencer ao mesmo fabricante de software, não serão aceitas composições de softwares de fabricantes distintos para o atendimento às especificações.
2. O licenciamento da solução ofertada não deverá possuir nenhum tipo de restrição de limite de volumetria de armazenamento (TB), seja por backend ou frontend, em qualquer componente da solução durante e após o término do CONTRATO.
3. Cada unidade deste item deverá licenciar o uso de 1 socket (processador físico) para os servidores de virtualização VMware ESXi, gerenciados pelo VMware vCenter, sem limite às máquinas virtuais em execução nos respectivos hospedeiros.
4. Prover licenciamento de software perpétuo, ou seja, não poderá perder nenhuma funcionalidade operacional e não poderão ser cobrados quaisquer valores adicionais pelo seu uso completo - durante e após o término do CONTRATO.
5. Prover licenciamento que englobe todas as funcionalidades e requisitos elencados neste Termo de Referência, independentemente de qualquer quantidade de utilização do referido serviço, sem nenhum tipo de cobrança adicional para a CONTRATANTE.
6. Deverá incluir funcionalidades de proteção (backup) e replicação integradas em uma única solução.
7. Não deverá necessitar de instalação de agentes para poder realizar suas tarefas de proteção, recuperação e replicação das máquinas virtuais.
8. Deverá garantir, no mínimo, a proteção de máquinas virtuais e seus dados, gerenciadas através das soluções de virtualização VMware e Microsoft Hyper-V;
9. A solução ofertada deverá possuir compatibilidade conforme as especificações abaixo:
    9.1. VMware vCenter e vSphere ESXi versões 6.0 e superiores.
    9.2. VMware vCloud Director versões 10.1 e superiores.
    9.3. Microsoft System Center Virtual Machine Manager e Hyper-V 2012 e superiores.
    9.4. Nuvem da Amazon Web Services (AWS) EC2 e Microsoft Azure VM.
    9.5. Microsoft Active Directory 2008 R2 e superiores.

9.6. Microsoft Exchange 2013 e superiores.
9.7. Microsoft File Server Failover Cluster 2016 e superiores.
9.8. Microsoft SQL Server 2008 SP4 e superiores.
9.9. Oracle Database 11g Release 2 e superiores.
9.10. MySQL 5.6 ou superiores.
9.11. PostgreSQL 9.6 ou superiores.
9.12. Suportar, nos clientes de backup, os sistemas operacionais:
9.13. Microsoft Windows Server 2008 R2 SP1 e superiores.
9.14. Microsoft Windows 7 SP1 e superiores.
9.15. CentOS Linux 7 e superiores.
9.16. Debian Linux 10 e superiores.
9.17. Oracle Linux 6 e superiores
9.18. SUSE Linux Enterprise Server 12 SP4 e superiores.
9.19. Ubuntu 16.04 LTS e versões LTS superiores.

10. Suportar, nos clientes para backup, os sistemas de arquivos do tipo: Btrfs, ext3, ext4, HFS, HFS+, JFS, ReiserFS, XFS, FAT32, NTFS e ReFS.
11. Deverá ter a capacidade de replicação de dados armazenados entre storages ou máquinas de configuração e de fabricantes diferentes.
12. Deverá proteger o ambiente, sem interromper a atividade das máquinas virtuais e sem prejudicar sua performance, facilitando as tarefas de proteção (backup) e migrações em conjunto.
13. Deverá ter a capacidade de testar a consistência do backup e replicação (S.O., aplicação, VM), emitindo relatório de auditoria para garantir a capacidade de recuperação.
14. Deverá prover a deduplicação e compressão durante a operação de qualquer backup sem a necessidade de hardware de terceiros (appliance deduplicadora).
15. Deverá possibilitar a cópia de uma máquina virtual completa ou discos virtuais específicos.
16. Deverá ser fornecida com ferramenta de gestão de arquivos para os administradores de máquinas virtuais no console do operador.
17. Deverá ter a capacidade de integração através de API’s dos fabricantes de infraestrutura virtualizada para a proteção de dados.
18. Deverá ter a capacidade de realizar proteção (backup) incremental e replicação diferencial, aproveitando a tecnologia de “rastreio de blocos modificados” CBT (Changed Block Tracking) e RCT (Resilient Change Tracking), reduzindo ao mínimo necessário, o tempo de backup e possibilitando proteção (backup e replicação).
19. Deverá oferecer múltiplas estratégias e opções de transporte de dados do VMware para as áreas de proteção (backup), a saber:
20. Diretamente através de Storage Area Network (SAN);
21. Diretamente do storage, através do hypervisor I/O (HotAdd);
22. Mediante uso da rede local (LAN/NBD);
23. Diretamente do snapshot do storage onde os dados das VMs estejam armazenados;
24. Deverá manter um backup sintético, eliminando assim a necessidade de realizar backups completos (full) periódicos, incremental permanente, o que permitirá economizar tempo e espaço.
25. Deverá possibilitar a inicialização de uma máquina virtual diretamente do arquivo de backup, inclusive sem necessidade de “hidratação” dos dados “deduplicados e “comprimidos”.
26. Deverá permitir a recuperação de mais de uma máquina virtual e/ou ponto de restauração simultâneo, permitindo assim, ter múltiplos pontos de tempo de uma ou mais máquinas virtuais.
27. Todo serviço de migração das máquinas virtuais do repositório de backup até o armazenamento na produção restabelecida não deverá afetar a disponibilidade e acesso pelo usuário, sem paradas.
28. Deverá prover acesso ao conteúdo das máquinas virtuais, para recuperação de arquivos, pastas ou anexos, diretamente do ambiente protegido (repositório de backup) ou replicados, sem a necessidade de recuperar completamente o backup e inicializar uma máquina virtual.

29. Deverá permitir realizar buscas rápidas mediante os índices dos arquivos que sejam controlados por um sistema operacional Windows, quando este seja o sistema operacional executado dentro da máquina virtual da qual se tenha realizado o backup.
30. Deverá permitir a recuperação de uma máquina/servidor físico instantâneamente no ambiente virtual Hyper-V e VMware, com inicialização rápida, a partir de seus arquivos de backup, sem a necessidade de esperar o término do processo de restauração.
31. Deverá manter todas as configurações originais de rede das Máquinas Virtuais sem ocasionar nenhum conflito com o ambiente de produção, ou seja, deverá ser um ambiente de rede isolado.
32. Deverá assegurar a consistência de aplicações transacionais de forma automática por meio da integração com Microsoft VSS, dentro de sistemas operacionais Windows.
33. Deverá permitir realizar a truncagem de logs transacionais (transaction logs) para máquinas virtuais com Microsoft Exchange, SQL Server e Oracle.
34. Deverá permitir notificações por correio eletrônico, SNMP ou através dos atributos da máquina virtual do resultado da execução de seus trabalhos.
35. Deverá prover meios automáticos de garantir a consistência do backup a nível de aplicação, ou seja, ser capaz de automatizar a restauração de uma máquina virtual e executar ações de testes previamente programadas para aquela determinada aplicação de forma a garantir que o backup está consistente.
36. Deverá permitir recuperar no nível de objetos e arquivos de qualquer aplicação virtualizada, em qualquer sistema operacional, utilizando as ferramentas de gestão das aplicações existentes.
37. Deverá incluir ferramentas de recuperação sem a necessidade de agentes, sem a necessidade de recuperar os arquivos da máquina virtual como um todo ou reiniciar a mesma (recuperação granular), para os servidores:
38. Microsoft Exchange 2016, possibilitando recuperar objetos individuais, tais como contatos, mensagens, compromissos, anexos, entre outros;
39. Microsoft Active Directory 2016, possibilitando recuperar objetos individuais, tais como usuários, recuperação de senhas de usuários e computadores, grupos, contas, Objetos de Política de Grupo (GPOs), registros do Microsoft DNS integrados ao Active Directory entre outros sem a necessidade de usar o agente tanto para backup e restauração;
40. Microsoft SQL Server 2014 ou superior, possibilitando recuperar objetos individuais, tais como bases, tabelas, registros, entre outros;
41. Microsoft Sharepoint 2016;
42. Deverá oferecer testes automatizados de recuperação para todas as máquinas virtuais protegidas, garantindo a confiabilidade na execução correta das máquinas virtuais e de suas aplicações (DNS Server, Controlador de domínio, Servidor de e-mail, etc.), no momento da recuperação.
43. Deverá ser possível executar uma ou várias máquinas virtuais a partir do arquivo de backup, em um ambiente isolado de forma automática através de schedule, sem a necessidade de espaço de armazenamento adicional e sem modificar os arquivos de backup (read-only), para criação de ambiente de homologação, teste, etc.
44. Deverá oferecer arquivamento em fita, suportando VTL (Virtual Tape Libraries), biblioteca de fitas e drives LTO5 ou superior, possibilitando a gravação paralela em múltiplos drives, além da criação de pools de mídia globais e pools de mídia GFS, sem a necessidade de licenciamento individual por drive;
45. Deverá oferecer trabalhos de cópia de backup com implementação de políticas de retenção.
46. Deverá operar em ambientes virtualizados através das soluções da Vmware, incluindo: VMware vSphere 6 e superiores.
47. Deverá ter a capacidade de monitoramento em tempo real, sem a necessidade de agentes, da infraestrutura virtual e de backup, inclusive máquinas virtuais, para VMware e Microsoft, com notificação de problemas de backup e desempenho, com geração de alertas e base de conhecimento embutida para resolução dos mesmos.

48. Deverá ter a capacidade de monitoramento e análise de capacidade do ambiente para crescimento, ajustes e planejamentos de crescimento.
49. Deverá garantir a recuperação granular e consistente, sem necessidade de instalação de agentes adicionais para o ambiente virtualizado através das soluções acima, principalmente para os seguintes softwares:
    49.1. Microsoft Active Directory 2016;
    49.2. Microsoft Exchange Server 2016;
    49.3. Microsoft Sharepoint 2013 ou superior
    49.4. Oracle Database 12 ou superior.
50. Deverá ser capaz de realizar réplicas em outros sites ou infraestruturas a partir dos backups realizados. Deve suportar a replicação remota a fim de replicar os dados das máquinas virtuais entre soluções de armazenamento distintas, inclusive de diferentes fabricantes e suportar a orquestração de failover e failback das máquinas virtuais replicadas;
51. Deverá regular de forma dinâmica e parametrizável, o uso de recursos computacionais, de forma que se possa diminuir o impacto na infraestrutura de produção, durante as atividades de backup.
52. Deverá permitir orquestração de máquinas virtuais em ambientes de contingência, com as ações pré-configuradas para evitar ações manuais em caso de desastre, similar a um botão de emergência.
53. Deverá oferecer a possibilidade de armazenar os arquivos de backup de forma criptografada, com algoritmo mínimo de 256 bits, ativando e desativando tal operação, assim como assegurar o trânsito da informação através desse cenário.
54. Deverá permitir cópias adicionais do backup principal com funcionalidade de criar múltiplas cópias em fitas.
55. Deverá permitir a criação de níveis de delegação de tarefas (perfis) de recuperação no nível de elementos da aplicação, inclusive para outros usuários, de forma a diminuir a carga de atividades executadas pelo administrador da plataforma.
56. A licença de software de Backup deverá, nativamente, ser capaz de emitir relatórios com informações completas, conforme subitens:
    56.1. Permitir acesso aos relatórios através de interface gráfica ou web;
    56.2. Suportar a geração de relatórios gráficos de atividades de backups/restores, contendo: Horário de início e término dos jobs; Tempo de duração dos Jobs; Status (situação) de execução dos jobs; Relação de jobs executados por status, como por exemplo: com sucesso e com erros; Logs dos jobs; Volume de dados na origem e no destino, total e por job; Suportar a geração de relatórios sobre o consumo de licenças; Dados históricos de, no mínimo, 12 (dozes) meses.
    56.3. Permitir a geração de relatórios sobre os testes automatizados do backup a nível de aplicação, incluindo a quantidade de rotinas de verificação, status das rotinas e quantidade de máquinas virtuais verificadas;
57. Deverá correlacionar a execução de trabalhos de backup e réplica com os objetos do ambiente virtual;
58. Deverá oferecer a capacidade de relatar o cumprimento das políticas de proteção de dados e disponibilidade de acordo com parâmetros definidos;
59. Deve suportar múltiplas operações dos componentes/servidores participantes da estrutura de backup, permitindo atividades de backup e recuperação simultâneas;
60. Deve suportar repositório de backup com aumento de escala ilimitado para o armazenamento de dados com suporte aos seguintes sistemas de armazenamento:
    60.1. Microsoft Windows;
    60.2. Linux;
    60.3. Pastas compartilhadas;
    60.4. Appliances deduplicadoras;
    60.5. Storages do tipo SAN e NAS;
    60.6. Nuvem (Amazon AWS, Microsoft Azure);

61. Deverá permitir a seleção de um destino de armazenamento do backup em um provedor de serviços em nuvem (BaaS – Backup as a Service);
62. Deverá permitir a seleção de um destino para a réplica dos dados que poderá ser em um provedor de serviços em nuvem (DRaaS – DR as a Service);
63. Possuir integração com armazenamento de objetos compatíveis com S3 como Amazon S3, Azure Blob Storage e qualquer outro dispositivo de armazenamento local compatível com S3;
64. Realizar arquivamento dos dados de backup nos dispositivos e locais de armazenamento de objetos compatíveis com S3;
65. Em caso de desastre, deverá ser possível realizar a recuperação dos dados diretamente do arquivamento em S3;
66. A solução deverá possuir integração com soluções de antivírus de modo a realizar uma varredura de segurança nos dados de backup antes de realizar sua recuperação;
67. Deve estar homologado para o Oracle Database 12c nos sistemas operacionais Linux através de plugin sem a necessidade de instalação de agentes;
68. A solução deve oferecer suporte aos ambientes Oracle RAC (versões 12 e superior) usando o RMAN e deve ser certificada;
69. Deve possuir a funcionalidade de recuperar dados para servidores diferentes do equipamento de origem;
70. Do serviço de suporte técnico e garantia:
    - 70.1. O prazo de garantia para suporte técnico é de no mínimo 60 (sessenta) meses contados a partir da ativação da licença.
    - 70.2. O suporte técnico deve ser 24x7x365, ou seja, 24 (vinte e quatro) horas por dia em 7 (sete) dias da semana por 365 (trezentos e sessenta e cinco) dias por ano em português.
    - 70.3. Deverá contemplar a atualização de versões do software aplicativo, as quais incorporam correções de erros ou problemas registrados e melhorias implementadas pela fabricante, num empacotamento estável do sistema. O serviço de atualização de versão tem por finalidade assegurar a devida atualização da solução durante o período de vigência da garantia. Refere-se ao fornecimento de novas versões e releases da solução lançados no período.
    - 70.4. Deverá ser prestado suporte técnico remoto com atendimento mediante registro de chamados em página de website, em sistema fornecido pela contratada e/ou pelo fabricante; e também através de contato telefônico. Esse serviço destina-se a esclarecimento de dúvidas e resolução de problemas relacionados à configuração e uso dos componentes da solução contratada durante o período de vigência da garantia para suporte técnico.
    - 70.5. Deverá ter resposta de atendimento em até 02 (duas) horas e resolução do problema ou contorno em até 7 (sete) dias úteis após a abertura do chamado, independente da severidade.

IX - Servidor de Backup (Grupo 2 - item 7)

1. 2 (dois) Processadores Xeon 2,4 GHz com no mínimo 12 núcleos/threads (equivalente ou superior) cada;
2. 192GB (ou mais) de memória DDR4 com 2.933 MHz cada, padrão ECC;
3. Capacidade de expansão da memória de cada servidor para até 768 GB;
4. 1 (uma) Gaveta 2U 3,5 pol. SATA/SAS de 12 compartimentos;
5. 1 (uma) Controladora RAID PCIe Flash de 4 GB 12 Gb;
6. 96TB (ou mais) de armazenamento em HDD Hot-swap com discos de 3,5 polegadas 7200RPM NLSAS (ou equivalente);
7. 1 (um) M.2 com Kit de Ativação de Espelhamento;
8. 2 (dois) SSD 480GB SATA3 6Gb;
9. 1 (um) LOM SFP+ 2 portas 10 Gb;
10. 2 (dois) Transceptor SFP+ SR;
11. 2 (duas) Fonte de alimentação hotswap 550W (bivolt) ou superior;

12. 2 (dois) Cabo de Energia de Rack com 1,5 m, 10 A/100-250 V, C13 a IEC 320-C14;
13. 1 (uma) Interface de Gerenciamento com atualização/suporte;
14. 1 (um) Trilho de Corrediça sem necessidade de ferramentas;
15. 1 (um) Painel de Segurança 2U;
16. Garantia de 60 meses com atendimento on-site 24x7, com atendimento em até 24 horas a partir da abertura do chamado;
17. Suporte direto com o fabricante através de ligação gratuita do tipo 0800 e/ou acesso pela internet, com disponibilidade de atendimento e de resolução em regime de 24x7, incluindo-se os dias úteis, feriados e finais de semana.

X - Serviço de instalação e configuração da solução de backup (Grupo 2 - item 8)

1. O serviço de instalação e configuração deverá ser *onsite* em Campo Grande/MS, além de ser realizado preferencialmente em horário comercial;
2. A solução de backup configurada deverá ser capaz de realizar as rotinas de backup dos principais serviços da instituição;
3. Deverão ser configurados e testados os dois servidores de backup adquiridos: Um na reitoria - sede definitiva - como principal e outro, como serviço de replicação, a ser instalado no Campus Campo Grande, ambos em Campo Grande/MS;
4. Os serviços devem ser executados e planejados por técnicos certificados em gerenciamento de projetos. Fica a cargo deste órgão a solicitação da comprovação das certificações dos técnicos responsáveis pela realização dos serviços;
5. A realização dos serviços deve ser planejada de acordo com disponibilidade de ambas as partes, em prazo máximo de 30 dias após a entrega definitiva dos bens ou oficialização da ordem de empenho. O planejamento anterior ao serviço pode ser realizado remotamente através de webconferência e videoconferência;
6. O planejamento dos serviços de instalação deve resultar em um documento tipo SOW (em tradução livre, escopo de trabalho). Neste documento devem conter a relação de produtos; descrição e quantidades de equipamentos e serviços; descrição da infraestrutura atual e desejada; detalhamento dos serviços que serão executados; premissas do projeto; local, horários e condições de execução dos serviços; pontos de contato da contratante e contratada; cronograma faseado do projeto, dividido em etapas, com responsáveis e data e início e fim (se aplicável); relação da documentação a ser entregue ao final da execução dos serviços; responsabilidade da contratante e contratada; plano de gerenciamento de mudanças; itens excluídos no projeto; e termo de aceite. Os serviços não poderão ser iniciados antes da apresentação e assinatura de concordância de ambas as partes;
7. Ao término dos serviços deve ser criado um relatório detalhado contendo todos os itens configurados no projeto (as-built), etapas de execução e toda informação pertinente a posterior continuidade e manutenção da solução instalada;
8. Deve ser entregue relatório contendo todo o serviço realizado executado;
9. Deverá ser feita por profissionais devidamente qualificados e certificados pelo fabricante e acompanhada pelos técnicos da contratante.

XI - Serviço de Treinamento Oficial do Fabricante da Solução de Backup (Grupo 2 - item 9)

1. O treinamento poderá ser presencial (*in loco*) ou remoto;
2. A empresa a ministrar o curso deve ser um centro de educação autorizado e estar listado como tal no site do fabricante.
3. O treinamento deve compreender toda a parte de gestão da solução de software vencedora aplicável à solução de backup do IFMS, contendo mas não se limitando, os tópicos abaixo:
   - 3.1. Instalação, atualização e configuração do software e seus componentes;
   - 3.2. Configuração e gerenciamento dos dispositivos de armazenamento;
   - 3.3. Proteção e Recuperação dos Dados;
   - 3.4. Segurança;

3.5. Desduplicação e Arquivamento;
3.6. Criação e gerenciamento de políticas e replicação de dados;
3.7. Criação e gerenciamento de Schedules, Jobs, Scripts e relatórios;
3.8. Manutenção e monitoramento diários;
3.9. Troubleshooting e recuperação;

4. Deverá ser emitido certificado para os participantes do treinamento.

XII - Especificações gerais para os itens do Grupo 1 e Grupo 2

1. Condições de Participação e Realização dos Serviços:
   1.1. Cada grupo (lote) de solução deverá ser constituída dos equipamentos relacionados em seus itens, sendo todos de um mesmo fabricante, garantindo a entrega e execução dos serviços por uma única empresa e a total compatibilidade entre eles;
   1.2. A escolha do agrupamento dos itens em grupo visa a plena qualificação da empresa fornecedora que prestará os serviços de fornecimento, bem como prestará os serviços de suporte durante a vigência do contrato e da garantia dos equipamentos, a total compatibilidade entre os equipamentos solicitados, a redução de custos operacionais e de infraestrutura física, a capacidade técnica de manter a solução em operação, os recursos humanos disponíveis para prestarem o devido apoio, treinamento e curva de aprendizagem e o custo total de propriedade.
2. Garantia:
   2.1. Os equipamentos fornecidos deverão estar cobertos por garantia do fabricante no Brasil pelo período especificado;
   2.2. A garantia deve incluir substituição de peças decorrente de vícios de projeto, fabricação, construção e montagem, pelo período especificado no termo de referência, a contar da data de aceite provisório dos equipamentos;
   2.3. Os softwares fornecidos deverão estar cobertos por garantia que ofereça atualizações necessárias para a correção de vícios, pelo período especificado no termo de referência, a contar da data de ativação dos softwares;
   2.4. A garantia deve incluir também envio de peças/equipamentos de reposição, que deverão ser entregues nos locais especificados neste termo de referência, ou na sua ausência, na sede da contratante, abrangendo-se todos os custos de deslocamento (envio e retorno) das peças/equipamentos de substituição.
   2.5. Devem ser descritos, no momento da proposta, qual o tipo de garantia fornecida. Os equipamentos devem ter seus números seriais atrelados ao sistema de suporte do fabricante dos equipamentos com data específica de início e fim do suporte.
3. Atualizações:
   3.1. A contratada deverá disponibilizar, na vigência da garantia, todas as atualizações dos softwares e *firmwares* dos equipamentos, concebidas em data posterior ao seu fornecimento, pelo período especificado no termo de referência, sem qualquer ônus adicional para o contratante;
   3.2. As atualizações incluídas devem ser do tipo "*minor release*" e "*major release*", permitindo manter os equipamentos atualizados em sua última versão de software/firmware.
4. Condições de aceite:
   4.1. Os equipamentos deverão ser novos e sem uso. Não serão aceitos equipamentos usados, remanufaturados ou de demonstração; Os equipamentos deverão ser entregues nas caixas lacradas pelo fabricante, não sendo aceitos equipamentos com caixas violadas;
   4.2. Este órgão poderá efetuar consulta do número de série do equipamento, junto ao fabricante, informando data de compra e empresa adquirente, confirmando a procedência legal dos equipamentos;

4.3. Este órgão também poderá efetuar consulta junto aos órgãos competentes para certificar a legalidade do processo de importação;

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

5. Atendimento às Especificações:

5.1. Todas as características técnicas obrigatórias deverão ser comprovadas por meio de folders, catálogos, manuais, guias de instalação, informações da interface de gerência da solução e impressão de páginas do fabricante na Internet;

5.2. Apresentação de documento denominado “Atendimento às Especificações” para demonstrar o atendimento ponto-a-ponto dos itens e subitens obrigatórios constantes deste Termo de Referência;

5.3. No documento “Atendimento às Especificações”, deverá estar indicada a localização exata da informação que garante o atendimento ao item e subitem, explicitando o documento/página; A informação deverá estar grifada para melhor visualização.

ANEXO A - ENDEREÇOS DAS UNIDADES

CIDADE	UNIDADE	ENDEREÇO	TELEFONE
Aquidauana-MS	Campus Aquidauana	Rua José Tadao Arima, 222, Bairro Ycaraí CEP 79200-000	(67) 3240-1600
Campo Grande-MS	Reitoria	Av. Ceará, 972, Bairro Santa Fé CEP 79021-000	(67) 3378-9501
Campo Grande-MS	Campus Campo Grande	Rua Taquari, 831, Bairro Santo Antônio CEP 79100-510	(67) 3357-8501
Corumbá-MS	Campus Corumbá	Rua Pedro de Medeiros, 941, Bairro Popular Velha CEP 79310-110	(67) 3234-9101
Coxim-MS	Campus Coxim	Rua Salime Tanure, s/n, Bairro Santa Tereza CEP 79400-000	(67) 3291-9600
Dourados-MS	Campus Dourados	Rua Filinto Müller, 1.790, Jardim Canaã I CEP 79833-520	(67) 3410-8500
Jardim-MS	Campus Jardim	Rodovia BR-060, s/n, saída para Bela Vista CEP 79240-000	(67) 3209-0200

Naviraí-MS	Campus Naviraí	Endereço provisório: Rua Hilda, 203, Bairro Boa Vista CEP 79950-000 Endereço definitivo: Rodovia MS 141, km 04, s/nº CEP 79950-000	(67) 3409-2501
Nova Andradina-MS	Campus Nova Andradina	Avenida Rosilene Lima Oliveira, 64, Bairro Universitário. CEP 79750-000 (UFMS)	(67) 3441-9600
Ponta Porã-MS	Campus Ponta Porã	Rodovia BR-463, km 14, s/n CEP 79909-000	(67) 3437-9600
Três Lagoas-MS	Campus Três Lagoas	Rua Ângelo Melão, 790, Jardim das Paineiras CEP 79641-162	(67) 3509-9500

ANEXO B - MODELO DE TERMO DE COMPROMISSO DE MANUTENÇÃO DO SIGILO E SEGURANÇA DA INFORMAÇÃO

TERMO DE COMPROMISSO DE MANUTENÇÃO DE SIGILO

INTRODUÇÃO
O Termo de Compromisso de Manutenção de Sigilo registra o comprometimento formal da Contratada em cumprir as condições estabelecidas no documento relativas ao acesso e utilização de informações sigilosas da Contratante em decorrência de relação contratual, vigente ou não. **Referência: Art. 18, Inciso V, alínea "a" da IN SGD/ME Nº 1/2019.**

Pelo presente instrumento o **Instituto Federal de Educação, Ciência e Tecnologia de Mato Grosso do Sul**, com sede provisória na Rua Jorn. Belizário Lima, 236, bairro Vila Glória, CEP: 79.004-270, na cidade de Campo Grande – MS, CNPJ n° 10.673.078/0001-20, doravante denominado **CONTRATANTE**, e, de outro lado, a <XXXXXXXXXXXXXX>, com sede na <Rua XXXX, nº XXXX, Bairro, Cidade/UF, CNPJ n° XX.XXX.XXX/XXXX-XX>, doravante denominada **CONTRATADA**;
CONSIDERANDO que, em razão do **CONTRATO N.º <nº do contrato>** doravante denominado **CONTRATO PRINCIPAL**, a **CONTRATADA** poderá ter acesso a informações sigilosas do **CONTRATANTE**; CONSIDERANDO a necessidade de ajustar as condições de revelação destas informações sigilosas, bem como definir as regras para o seu uso e proteção; CONSIDERANDO o disposto na Política de Segurança da Informação e Privacidade da **CONTRATANTE**;
Resolvem celebrar o presente **TERMO DE COMPROMISSO DE MANUTENÇÃO DE SIGILO,** doravante **TERMO**, vinculado ao **CONTRATO PRINCIPAL**, mediante as seguintes cláusulas e condições abaixo discriminadas.

1 – OBJETO

Constitui objeto deste TERMO o estabelecimento de condições específicas para regulamentar as obrigações a serem observadas pela CONTRATADA, no que diz respeito ao trato de informações sigilosas disponibilizadas pela CONTRATANTE e a observância às normas de segurança da informação e privacidade por força dos procedimentos necessários para a execução do objeto do CONTRATO PRINCIPAL celebrado entre as partes e em acordo com o que dispõem a Lei 12.527, de 18 de novembro de 2011, Lei nº 13.709, de 14 de agosto de 2018, e os Decretos 7.724, de 16 de maio de 2012, e 7.845, de 14 de novembro de 2012, que regulamentam os procedimentos para acesso e tratamento de informação classificada em qualquer grau de sigilo.

2 – CONCEITOS E DEFINIÇÕES

Para os efeitos deste TERMO, são estabelecidos os seguintes conceitos e definições:

INFORMAÇÃO: dados, processados ou não, que podem ser utilizados para produção e transmissão de conhecimento, contidos em qualquer meio, suporte ou formato.

INFORMAÇÃO SIGILOSA: aquela submetida temporariamente à restrição de acesso público em razão de sua imprescindibilidade para a segurança da sociedade e do Estado, e aquela abrangida pelas demais hipóteses legais de sigilo.

CONTRATO PRINCIPAL: contrato celebrado entre as partes, ao qual este TERMO se vincula.

3 – DA INFORMAÇÃO SIGILOSA

Serão consideradas como informação sigilosa, toda e qualquer informação classificada ou não nos graus de sigilo ultrassecreto, secreto e reservado. O TERMO abrangerá toda informação escrita, verbal, ou em linguagem computacional em qualquer nível, ou de qualquer outro modo apresentada, tangível ou intangível, podendo incluir, mas não se limitando a: *know-how*, técnicas, especificações, relatórios, compilações, código fonte de programas de computador na íntegra ou em partes, fórmulas, desenhos, cópias, modelos, amostras de idéias, aspectos financeiros e econômicos, definições, informações sobre as atividades da CONTRATANTE e/ou quaisquer informações técnicas/comerciais relacionadas/resultantes ou não ao CONTRATO PRINCIPAL, doravante denominados INFORMAÇÕES, a que diretamente ou pelos seus empregados, a CONTRATADA venha a ter acesso, conhecimento ou que venha a lhe ser confiada durante e em razão das atuações de execução do CONTRATO PRINCIPAL celebrado entre as partes.

4 – DOS LIMITES DO SIGILO

As obrigações constantes deste TERMO não serão aplicadas às INFORMAÇÕES que:

I – sejam comprovadamente de domínio público no momento da revelação, exceto se tal fato decorrer de ato ou omissão da CONTRATADA;

II – tenham sido comprovadas e legitimamente recebidas de terceiros, estranhos ao presente TERMO;

III – sejam reveladas em razão de requisição judicial ou outra determinação válida do Governo, somente até a extensão de tais ordens, desde que as partes cumpram qualquer medida de proteção pertinente e tenham sido notificadas sobre a existência de tal ordem, previamente e por escrito, dando a esta, na medida do possível, tempo hábil para pleitear medidas de proteção que julgar cabíveis.

5 – DIREITOS E OBRIGAÇÕES

As partes se comprometem a não revelar, copiar, transmitir, reproduzir, utilizar, transportar ou dar conhecimento, em hipótese alguma, a terceiros, bem como a não permitir que qualquer empregado envolvido direta ou indiretamente na execução do CONTRATO PRINCIPAL, em qualquer nível hierárquico de sua estrutura organizacional e sob quaisquer alegações, faça uso dessas INFORMAÇÕES, que se restringem estritamente ao cumprimento do CONTRATO PRINCIPAL.

Parágrafo Primeiro – A CONTRATADA se compromete a não efetuar qualquer tipo de cópia da informação sigilosa sem o consentimento prévio e expresso da CONTRATANTE.

Parágrafo Segundo – A CONTRATADA compromete-se a dar ciência e obter o aceite formal

da direção e empregados que atuarão direta ou indiretamente na execução do CONTRATO PRINCIPAL sobre a existência deste TERMO bem como da natureza sigilosa das informações.

I – A CONTRATADA deverá firmar acordos por escrito com seus empregados visando garantir o cumprimento de todas as disposições do presente TERMO e dará ciência à CONTRATANTE dos documentos comprobatórios.

Parágrafo Terceiro – A CONTRATADA obriga-se a tomar todas as medidas necessárias à proteção da informação sigilosa da CONTRATANTE, bem como evitar e prevenir a revelação a terceiros, exceto se devidamente autorizado por escrito pela CONTRATANTE.

Parágrafo Quarto – Cada parte permanecerá como fiel depositária das informações reveladas à outra parte em função deste TERMO.

I – Quando requeridas, as INFORMAÇÕES deverão retornar imediatamente ao proprietário, bem como todas e quaisquer cópias eventualmente existentes.

Parágrafo Quinto – A CONTRATADA obriga-se por si, sua controladora, suas controladas, coligadas, representantes, procuradores, sócios, acionistas e cotistas, por terceiros eventualmente consultados, seus empregados, contratados e subcontratados, assim como por quaisquer outras pessoas vinculadas à CONTRATADA, direta ou indiretamente, a manter sigilo, bem como a limitar a utilização das informações disponibilizadas em face da execução do CONTRATO PRINCIPAL.

Parágrafo Sexto – A CONTRATADA, na forma disposta no parágrafo primeiro, acima, também se obriga a:

I – Não discutir perante terceiros, usar, divulgar, revelar, ceder a qualquer título ou dispor das INFORMAÇÕES, no território brasileiro ou no exterior, para nenhuma pessoa, física ou jurídica, e para nenhuma outra finalidade que não seja exclusivamente relacionada ao objetivo aqui referido, cumprindo-lhe adotar cautelas e precauções adequadas no sentido de impedir o uso indevido por qualquer pessoa que, por qualquer razão, tenha acesso a elas;

II – Responsabilizar-se por impedir, por qualquer meio em direito admitido, arcando com todos os custos do impedimento, mesmos judiciais, inclusive as despesas processuais e outras despesas derivadas, a divulgação ou utilização das INFORMAÇÕES por seus agentes, representantes ou por terceiros;

III – Comunicar à CONTRATANTE, de imediato, de forma expressa e antes de qualquer divulgação, caso tenha que revelar qualquer uma das INFORMAÇÕES, por determinação judicial ou ordem de atendimento obrigatório determinado por órgão competente; e

IV – Identificar as pessoas que, em nome da CONTRATADA, terão acesso às informações sigilosas.

6 – VIGÊNCIA

O presente TERMO tem natureza irrevogável e irretratável, permanecendo em vigor desde a data de sua assinatura até expirar o prazo de classificação da informação a que a CONTRATADA teve acesso em razão do CONTRATO PRINCIPAL.

7 – PENALIDADES

A quebra do sigilo e/ou da confidencialidade das INFORMAÇÕES, devidamente comprovada,

possibilitará a imediata aplicação de penalidades previstas conforme disposições contratuais e legislações em vigor que tratam desse assunto, podendo até culminar na rescisão do CONTRATO PRINCIPAL firmado entre as PARTES. Neste caso, a CONTRATADA, estará sujeita, por ação ou omissão, ao pagamento ou recomposição de todas as perdas e danos sofridos pela CONTRATANTE, inclusive as de ordem moral, bem como as de responsabilidades civil e criminal, as quais serão apuradas em regular processo administrativo ou judicial, sem prejuízo das demais sanções legais cabíveis, conforme Art. 87 da Lei nº. 8.666/93.

8 – DISPOSIÇÕES GERAIS

Este TERMO de Confidencialidade é parte integrante e inseparável do CONTRATO PRINCIPAL.

Parágrafo Primeiro – Surgindo divergências quanto à interpretação do disposto neste instrumento, ou quanto à execução das obrigações dele decorrentes, ou constatando-se casos omissos, as partes buscarão solucionar as divergências de acordo com os princípios de boa fé, da equidade, da razoabilidade, da economicidade e da moralidade.

Parágrafo Segundo – O disposto no presente TERMO prevalecerá sempre em caso de dúvida e, salvo expressa determinação em contrário, sobre eventuais disposições constantes de outros instrumentos conexos firmados entre as partes quanto ao sigilo de informações, tal como aqui definidas.

Parágrafo Terceiro – Ao assinar o presente instrumento, a CONTRATADA manifesta sua concordância no sentido de que:

I – A CONTRATANTE terá o direito de, a qualquer tempo e sob qualquer motivo, auditar e monitorar as atividades da CONTRATADA;

II – A CONTRATADA deverá disponibilizar, sempre que solicitadas formalmente pela CONTRATANTE, todas as informações requeridas pertinentes ao CONTRATO PRINCIPAL.

III – A omissão ou tolerância das partes, em exigir o estrito cumprimento das condições estabelecidas neste instrumento, não constituirá novação ou renúncia, nem afetará os direitos, que poderão ser exercidos a qualquer tempo;

IV – Todas as condições, termos e obrigações ora constituídos serão regidos pela legislação e regulamentação brasileiras pertinentes;

V – O presente TERMO somente poderá ser alterado mediante TERMO aditivo firmado pelas partes;

VI – Alterações do número, natureza e quantidade das informações disponibilizadas para a CONTRATADA não descaracterizarão ou reduzirão o compromisso e as obrigações pactuadas neste TERMO, que permanecerá válido e com todos seus efeitos legais em qualquer uma das situações tipificadas neste instrumento;

VII – O acréscimo, complementação, substituição ou esclarecimento de qualquer uma das informações, conforme definição do item 3 deste documento, disponibilizadas para a CONTRATADA, serão incorporados 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, sendo necessário a formalização de TERMO aditivo ao CONTRATO PRINCIPAL;

VIII – Este TERMO não deve ser interpretado como criação ou envolvimento das Partes, ou suas filiadas, nem em obrigação de divulgar INFORMAÇÕES para a outra Parte, nem como

obrigação de celebrarem qualquer outro acordo entre si.

9 – FORO

A CONTRATANTE elege o foro da Campo Grande - MS, onde está localizada a sede da CONTRATANTE, para dirimir quaisquer dúvidas originadas do presente TERMO, com renúncia expressa a qualquer outro, por mais privilegiado que seja.

10 – ASSINATURAS

E, por assim estarem justas e estabelecidas as condições, o presente TERMO DE COMPROMISSO DE MANUTENÇÃO DE SIGILO é assinado pelas partes em 2 vias de igual teor e um só efeito.

CONTRATADA	CONTRATANTE
_____ <Nome> <Qualificação>	_____ <Nome> **Matrícula:** xxxxxxxx

TESTEMUNHAS	
_____ <Nome> <Qualificação>	_____ <Nome> <Qualificação>

<Local>, <dia> de <mês> de <ano>.

ANEXO C - MODELO DE TERMO DE CIÊNCIA INDIVIDUAL DE SIGILO E SEGURANÇA DA INFORMAÇÃO

TERMO DE CIÊNCIA

INTRODUÇÃO
< O Termo de Ciência visa obter o comprometimento formal dos empregados da contratada diretamente envolvidos na contratação quanto ao conhecimento da declaração de manutenção de sigilo e das normas de segurança vigentes no Órgão/Entidade>. < No caso de substituição ou inclusão de empregados da contratada, o preposto deverá entregar ao Fiscal Administrativo do Contrato os Termos de Ciência assinados pelos novos empregados envolvidos na execução dos serviços contratados>. **Referência: Art. 18, Inciso V, alínea "b" da IN SGD/ME Nº 1/2019.**

1 – IDENTIFICAÇÃO

CONTRATO Nº	XX/AAAA		
OBJETO	<Descrição do Objeto>		
CONTRATADA	<Nome da contratada>	**CNPJ**	<XXXXX>
PREPOSTO	<Nome do Preposto da Contratada>		
GESTOR DO CONTRATO	<Nome do Gestor do Contrato>	**MATR.**	<XXXXXX>

2 – CIÊNCIA

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

Funcionários da Contratada		
Nome	**Matrícula**	**Assinatura**
<Nome do(a) Funcionário(a)>	<XXXXXX>	

<Local>, <dia> de <mês> de <ano>.

ANEXO D - MODELO DE ORDEM DE FORNECIMENTO DE BENS / ORDEM DE SERVIÇO

ORDEM DE SERVIÇO E/OU FORNECIMENTO DE BENS

1 – IDENTIFICAÇÃO			
Nº da OS/OFB		Data de emissão	
Contrato nº			
Objeto do Contrato			
Contratada		CNPJ	
Preposto			
Gestor do Contrato			
Fiscal Requisitante			

2 – ESPECIFICAÇÃO DOS BENS/SERVIÇOS E VOLUMES ESTIMADOS					
Item	Descrição	Uni.	Qtde	Valor Uni.	Valor Total
Valor Total Estimado					

3 – CRONOGRAMA			
Grupo/Item	Prazo (em dias)	Data Início	Data Entrega

4 – INFORMAÇÕES COMPLEMENTARES

<Local>, <dia> de <mês> de <ano>.

ANEXO II – MINUTA ATA DE REGISTRO DE PREÇOS
(SOLUÇÃO DE TECNOLOGIA DA INFORMAÇÃO E COMUNICAÇÃO)

INSTITUTO FEDERAL DE MATO GROSSO DO SUL

ATA DE REGISTRO DE PREÇOS
N.º .....

O **Instituto Federal de Educação, Ciência e Tecnologia de Mato Grosso do Sul**, com sede à Rua Jornalista Belizário Lima, 236, Bairro Vila Glória, na cidade de Campo Grande, inscrito no CNPJ/MF sob o nº **10.673.078/0001-20**, neste ato representado pela **Reitora Elaine Borges Monteiro Cassiano**, nomeada pelo **Decreto de 25 de Novembro de 2019**, publicado no Diário Oficial da União de 26 de novembro de 2019, portador da matrícula funcional nº 1941845, considerando o julgamento da licitação na modalidade de pregão, na forma eletrônica, para REGISTRO DE PREÇOS nº xx/2022, publicada no https://www.gov.br/compras/pt-br/ de xxxx, processo administrativo n° **23347.009360.2021-94**, RESOLVE registrar os preços da(s) empresa(s) indicada(s) e qualificada(s) nesta ATA, de acordo com a classificação por ela(s) alcançada(s) e na(s) quantidade(s) cotada(s), atendendo as condições previstas no edital, sujeitando-se as partes às normas constantes na Lei nº 8.666, de 21 de junho de 1993 e suas alterações, no Decreto nº 7.892, de 23 de janeiro de 2013, e em conformidade com as disposições a seguir:

1. DO OBJETO

1.1. A presente Ata tem por objeto o registro de preços para eventual fornecimento da solução de tecnologia da informação e comunicação consistente de solução de segurança - firewall e backup - incluindo hardware, software, instalação, treinamento, suporte e garantia, pelo período de 60 (sessenta) meses com o objetivo de atender as demandas relacionadas à proteção da rede e dos dados, continuidade dos serviços da TI e recuperação de desastres especificado(s) no(s) item(ns) 01, 02 e 03 do Termo de Referência, anexo I do edital de Pregão nº 17/2022, que é parte integrante desta Ata, assim como a proposta vencedora, independentemente de transcrição.

2. DOS PREÇOS, ESPECIFICAÇÕES E QUANTITATIVOS

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

Fornecedor da solução (razão social, CNPJ/MF, endereço, contatos, representante)				
ITEM	DESCRIÇÃO/ ESPECIFICAÇÃO	Unidade de Medida	Quantidade	Valor Unitário
1				
2				
3				

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

3. ÓRGÃO(S) GERENCIADOR E PARTICIPANTE(S)

3.1. O órgão gerenciador será o Instituto Federal de Educação, Ciência e Tecnologia do Mato Grosso do Sul.

3.2. São órgãos e entidades públicas participantes do registro de preços:

Solução de segurança - Backup e Firewall					
Grupo 1 - Solução de segurança - *firewall*					
Item	**Descrição do Bem ou Serviço**	**Unidade de medida**	**Quantidade**	**UASG**	**Município/UF de entrega**
1	Solução de Firewall em Appliance - Tipo 1 (Palo Alto Networks PA-460)	unidade	2	158132 – IFMS	Campo Grande/MS
			2	155016 – Hospital Universitário Grande Dourados	Dourados/MS
			1	158144 - IFMT	Cuiabá/MT
			2	158156 - IFAC	Rio Branco/AC
2	Solução de Firewall em Appliance - Tipo 2 (Palo Alto Networks PA-440)	unidade	10	158132 – IFMS	Campo Grande/MS
			18	158144 - IFMT	Cuiabá/MT
			7	158156 - IFAC	Rio Branco/AC

			2	158127 –IFFAR	Santa Maria/RS
3	Renovação de solução de Gerenciamento de Firewall Centralizado (Panorama) para 25 dispositivos	Unidade	1	158132 – IFMS	Campo Grande/MS
			1	158144 - IFMT	Cuiabá/MT
4	Serviço de Instalação e Configuração da Solução de Firewall Tipo 1 (item 1) - ONSITE em Campo Grande/MS	unidade	1	158132 – IFMS	Campo Grande/MS
			2	155016 – Hospital Universitário Grande Dourados	Dourados/MS
			2	158156 - IFAC	Rio Branco/AC
5	Serviço de Projeto, Instalação e Configuração da Solução de Firewall Tipo 2 (item 2) - REMOTO	unidade	10	158132 – IFMS	Campo Grande/MS
			19	158144 - IFMT	Cuiabá/MT
			7	158156 - IFAC	Rio Branco/AC
			2	158127 –IFFAR	Santa Maria/RS
Grupo 2 - Solução de segurança - *backup*					
Item	**Descrição do Bem ou Serviço**	**Unidade de medida**	**Quantidade**	**UASG**	**Município/UF de entrega**
6	Software de backup com licenciamento por socket, conforme	Licença por Socket	24	158132 – IFMS	Campo Grande/MS

	descrito na especificação técnica				
7	Servidor de Backup	Unidade	2	158132 – IFMS	Campo Grande/MS
8	Serviço de Instalação e Configuração da Solução de Backup	Unidade	1	158132 – IFMS	Campo Grande/MS
9	Serviço de Treinamento Oficial do Fabricante da Solução de Backup	Unidade	4	158132 – IFMS	Campo Grande/MS

4. DA ADESÃO À ATA DE REGISTRO DE PREÇOS (item obrigatório)

4.1 Não será admitida a adesão à ata de registro de preços decorrente desta licitação.

5. VALIDADE DA ATA

5.1. A validade da Ata de Registro de Preços será de 12 meses, a partir do(a) sua assinatura, não podendo ser prorrogada.

6. REVISÃO E CANCELAMENTO

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

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

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

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

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

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

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

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

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

6.7. O registro do fornecedor será cancelado quando:

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

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

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

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

6.8. O cancelamento de registros nas hipóteses previstas nos itens 6.7.1, 6.7.2 e 6.7.4 será formalizado por despacho do órgão gerenciador, assegurado o contraditório e a ampla defesa.

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

6.9.1. por razão de interesse público; ou

6.9.2. a pedido do fornecedor.

7. DAS PENALIDADES

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

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

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

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

8. CONDIÇÕES GERAIS

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

8.2. É vedado efetuar acréscimos nos quantitativos fixados nesta ata de registro de preços, inclusive o acréscimo de que trata o § 1º do art. 65 da Lei nº 8.666/93, nos termos do art. 12, §1º do Decreto nº 7.892/13.

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

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

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

8.4. A ata de realização da sessão pública do pregão, contendo a relação dos licitantes que aceitarem cotar os bens ou serviços com preços iguais ao do licitante vencedor do certame, será anexada a esta Ata de Registro de Preços, nos termos do art. 11, §4º do Decreto n. 7.892, de 2013.

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

Local e data
Assinaturas

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

ANEXO III – MINUTA TERMO DE CONTRATO DE FORNECIMENTO DE SOLUÇÃO DE TECNOLOGIA DA INFORMAÇÃO E COMUNICAÇÃO

TERMO DE CONTRATO DE FORNECIMENTO DE SOLUÇÃO DE TECNOLOGIA DE INFORMAÇÃO E COMUNICAÇÃO Nº ...../...., QUE FAZEM ENTRE SI A UNIÃO, POR INTERMÉDIO DO (A) ..... E A EMPRESA .....

O Instituto Federal de Educação, Ciência e Tecnologia de Mato Grosso do Sul, com sede à Rua Jornalista Belizário Lima, 236, Bairro Vila Glória, na cidade de Campo Grande, inscrito no CNPJ/MF sob o nº **10.673.078/0001-20**, neste ato representado pela **Reitora Elaine Borges Monteiro Cassiano**, nomeada pelo **Decreto de 25 de Novembro de 2019**, publicado no Diário Oficial da União de 26 de novembro de 2019, portador da matrícula funcional nº 1941845 doravante denominada CONTRATANTE, e o(a) ..... inscrito(a) no CNPJ/MF sob o nº ....., sediado(a) na ....., em ..... doravante designada CONTRATADA, neste ato representada pelo(a) Sr.(a) ....., portador(a) da Carteira de Identidade nº ....., expedida pela (o) ....., e CPF nº ....., tendo em vista o que consta no Processo nº ..... 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 7.892, de 23 de janeiro de 2013*, 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 *por Sistema de Registro de Preços* nº ...../20...., mediante as cláusulas e condições a seguir enunciadas.

1. CLÁUSULA PRIMEIRA – OBJETO

1.1. O objeto do presente instrumento é a contratação de solução de tecnologia da informação e comunicação de solução de segurança - firewall e backup - incluindo hardware, software, instalação, treinamento, suporte e garantia, pelo período de 60 (sessenta) meses com o objetivo de atender as demandas relacionadas à proteção da rede e dos dados, continuidade dos serviços da TI e recuperação de desastres, 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. Objeto da contratação:

ITEM	DESCRIÇÃO/ ESPECIFICAÇÃO	Unidade de Medida	Quantidade	Valor Unitário

1				
2				
3				
...				

2. CLÁUSULA SEGUNDA – VIGÊNCIA

2.1. O prazo de vigência deste Contrato é aquele fixado no Edital, com início na data de ...../...../..... e encerramento em ...../...../....., não *podendo ser prorrogado.*

2.2. O encerramento da vigência contratual, não interrompe a obrigação de prestação da GARANTIA TÉCNICA, por 60 meses, devendo a CONTRATADA honrá-la durante todo o período estipulado.

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.

3.3. O valor acima é meramente estimativo, de forma que os pagamentos devidos à CONTRATADA dependerão dos quantitativos da solução efetivamente prestados.

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 2022, 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 – REAJUSTAMENTO DE PREÇOS EM SENTIDO AMPLO.

6.1. As regras acerca do reajustamento de preços em sentido amplo do valor contratual (reajuste em sentido estrito e/ou repactuação) são as estabelecidas no Termo de Referência, anexo a este Contrato.

7. CLÁUSULA SÉTIMA – GARANTIA DE EXECUÇÃO

7.1. Não haverá exigência de garantia de execução para a presente contratação.

8. CLÁUSULA OITAVA – MODELO DE EXECUÇÃO DO CONTRATO E FISCALIZAÇÃO

8.1. O modelo de execução do contrato, 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.

9. CLÁUSULA NONA – OBRIGAÇÕES DA CONTRATANTE E DA CONTRATADA

9.1. As obrigações da CONTRATANTE e da CONTRATADA (deveres e responsabilidades) são aquelas previstas no Termo de Referência, anexo do Edital.

10. CLÁUSULA DÉCIMA – SANÇÕES ADMINISTRATIVAS.

10.1. As sanções relacionadas à execução do contrato são aquelas previstas no Edital e no Termo de Referência, que constitui seu anexo.

11. CLÁUSULA DÉCIMA PRIMEIRA – RESCISÃO

11.1. O presente Termo de Contrato poderá ser rescindido:

11.1.1. 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;

11.1.2. amigavelmente, nos termos do art. 79, inciso II, da Lei nº 8.666, de 1993.

11.2. Os casos de rescisão contratual serão formalmente motivados, assegurando-se à CONTRATADA o direito à prévia e ampla defesa.

11.3. A CONTRATADA reconhece os direitos da CONTRATANTE em caso de rescisão administrativa prevista no art. 77 da Lei nº 8.666, de 1993.

11.4. O termo de rescisão, sempre que possível, será precedido de Relatório indicativo dos seguintes aspectos, conforme o caso:

11.4.1. Balanço dos eventos contratuais já cumpridos ou parcialmente cumpridos;

11.4.2. Relação dos pagamentos já efetuados e ainda devidos;

11.4.3. Indenizações e multas.

12. CLÁUSULA DÉCIMA SEGUNDA – VEDAÇÕES E PERMISSÕES

12.1. É vedado à CONTRATADA interromper o fornecimento da solução sob alegação de inadimplemento por parte da CONTRATANTE, salvo nos casos previstos em lei.

12.2. 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.

12.2.1. 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.

12.2.2. A 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.

13. CLÁUSULA DÉCIMA TERCEIRA – ALTERAÇÕES

13.1. 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.

13.2. 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.

13.3. 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.

14. CLÁUSULA DÉCIMA QUARTA – DOS CASOS OMISSOS

14.1. 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.

15. CLÁUSULA DÉCIMA QUINTA – PUBLICAÇÃO

15.1. 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.

16. CLÁUSULA DÉCIMA SEXTA – FORO

16.1. É eleito o Foro da Justiça Federal do MS, Seção Judiciária de Campo Grande-MS 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 em duas (duas) vias de igual teor, que, depois de lido e achado em ordem, vai assinado pelos contraentes e por duas testemunhas.

....., ... de..... de 20.....

_____

Representante legal da CONTRATANTE

_____

Representante legal da CONTRATADA

TESTEMUNHAS:

1-
2-

ANEXO IV – Estudo Técnico Preliminar - 50/2022

1. Informações Básicas

Número do processo: 23347.009360.2021-94

2. Descrição da necessidade

Contratação de solução de segurança e backup.

3. Área requisitante

Área Requisitante	Responsável
COIRT	Matheus Jardim Guerreiro da Silva

4. Necessidades de Negócio

4.1 Solução de segurança- *firewall*

A segurança da rede de dados de uma instituição é fundamental para o bom andamento das atividades cotidianas, uma vez que, quase todas as ações envolvem um computador ou dispositivo móvel conectado à rede local e à Internet. O *firewall* é o equipamento responsável pelo monitoramento, bloqueio e gerenciamento da rede e é capaz de permitir:

- A autenticação e rastreabilidade das informações de acesso dos usuários, sejam eles estudantes, professores, técnicos administrativos ou visitantes;
- A preservação da integridade e da confidencialidade dos dados dos usuários, para conformidade com a Lei Geral de Proteção de Dados (Lei nº 13.709/2018);
- O aumento do nível de qualidade e segurança dos serviços das aplicações internas do IFMS;

A proteção da infraestrutura de TI de modo a impedir que a mesma seja utilizada para uso indevido (por exemplo: utilização dos recursos computacionais para mineração de criptomoedas, *download* de conteúdo ilícito, ataques de negação de serviço - DDoS, entre outros).

4.2 Solução de segurança - *backup*

Sabe-se que atualmente os bens mais valiosos de um órgão público, assim como de uma empresa privada, são as informações institucionais. São os dados armazenados que compõem os processos, os serviços disponibilizados, as informações pessoais (de servidores e terceiros), entre outros. A necessidade de guardar essas informações de maneira segura e com possibilidade de resgate dos dados, em caso de desastres, faz com que as soluções de backup sejam fundamentais para o desenvolvimento das atividades.

Por definição, temos que backup é uma cópia de segurança de dados armazenados em dispositivos tais como: computadores, celulares, servidores de armazenamentos, pendrives, entre outros e também dados de sistemas como: softwares, páginas web etc. De maneira que essas informações possam ser resgatadas em caso de perda dos dados originais. A realização dessas cópias é algo complexo, pois, especialmente falando em backup de softwares, é necessário criar arquivos que possam ser facilmente resgatados e ao mesmo tempo que não ocupem um espaço tão grande de armazenamento. Além disso, existe a necessidade de se programar a realização automática do backup para que não exista falha (por esquecimento, por exemplo), esses e outros detalhes fazem com que a automatização dessesprocedimentos seja o caminho ideal para a realização das cópias de segurança.

Nesse sentido, vemos que o IFMS está desprovido, pois nunca houve uma aquisição de solução profissional e automatizada para realização de backups, o que nos deixa vulneráveis e bastante preocupados.

5. Necessidades Tecnológicas

5.1 Solução de segurança - *firewall*

Aquisição de equipamentos de *firewall* (*appliance*), garantia, serviço de manutenção evolutiva, atualização de versão e suporte técnico dos appliances de firewall, pelo período de 60 (sessenta) meses. Renovação do software de gerenciamento centralizado, serviço de manutenção evolutiva, atualização de versão e suporte técnico do software de gerenciamento centralizado, pelo período de 60 (sessenta) meses. Essa solução visa manter a infraestrutura de segurança de redes, atendendo as necessidades do IFMS e deve prover as mínimas funcionalidades, quais sejam:

- Permitir o bloqueio de ameaças à rede interna do IFMS;
- Permitir o bloqueio de ameaças ao *data center* do IFMS;
- Filtrar ameaças;
- NGFW (*Next Generation Firewall*);
- Identificar usuário por meio do LDAP institucional;
- Permitir a interconexão das unidades (*site-to-site*) de forma segura através de VPN (Rede Privada Virtual) dinâmica;
- Permitir, através de VPN *client-to-site*, que pessoas acessem remotamente a rede interna do IFMS;
- Propiciar análise de tráfego em tempo real;
- Propiciar gerenciamento centralizado;
- Gerar relatórios customizáveis;

Assegurar a retenção de *logs* centralizada.

5.2 Solução de segurança - *backup*

Aquisição de licenças de software de *backup*, serviço de manutenção evolutiva, atualização de versão e suporte técnico de licenças de backup, pelo período de 60 (sessenta) meses. Aquisição de servidor de dados para armazenamento de backup, serviço de manutenção evolutiva, atualização de versão e suporte técnico do servidor de dados, pelo período de 60 (sessenta) meses. Essa solução visa manter a integridade dos dados ao permitir que, em caso de perdas, os dados sejam rapidamente recuperados e deve prover as mínimas funcionalidades descritas abaixo:

- Disponibilizar proteção (*backup*) e replicação integradas em uma única solução;
- Não necessitar de instalação de agentes para poder realizar suas tarefas de proteção, recuperação e replicação das máquinas virtuais;
- Garantir, no mínimo, a proteção de máquinas virtuais e seus dados, gerenciadas através das soluções de virtualização VMware e Microsoft Hyper-V;
- Ter a capacidade de replicação de dados armazenados entre storages ou máquinas de configuração e de fabricantes diferentes;
- Proteger o ambiente, sem interromper a atividade das máquinas virtuais e sem prejudicar sua performance, facilitando as tarefas de proteção (backup) e migrações em conjunto;
- Ter a capacidade de testar a consistência do backup e replicação (S.O., aplicação, VM), emitindo relatório de auditoria para garantir a capacidade de recuperação;
- Deverá prover a deduplicação e compressão durante a operação de qualquer backup sem a necessidade de *hardware* de terceiros (*appliance* deduplicadora);
- Deverá possibilitar a cópia de uma máquina virtual completa ou discos virtuais específicos;
- Deverá ser fornecida com ferramenta de gestão de arquivos para os administradores de máquinas virtuais no console do operador;
- Deverá ter a capacidade de integração através de API's dos fabricantes de infraestrutura virtualizada para a proteção de dados.

6. Demais requisitos necessários e suficientes à escolha da solução de TIC

Não se aplica.

7. Estimativa da demanda - quantidade de bens e serviços

7.1 - Estimativa da demanda - Quantidade de bens e serviços

Atualmente, o IFMS disponibiliza uma infraestrutura de TI para atender cerca de 25.000 (vinte e cinco mil) usuários da comunidade acadêmica, sendo composta por estudantes, professores e técnicos administrativos. A equipe que cuida da segurança da informação na Reitoria, parte da Coordenação de Infraestrutura, Redes e Telecomunicação, é composta por 01 (um) analista e 04 (quatro) técnicos que são responsáveis por planejar, executar e manter políticas e medidas de garantia da segurança e da proteção da rede e dos sistemas computacionais do IFMS. Dessa forma, essa equipe atua diretamente na implementação e manutenção dos sistemas de proteção, disponibilidade, preservação e segurança dos serviços e dados, como por exemplo, o *firewall* e o *backup*.

No momento, o IFMS conta com uma solução de *firewall* de próxima geração (*Next Generation Firewall – NGFW*), solução paga, da marca Palo Alto, adquirida no último processo de aquisição de equipamentos para segurança de rede (SRP 18/2014). Esse *firewall* em produção é uma solução completa, porém está desatualizada devido ao vencimento do período de garantia. Desta forma estamos sem as atualizações de *software* necessárias e com equipamentos (*hardware*) defasados. Além disso, alguns desses equipamentos apresentaram problemas físicos e não estão funcionando ou estão com o funcionamento comprometido, o que deixa a rede do IFMS em vulnerabilidade, já que as soluções alternativas (gratuitas) não atendem a todas as necessidades de proteção demandadas pela instituição. E, com ameaças tecnológicas que surgem a todo momento, precisamos de equipamentos e *softwares* atualizados para a garantia da nossa proteção.

Houve uma tentativa de renovação das garantias dos equipamentos em 2018 (Processo 23347.005309.2018-16), frustrada devido à restrição orçamentária do IFMS à época.

Quanto ao *backup*, atualmente o IFMS realiza *backups* dos principais sistemas e serviços utilizando uma solução gratuita (o comando *rsync*) em máquinas Linux. Os arquivos são armazenados em outro local, distribuídos entre 04 (quatro) servidores das unidades (*campi*). Apesar dos *backups* serem feitos diariamente no período noturno, muitos (especialmente os dos principais serviços, que requerem um grande volume de armazenamento) não conseguem completar a operação durante a noite, avançando o próximo dia implicando em: i) lentidão no acesso a Internet e no uso da rede devido ao grande volume de dados sendo trafegados e ii) lentidão no uso dos serviços e sistemas, por conta do processamento e do acesso ao disco sendo utilizado durante o horário de pleno funcionamento da instituição, acarretando em uma grande perda de performance dos sistemas. Além disso, existe ainda um grande risco de perda dos dados, principalmente por ataques do tipo *ransomware*, como tem sido comum ultimamente, uma vez que o *backup* é uma cópia idêntica dos arquivos originais que são replicados diariamente, porém sem um sistema próprio para proteção desses dados. O IFMS possuí uma *storage* que estava sendo utilizada para armazenamento dos *backups* localmente no prédio da Reitoria, porém após diversos incidentes de perda de dados nela, não é um armazenamento em que podemos confiar, visto que a cada queda de energia ou desligamento abrupto, um ou mais discos do equipamento tem apresentado problemas, sendo necessário refazer todo o sistema de *backup* em um espaço cada vez menor. Atualmente dos 16 discos de 3TB que a storage possui, apenas 5 estão em funcionamento, o que já não é capaz de armazenar todos os dados dos nossos serviços essenciais. No raid 5 montado já foram perdidos dois discos de *hot spare* e um disco do raid, podendo ser o raid perdido novamente a qualquer momento, sendo necessário refazê-lo utilizando os discos que sobrarem, porém com menos capacidade de armazenamento. Dessa forma a solução utilizada é apenas uma forma de minimizar os impactos de uma eventual perda de dados no *data center* da Reitoria, porém sem garantias de recuperação dos dados em caso de um desastre e sem proteção aos mais diversos tipos de ataques cibernéticos que vem se tornando cada vez mais comuns, não atendendo aos objetivos
/requisitos de segurança e confiabilidade exigidos, dada a criticidade dos sistemas utilizados hoje para o IFMS, tais como SUAP e Sistema Acadêmico, cuja eventual perda de dados pode ser algo irreparável para o funcionamento da instituição.

Em auditoria sobre a efetividade dos procedimentos de backup das organizações públicas federais (TC 036.620/2020-3) realizado pelo TCU em 2021, por meio de relatório individual de autoavaliação (Processo n.º 23347.007027.2021-41), foram identificadas diversos pontos que precisam ser implementados e corrigidos com relação aos *backups* no IFMS, reforçando a necessidade da contrataçãode uma solução especialista.

O dimensionamento da solução de *firewall* foi calculado considerando a demanda atual do IFMS, acrescida de uma previsão de crescimento, o que permitirá manter a solução por mais tempo, preservando o investimento realizado.

Não existe uma Política de Backup na instituição, assim o dimensionamento da solução de *backup* foi estimado considerando a frequência dos *backups* realizados pela equipe de TI e a quantidade de armazenamento utilizada atualmente para essa finalidade conforme tabela abaixo. Acrescentamos uma margem de cerca de 30% levando em consideração que o volume de *backup* é somente de arquivos pois não fazemos o *backup* das máquinas virtuais com os arquivos do sistema operacional e demais programas instalados, além de ser feito o *backup* apenas dos servidores mais importantes para não ocupar todo o espaço disponível, deixando de realizar cópias de segurança de alguns sistemas secundários (por exemplo servidor de ftp e sistemas menores) que apesar de não críticos também é desejável que se tenha as cópias de segurança (*backup*). Assim, ao todo são necessários 96TB.

Consideramos ainda o uso de dois servidores: um para ficar hospedado no *data center* da Reitoria e outro para ser a redundância do primeiro. Este segundo ficará hospedado na sala de TI do *Campus* Campo Grande. A quantidade de licenças foi pensada considerando a quantidade de servidores que hoje armazenam os serviços que serão protegidos, com uma margem para expansão dentro da vigência do contrato.

Serviço/Sistema	Tamanho atual do arquivo de backup	Quantidade de backups realizados	Armazenamento total utilizado (aproximado)
Sistemas (SUAP, Acadêmico, AVEA, Seleção, etc.)	3,2 TB	1 (diário), 7 dias (semana)	22,4 TB
Servidores de arquivos	7,1 TB	1 (diário), 7 dias (semana)	49,7 TB
TOTAL			**72,1 TB**

7.1.1 - Estimativa da demanda - Solução de segurança - *firewall*

No caso dos *firewalls*, como se trata de substituição de equipamentos, consideramos a quantidade atual (01 por campus e 02 para a Reitoria) e ampliamos a configuração dos equipamentos em termos de processamento e capacidade de atendimento, o que permitirá a ampliação futura da infraestrutura de *links* de dados (Internet) e o aumento da quantidade de usuários e serviços na rede.

	Item	Descrição	Quantidade
Grupo 1 - Solução de segurança - *firewall*	1	**Solução de *firewall* de próxima geração em appliance (*Next Generation Firewall – NGFW*) para a Reitoria, incluindo:** • *Threat Prevention*; • ADV URL *Filtering*; • Suporte por 60 meses.	2
	2	**Solução de *firewall* de próxima geração em appliance (*Next Generation Firewall – NGFW*) para os *campi*, incluindo:** • *Threat Prevention*; • ADV URL Filtering; • Suporte por 60 meses.	10
	3	**Renovação do suporte do gerenciador de *firewall* para 25 dispositivos, por 60 meses.**	1

	4	**Serviço de instalação e configuração da solução de *firewall* - ONSITE (Campo Grande/MS)**	1
	5	**Serviço de Projeto, Instalação e Configuração da solução de *firewall* - REMOTO**	10

A tabela acima apresenta as descrições dos itens que compõem a solução de segurança - *firewall* e suas quantidades serão justificadas abaixo:

Item 1 - Solução de Segurança com *Firewall* em *Appliance* para a Reitoria:

Quando falamos em segurança da informação um ponto muito importante é a redundância. O cenário ideal para equipamentos de alta disponibilidade é trabalhar em pares, pois, caso um dispositivo apresente alguma falha o outro assume de maneira imperceptível ao usuário. Desta forma, enquanto o equipamento secundário funciona normalmente, a equipe de TI tem tempo para identificar o que houve com o equipamento primário, resolver ou acionar o suporte para solucionar o problema. O *data center* do IFMS já trabalha com a redundância de *firewall* e sem esse recurso poderíamos ter sofrido com diversas interrupções dos serviços, pois os principais serviços da instituição, tais como: Portal Institucional,Sistema Administrativo (SUAP), Sistema Acadêmico, Ambiente Virtual de Aprendizagem (Moodle),Central de Seleção, entre outros, ficam hospedados em servidores virtuais no *data center*. Por isso, foram solicitados 02 (dois) *appliances* físicos de *firewall* para a Reitoria.

Item 2 - Solução de *Firewall* em *Appliance* para os Campi:

Mesmo com os principais serviços na Reitoria, os *Campi* precisam de *firewall* para gerenciamento da rede, controle de acesso, configuração de *links*, VPN, entre outros. Nesse caso solicitamos apenas 01 (uma) unidade de *appliance* para cada localidade, por conta do alto valor de investimento, e também porque os *campi* não possuem serviços tão críticos e que necessitem de alta disponibilidade.

Item 3 - Renovação do Software do Gerenciador de *Firewall*:

Gerir implantações de segurança, com regras complexas e dados de fontes diversas, não é uma tarefa simples, principalmente com uma equipe pequena. Uma ferramenta de gerenciamento de *firewall* é fundamental para a gestão desses ativos, pois ela permite o gerenciamento centralizado e a criação de políticas consolidadas fáceis de implementar.

O IFMS utilizava o *software* de gerenciamento dos *firewalls* da Palo Alto, o Panorama, a licença já foi adquirida anteriormente, mas atualmente estamos sem atualizações e sem suporte técnico em caso de problemas. Assim, devido a falta de suporte técnico, o *software* encontra-se sem possibilidade de uso no momento. Esse serviço de suporte é fundamental, pois qualquer solução de segurança de redes é demasiadamente complexa e com esse serviço obtemos ajuda e resolução de problemas num tempo muito menor do que se o fizéssemos por conta própria.

Item 4 - Serviço de instalação e configuração da solução de firewall - ONSITE:

Como se trata de uma atualização de tecnologia, com mudança de *hardware*, é importante a contratação do serviço de instalação dos equipamentos para o início da utilização da solução. Além de todo o trabalho de configuração e adequação da solução à nossa infraestrutura local, também tem o repasse de conhecimento que a empresa precisa fazer junto à equipe de TI local.

Também, por se tratar do serviço de instalação e configuração da parte concentradora da solução de firewall e pelo procedimento ocorrer no local de ambiente de trabalho da equipe de TI local (data center da Reitoria), solicitamos que o serviço seja feito de forma ONSITE, ou seja, presencialmente em Campo Grande/MS, no data center da Reitoria do IFMS.

Item 5 - Serviço de Projeto, Instalação e Configuração da solução de firewall - REMOTO:

Seguindo a mesma proposta do item 4, é necessário o apoio técnico especializado para a instalação e configuração dos novos equipamentos e da atualização da tecnologia nas unidades dos campi. Sendo assim, solicitamos uma unidade deste serviço para cada um dos 10 campi (mesma quantidade do item 2).

Neste caso, diferentemente do item 4, a empresa prestadora de serviços poderá efetuar os trabalhos junto a equipe de TI do IFMS de forma REMOTA, sem a necessidade de estar presente nos locais.

7.1.2 - Estimativa da demanda - Solução de segurança - *backup*

Para a solução de *backup*, planejamos uma quantidade de licenças que atenda a Reitoria e uma quantidade menor para o atendimento de cada *campus*, uma vez que o licenciamento do *backup* é por *socket* de processador e a maioria dos *campi* só tem um servidor de dados com 2 processadores.

	Item	Descrição	Quantidade
Grupo 2 - Solução de segurança - *backup*	5	***Software* de *backup* – licença perpétua baseada em *socket* com suporte por 60 meses**	24
	6	**Servidor de *backup* - *appliance* de backup com garantia e suporte por 60 meses**	2
	7	**Serviço de instalação e configuração da solução de *backup***	1
	8	**Serviço de treinamento oficial do fabricante da solução de *backup***	4

A tabela acima apresenta as descrições dos itens que compõem a solução de segurança - *backup* e suas quantidades serão justificadas abaixo:

Item 5 - *Software* de Backup - Licença Perpétua Baseada em *Socket* com suporte por 60 meses:

A solução de *backup* baseada em *socket*, considera para licenciamento uma unidade de licença por processador do equipamento que terá o *software* instalado. Por isso, estamos considerando quatro licenças para a Reitoria (2 por servidor cada um com dois processadores) e duas licenças para cada *Campi*, pois nos *campi* existe um servidor principal com dois processadores.

Item 6 - Servidor de *Backup* - *Appliance* de *Backup* com Garantia e Suporte por 60 Meses:

Os servidores de *backup* são os equipamentos que armazenarão as cópias de segurança. Como todos os serviços essenciais estão concentrados no *data center* da Reitoria, solicitamos um servidor para atender o *data center* e outro para ficar como redundância em outra unidade (fora da Reitoria), garantindo assim, maior segurança no armazenamento das informações institucionais através de uma redundância destes backups em locais fisicamente separados (inclusive prédios distintos).

Item 7 - Serviço de Instalação e Configuração da Solução de Backup:

A solução é nova para a instituição, por isso é fundamental a contratação de serviço de instalação dos equipamentos e do *software* por parte do fornecedor, para o início da utilização. O serviço de instalação e configuração, da tecnologia a ser contratada, engloba entre outras coisas:

- Reunião de planejamento para criação do escopo do projeto, definição de prioridades, análise da arquitetura da rede;
- Alinhamento da instalação em modo de alta disponibilidade (os serviços não podem parar, ou devem ficar indisponíveis o menor tempo possível);
- Repasse de conhecimento no modelo *hands-on* (onde cada passo é acompanhado pela equipe de TI do IFMS que, em tradução livre, irá “aprender fazendo”);
- Testes para validação da instalação e configuração dos equipamentos.

Item 8 - Treinamento Oficial do Fabricante do *Software* de *Backup*:

A cada nova solução de TIC implantada temos um período grande de adaptação da equipe à tecnologia em que, mesmo com o repasse de conhecimento por parte do fornecedor, ainda ficam muitas dúvidas que acabam prejudicando o desenvolvimento das atividades diárias. Considerando que a equipe é pequena e que é uma tecnologia nova, entendemos que o treinamento oficial do fabricante para a solução é a forma mais adequada de capacitar a equipe para operacionalizar a tecnologia adquirida.

O treinamento deve ser realizado pelo próprio fabricante ou empresa que conste no site do fabricante como: Centro de Formação Autorizado, e o conteúdo do curso deve abranger toda a solução contratada.

O treinamento poderá ser ministrado localmente ou remotamente.

Suporte por 60 Meses:

Para a solução de segurança acima (*firewall* e *backup*) solicitamos suporte de 60 meses. Embora o valor seja incrementado com essa opção, a solução se torna mais vantajosa, pois apesar da expectativa de vida útil de um equipamento girar em torno de 8 anos, alguns podem apresentar problemas em um tempo menor, até mesmo no primeiro ano de uso, como já ocorreu aqui na instituição. Por se tratar de equipamentos de alta disponibilidade que ficam ligados 24 horas por dia, 7 dias por semana, e que utilizam boa parte de sua capacidade de processamento, o seu uso exige muito mais do *hardware* do que em equipamentos comuns. Além disso, não é só uma questão de substituição de equipamentos ou manutenção, neste serviço estão inclusas atualizações essenciais para o bom funcionamento do equipamento e também o suporte técnico (ajuda) do fabricante, que é fundamental na resolução de problemas.

Com novas ameaças sendo criadas a cada dia, é imprescindível a adoção de soluções que contemplem atualizações periódicas, além do apoio dos fabricantes em situações críticas para lidar com problemas relacionados à segurança de forma ágil e precisa a fim de evitar a perda e/ou roubo de informações.

Portanto, o serviço de suporte e garantia é uma forma de preservação do investimento realizado, pois, em caso de defeito o equipamento é substituído sem qualquer custo adicional e em caso de problemas técnicos, os especialistas do fabricante auxiliam na resolução, o que garante economia de tempo para a Instituição.

8. Levantamento de soluções

8.1 – IDENTIFICAÇÃO DAS SOLUÇÕES

Para o Grupo 1 - Solução de Segurança - *Firewall*:

Id	**Descrição da solução (ou cenário)**
1	*Firewall* baseado em *software* livre
2	*Firewall* de próxima geração (*Next Generation Firewall – NGFW*) - Nova solução
3	*Firewall* de próxima geração (*Next Generation Firewall – NGFW*) - Palo Alto

Para o Grupo 2 - Solução de Segurança - *Backup*:

Id	**Descrição da solução (ou cenário)**
1	Solução baseada em *software* livre

2	*Software* disponibilizado no Portal do Software Público Brasileiro
3	Solução de *backup* com licenciamento por *socket*

9. Análise comparativa de soluções

9.1 – IDENTIFICAÇÃO DAS SOLUÇÕES

Solução 1 - Grupo 1: *Firewall* baseado em *software* livre

Essa solução já foi utilizada como padrão em todas as unidades do IFMS e continua em funcionamento em alguns *Campi* como solução paliativa para atendimento de mais de uma localidade ou em substituição ao equipamento de *firewall* com problema. Embora existam diversas possibilidades com esse tipo de solução, hoje no IFMS não temos um servidor de TIC devidamente capacitado ou com domínio pleno dessa ferramenta, além disso, soluções livres não contam com suporte do fabricante e no caso de problemas é preciso contar com a documentação disponível, que nem sempre é completa ou atualizada, ou ainda pesquisas em outros locais, o que geralmente demanda muito tempo. Outro ponto importante aser considerado é que soluções baseadas em software livre são desenvolvidas por comunidades de voluntários, ou seja, não existe nenhuma obrigação de resolução de problemas ou prazo para desenvolvimento de *patches* (pequenas atualizações de segurança) necessárias em caso de surgimento de uma nova vulnerabilidade.

Nesse tipo de tecnologia as configurações são manuais, ou seja, existem poucas automações, o que demanda um amplo conhecimento para implementação. Fazendo ainda com que essa opção exija mais tempo dos técnicos e, consequentemente, mais recursos dispensados em aquisição de conhecimento para seu uso, uma vez que o suporte é obtido por meio da comunidade usuária e não da própria desenvolvedora (as exceções são as com suporte vendido, o que acaba tirando o sentido de estar-se utilizando um software livre justamente por ser gratuito).

Entre os recursos que não são comuns nas soluções gratuitas podemos citar algumas, tais como:

- Suporte técnico próprio da desenvolvedora dedicado à aplicação em casos de indisponibilidade e emergências, além de contato direto com a representante a fim de soluções integradas e resolução de problemas;
- Atualizações diárias automáticas de correções de vulnerabilidade ou listas de sites e *links* maliciosos;
- *Hardware* próprio dimensionado adequadamente para a utilização do *software* embutido, trazendo melhor desempenho e prevenção a falhas;
- *Software* de gerenciamento da solução presente em todos os campi além de um controle de *logs* e acessos, relatórios e ameaças em uma única solução que dê uma visão geral de todas as unidades.

Utilizando-se de uma opção de software livre, seria necessário ainda adquirir o *hardware*, que basicamente seria um computador do tipo servidor de dados, exclusivamente dedicado à função de *firewall*. Quanto à capacitação, teríamos que contratar treinamento para a maioria dos servidores técnicos de TIC, pois sabemos que a disseminação do conhecimento adquirido por cada um não é tão eficiente

sem uma capacitação, e no dia-a-dia os servidores não têm tempo para repassar as informações e parte do conhecimento acaba sendo esquecida. Ainda quanto à capacitação, hoje temos uma grande rotatividade de servidores de TIC na instituição, de forma que seria necessário a manutenção de um plano constante de capacitação para evitar que o conhecimento seja perdido.

Nossa equipe técnica já testou algumas soluções de *software* livre de *firewall*, como: **Pfsense** (https://www.pfsense.org/), **Endian firewall** (https://www.endian.com/de/community/) e o próprio **IPTBLES** (nativo nas distribuições Linux). Dentre as soluções citadas, a Pfsense foi a que mostrou os melhores resultados e, inclusive, é utilizada em algumas unidades do IFMS que tiveram problemas com o equipamento de *firewall* principal (Paloalto, que atualmente está sem suporte). Nessas soluções no ambiente de produção foram observados alguns pequenos erros (*bugs*) que exigem a reinicialização do equipamento para o funcionamento correto, como por exemplo a VPN no ambiente misto (Pfsense x Paloalto) que após iniciada não permitia o tráfego de rede pelo túnel na versão 2.5.2, em uma nova versão lançada para correção dos problemas (2.6.0) esse problema foi corrigido, porém após algum tempo funcionando, surgiu um novo problema que só é corrigido após a reinicialização do equipamento.

Solução 2 - Grupo 1: *Firewall* de próxima geração (*Next Generation Firewall – NGFW*) - Nova solução

Ao optar por uma solução ou tecnologia diferente da que está atualmente em produção deve-se levar em consideração alguns fatores como: a necessidade de reconfiguração de todos os equipamentos que trabalham em conjunto com o *firewall*, treinamento da equipe responsável por operacionalizar a nova solução na Reitoria e nos *campi*, substituição e inutilização dos equipamentos e *software* de gerenciamento atualmente em produção.

Por se tratar de uma solução de segurança, a imperícia dos servidores em operar a nova solução pode acarretar prejuízos como deixar algum serviço vulnerável a ataques cibernéticos, a perda de dados ou até mesmo a liberação de informações sensíveis da instituição.

A Instrução Normativa 01/2019 - SGD/ME orienta a verificação da vantajosidade financeira na substituição de tecnologia, para tal fizemos um levantamento de valores no painel de preços (https://paineldeprecos.planejamento.gov.br/) e as opções mais próximas em termos de configuração estavam com valores maiores do que a pesquisa de preços realizada com fornecedores para a manutenção da solução atual (Solução 3 - Grupo 1).Veja tabela abaixo:

Item	Descrição	Fonte	Marca/Modelo	Valor unitário para 12 meses	Valor unitário para 60 meses (Valor Unitário x 5 anos)
1	Solução de firewall de próxima geração em appliance (Reitoria)	Ata UASG: 158149 - Pregão SRP Nº 06/2022 - Item 2 - Grupo 1	Fortinet (contratado como serviço, por 36 meses)	R$ 37.333,33	R$ 186.666,67
		Ata UASG: 153103 - SRP Nº 62/2020 - Item 3	Fortigate FG-101F (36 meses)	R$ 39.200,00	R$ 196.000,00

2	Solução de firewall de próxima geração em appliance (campi)	Ata UASG: 158149 - Pregão SRP Nº 06/2022 - Item 1 - Grupo 1	Fortinet (contratado como serviço, por 36 meses)	R$ 6.633,33	R$ 33.166,67
		Ata UASG: 153103 - SRP Nº 62/2020 - Item 2	Fortigate FG-81F (36 meses)	R$ 14.733,33	R$ 73.666,67
3	Renovação do suporte do gerenciador de firewall para 25 dispositivos	-	-	-	-
4	Serviço de instalação e configuração da solução de firewall - ONSITE (Campo Grande/MS)	-	-	-	-
5	Serviço de Projeto, Instalação e Configuração da solução de firewall - REMOTO	-	-	-	-

Em buscas no Painel de Preços (https://paineldeprecos.planejamento.gov.br/) pelo CATMAT 150100 (Firewall), obtivemos uma lista com 19 processos de compra dentro da vigência (12 meses). Destes, apenas 13 são da esfera Federal. Analisando item a item da lista, foram descartados alguns itens cadastrados de forma equivocada. Ao final, ficaram na lista 17 itens, com um valor médio de R$352.497,84 (lembrando que cada item possui especificidades diferentes, como: marca, modelo, duração de suporte, garantia etc.). Boa parte da lista possuía itens com uma configuração muito superior a nossa necessidade e consequentemente preços mais elevados também. Alguns poucos itens, com uma configuração menor e insuficiente para o atendimento das nossas necessidades. Vale ressaltar também a grande quantidade de marcas e modelos que pudemos observar, dentre elas: Fortinet, CheckPoint, Sonicwall, CISCO, Sophos, Blockbit e Palo Alto. Dentro dos itens restantes, buscamos aqueles equipamentos que se enquadravam dentro das especificações, e que continham os requisitos e configurações necessários para o atendimento da nossa demanda. Assim, dentro dessa pesquisa, encontramos apenas duas ATAs (constantes na tabela acima) com itens de marca diferente da solução atualmente utilizada no IFMS, que continham especificações similares aos modelos de referência para o atendimento da demanda proposta, e em uma das ATAs (UASG: 158149 - Pregão SRP Nº 06/2022) a contratação não foi de aquisição do equipamento, mas sim uma contratação como serviço.

Os itens 3, 4 e 5 são muito específicos, pois estão muito atrelados a: a tecnologia utilizada, ao tamanho do parque (quantidade de equipamentos, quantidade de usuários, quantidade de conexões, banda etc.), se os equipamentos que compõem a solução foram contratados como serviço ou foi feita a compra do equipamento etc.. Em nossas pesquisas no Painel de Preços, dentro desses processos que envolviam a compra de firewall (CATMAT 150100), encontramos alguns itens de Gerenciador de Firewall (item 3) e Serviço de Instalação e Configuração de Firewall (itens 4 e 5), porém os valores variam muito de um processo para o outro, não servindo como base para cotação de preços, pois, conforme mencionado acima, são itens que dependem de outras muitas variáveis específicas do Termo de Referência de cada órgão.

Solução 3 - Grupo 1: Firewall de próxima geração (Next Generation Firewall – NGFW) - Palo Alto

Essa opção consiste na atualização da solução utilizada atualmente na instituição, com a aquisição de novos equipamentos e a renovação da licença do *software* gerenciador. Dentre as vantagens de se mantera tecnologia já utilizada, podemos citar: a familiaridade da equipe de técnicos locais com as ferramentas - consequentemente não há necessidade de contratação de treinamento, o aproveitamento dos recursos já investidos anteriormente - uma vez que é possível utilizar os equipamentos atuais como redundância ou para o atendimento à outras unidades (no caso de *campi* com mais de um endereço ou polo, por exemplo). Além disso, em levantamento de preços essa opção se mostrou mais vantajosa financeiramente.

Requisito	Solução	Sim	Não	Não se aplica
A Solução encontra-se implantada em outro órgão ou entidade da Administração Pública?	Solução 1 - Grupo 1	X		
	Solução 2 - Grupo 1	X		
	Solução 3 - Grupo 1	X		
A Solução está disponível no Portal do Software Público Brasileiro? (quando se tratar de software)	Solução 1 - Grupo 1			X
	Solução 2 - Grupo 1			X
	Solução 3 - Grupo 1			X
A Solução é composta por software livre ou software público? (quando se tratar de software)	Solução 1 - Grupo 1			X
	Solução 2 - Grupo 1			X
	Solução 3 - Grupo 1			X
A Solução é aderente às políticas, premissas e especificações técnicas definidas pelos Padrões de governo ePing, eMag, ePWG?	Solução 1 - Grupo 1			X
	Solução 2 - Grupo 1			X
	Solução 3 - Grupo 1			X
A Solução é aderente às regulamentações da ICP-Brasil? (quando houver necessidade de certificação digital)	Solução 1 - Grupo 1			X
	Solução 2 - Grupo 1			X

	Solução 3 - Grupo 1			X
A Solução é aderente às orientações, premissas e especificações técnicas e funcionais do e-ARQ Brasil? (quando o objetivo da solução abranger documentos arquivísticos)	Solução 1 - Grupo 1			X
	Solução 2 - Grupo 1			X
	Solução 3 - Grupo 1			X

Solução 1 - Grupo 2: Solução baseada em *software* livre

Essa opção consiste na busca de softwares que são baseados no conceito de software livre, licenciados sob algum modelo de licença livre compatíveis com GNU GPL (Licença Pública Geral) de maneira que atendesse às necessidades levantadas neste estudo.

Há várias soluções de software livre para *backup* disponíveis no mercado, e também, existe o fato das empresas líderes de mercado, disponibilizarem versões gratuitas de suas ferramentas com funcionalidades limitadas, voltadas mais para pequenos ambientes.

Seguem algumas das ferramentas livres disponíveis na Internet:

- **Bacula**: possui as versões *community*, que é gratuita e a versão *enterprise*, esta paga;
- **Amanda**: ela protege mais de um milhão de servidores e *desktops*, com diversas versões de sistemas operacionais Linux, UNIX, BSD, Mac OS-X e Windows, porém de pequeno porte e não fornecem suporte técnico;
- **Bareos**: é a sigla para Backup Archiving Open Sourced, uma ferramenta de *backup* desenvolvida com base no Bacula. Ele é distribuído sob a licença AGPL v3, e, por isso, qualquer um pode ter acesso ao código fonte do programa para realizar adaptações e mudanças.
- **BackupPC**: é altamente configurável e fácil de instalar e também é multiplataforma, mas está disponível apenas para Linux e Windows;

Como mencionado, as soluções listadas acima apresentam funcionalidades limitadas, direcionadas para pequenos ambientes. Todas elas já foram testadas em nosso ambiente de TIC e a que apresentou melhor desempenho foi o BackupPC, que inclusive está sendo usado atualmente para o *backups* dos dados das principais sistemas da instituição. Porém esta solução possui algumas limitações, como por exemplo:

- Não é possível fazer cópia de máquina virtual, apenas de arquivos em sistema operacional;
- O software tem a possibilidade de trabalhar com compressão do backup para economizar espaço de armazenamento, porém o tempo do backup aumenta muito, inviabilizando o seu uso;
- A ferramenta não oferece a funcionalidade de teste da cópia de segurança;
- A ferramenta apresenta problemas na cópia de servidores com grande volume de arquivos (por exemplo servidor de arquivos), apresentando erros durante o backup após longos períodos tentando realizar a cópia;
- A ferramenta possui um tempo muito alto para restauração completa dos arquivos em caso de desastre (descompactação);
- Dificuldade para realização de testes dos backups, uma vez que é necessário refazer as máquinas virtuais em um novo ambiente para poder restaurar os arquivos backupeados nessa nova máquina, um procedimento extremamente demorado e manual que consome muito tempo da equipe de TI;

- Exposição a criptografia dos dados utilizados por vírus do tipo ransomware.

Solução 2 - Grupo 2: Software disponibilizado no portal do Software Público Brasileiro

Essa alternativa consiste na busca de solução por meio do sítio eletrônico https://www.gov.br/governodigital/pt-br/software-publico, conforme especifíca a alínea "c" do inciso II do art. 11 da IN nº 01/2019. Após a consulta, constatou-se que o catálogo disponibilizado no referido site não possui *software* com características semelhantes às necessidades levantadas neste estudo, com relação à solução de *backup*.

Portanto, não foi encontrada nenhuma solução de *backup* no Portal do Software Público Brasileiro.

Solução 3 - Grupo 2: Solução com servidor de armazenamento de dados e *software* de automatização de *backup* com licenciamento por *socket*

Essa solução baseia-se na contratação de licenças de uso perpétuo e servidor de armazenamento para automatização de *backup* com recursos de segurança, redundância, garantia e suporte do *hardware* e suporte do *software*.

Existem várias soluções de *backup* proprietárias no mercado, com diferentes formatos de organização e para diferentes tamanho de demanda. Considerando a infraestrutura de TIC da nossa instituição (sua composição, tamanho, distribuição etc.), o formato da solução que melhor se encaixa é a de um software (licença/serviço) que trabalhe de forma integrada junto a um servidor físico (equipamento), garantindo assim uma solução coesa, com segurança anti-incidentes dado que possui estrutura dedicada e isolada das demais soluções que compõem a infraestrutura de TIC da instituição, com recursos próprios para sua finalidade.

Considerando nossos requisitos de armazenamento, a quantidade de servidores, a necessidade da replicação em local distinto, além dos demais requisitos técnicos, optamos por esta solução como a alternativa mais viável para o atendimento desta demanda.

Requisito	Solução	Sim	Não	Não se aplica
A Solução encontra-se implantada em outro órgão ou entidade da Administração Pública?	Solução 1 - Grupo 2	X		
	Solução 2 - Grupo 2		X	
	Solução 3 - Grupo 2	X		
A Solução está disponível no Portal do Software Público Brasileiro? (quando se tratar de software)	Solução 1 - Grupo 2		X	
	Solução 2 - Grupo 2		X	

	Solução 3 - Grupo 2		X	
A Solução é composta por software livre ou software público? (quando se tratar de software)	Solução 1 - Grupo 2	X		
	Solução 2 - Grupo 2	X		
	Solução 3 - Grupo 2		X	
A Solução é aderente às políticas, premissas e especificações técnicas definidas pelos Padrões de governo ePing, eMag, ePWG?	Solução 1 - Grupo 2			X
	Solução 2 - Grupo 2			X
	Solução 3 - Grupo 2			X
A Solução é aderente às regulamentações da ICP-Brasil? (quando houver necessidade de certificação digital)	Solução 1 - Grupo 2			X
	Solução 2 - Grupo 2			X
	Solução 3 - Grupo 2			X
A Solução é aderente às orientações, premissas e especificações técnicas e funcionais do e-ARQ Brasil? (quando o objetivo da solução abranger documentos arquivísticos)	Solução 1 - Grupo 2			X
	Solução 2 - Grupo 2			X
	Solução 3 - Grupo 2			X

10. Registro de soluções consideradas inviáveis

Conforme § 1º do art. 11, as soluções consideradas inviáveis deverão ser registradas no Estudo Técnico Preliminar da Contratação.

Para solução de segurança - *firewall*, as opções 1 e 2 são inviáveis para implementação no IFMS, sob o ponto de vista técnico e financeiro, pois apresentam funcionalidades limitadas ou custos maiores que a opção escolhida.

Para a solução de segurança - *backup*, a opção 1 é inviável por apresentar funcionalidades limitadas, voltadas mais para organizações menores. Inviável também a opção 2, visto que não foi encontrada uma solução no portal do Software Público Brasileiro com as características que atendam as necessidades desta instituição neste momento.

11. Análise comparativa de custos (TCO)

A presente seção registra comparação de Custos Totais de Propriedade para as soluções técnica e funcionalmente viáveis, nos termos do inciso III do art. 11. da IN 01.2019 SGD/ME. A identificação dos custos totais das soluções pautou-se pela obtenção de preços conforme parâmetros descritos na Instrução Normativa/ME nº 73/2020.

11.1 – CÁLCULO DOS CUSTOS TOTAIS DE PROPRIEDADE

Na análise de soluções, verificou-se que a aquisição da Solução de Segurança - Firewall e Backup, por meio de processo licitatório, na modalidade Pregão, é a solução viável no momento para o IFMS.

Após essa definição, teve início o estudo dos diferentes modos de contratação, levando-se em conta os tipos de equipamentos e licenças, conforme a aplicação e o uso, o prazo de contratação, os custos envolvidos e alguns pontos a mais, relevantes para escolha da solução a ser contratada.

A estimativa de custo foi baseada em pesquisa de preço realizada no painel de preços, em contratações similares de outros órgãos públicos e com fornecedores, tendo como observação a Instrução Normativa /ME nº 73/2020 que dispõe sobre procedimentos para realização de pesquisa de preços na Administração Pública Federal.

Para a obtenção do valor unitário estimado, foi utilizada a **média saneada**, defendida pelo professor Túlio Bastos e apresentada pelo auditor da CGU Franklin Brasil Santos, autor do citado guia de Preços Referenciais em Compras Publicas disponibilizado pelo TCU. Pois este método consegue avaliar de forma crítica os preços obtidos na pesquisa, descartando os valores que apresentam grandes variações para mais ou para menos dos demais. Segue a especificação da fórmula:

$$CV = DPM100$$

CV: coeficiente de variação

DP: desvio padrão

M: média

O coeficiente de variação deve ficar dentro de 25%, o que resulta numa pesquisa de preços homogênea.

Conforme mencionado anteriormente, em pesquisa ao Painel de Preços (https://paineldeprecos. planejamento.gov.br/) pelo CATMAT 150100 (Firewall), obtivemos uma lista com 19 processos decompra dentro da vigência (12 meses). Destes, apenas 13 são da esfera Federal. Analisando item a itemda lista, foram descartados alguns itens cadastrados de forma equivocada. Ao final, ficaram na lista 17 itens, com um valor médio de R$ 352.497,84 (lembrando que cada item possui especificidades diferentes, como: marca, modelo, duração de suporte, garantia etc.). De todos os itens, apenas um era da marca Palo Alto (Ata da Universidade Federal de Roraima - UASG: 154080 - Pregão SRP Nº 05/2021 - Item 1 - Grupo 1), porém de um modelo (PAN-PA-3260) muito superior a nossa necessidade e com um valormuito elevado também.

Assim, considerando a importância dessa contratação para o IFMS, bem como a nossa especificidade, foram feitas pesquisas diretas com fornecedores conforme Art. 5º, inciso IV da IN/ME nº 73/2020.

Abaixo, tabela com os valores encontrados na pesquisa de preços dos itens que compõem o Grupo 1 (Solução de Segurança - firewall):

Grupo 1 - Solução de segurança - *firewall*							
Item	**Descrição**	**Empresa TELTEC SOLUTIONS**	**Empresa PLUGNET**	**Empresa Planos Tecnologia**	**MÉDIA**	**DESVIO PADRÃO**	**COEFICIENTE VARIAÇÃO**
1	Solução de firewall de próxima geração em appliance (Reitoria)	R$ 176.475,15	R$ 184.915,00	R$ 189.950,00	R$ 183.780,05	R$ 5.559,32	3,02%
2	Solução de firewall de próxima geração em appliance (campi)	R$ 51.573,88	R$ 54.005,00	R$ 59.465,40	R$ 55.014,76	R$ 3.299,87	6,00%
3	Renovação do suporte do gerenciador de firewall para 25 dispositivos	R$ 98.095,00	R$ 110.490,00	R$ 118.008,35	R$ 108.864,45	R$ 8.210,45	7,54%
4	Serviço de instalação e configuração da solução de firewall - ONSITE (Campo Grande/MS)	R$ 32.000,00	R$ 35.500,00	R$ 45.000,00	R$ 37.500,00	R$ 5.492,42	14,65%
5	Serviço de Projeto, Instalação e Configuração da solução de firewall - REMOTO	R$ 15.000,00	R$ 14.050,00	R$ 17.000,00	R$ 15.350,00	R$ 1.229,50	8,01%

Na pesquisa de preços do Grupo 2, foi realizada busca no Painel de Preços (https://paineldeprecos.planejamento.gov.br/) pelo CATSER 27464, que é um código muito amplo e abrange todas as licenças de software instaladas em servidores, o que resultou numa lista com centenas de itens. Refinamos a busca usando como critério o termo “backup” presente na descrição ou objeto dos itens. Enfim, após analisar diversos pregões encontramos dois itens similares à demanda do item 5 - Grupo 2.

Depois foi realizada nova pesquisa ao Painel de Preços pelo CATMAT 457720 (Servidor), obtivemos uma lista com 7 itens de compra, todos de processos da esfera Federal, com um valor médio de R$ 196.144,57 (lembrando que cada item possui especificidades diferentes, como: marca, modelo, duração de suporte, garantia etc.).

Analisando item a item da lista, foram descartados alguns aqueles com configuração muito inferior ou muito superior, encontramos um item com configuração similar a presente demanda do item 6 - Grupo 2.

Já os itens 7 e 8 do Grupo 2 são bem específicos e estão fortemente relacionados ao item 5 do Grupo 2, de forma que seria necessário encontrar uma compra pública com um item correspondente ao item 5 e que contenha outros dois itens similares aos itens 7 e 8 para podemos utilizar para efeito de estimativa de custo. Não encontramos nenhuma compra com essa combinação.

Portanto, considerando a importância dessa contratação para o IFMS, bem como a nossa especificidade em alguns itens, foram feitas pesquisas diretas com fornecedores conforme Art. 5º, inciso IV da IN/ME nº 73/2020, para composição do mapa de preços.

Abaixo, tabelas com os valores encontrados na pesquisa de preços dos itens que compõem o Grupo 2 (Solução de Segurança - *backup*):

Grupo 2 - Solução de segurança - *backup* (média comum)											
Item	**Descrição**	**Empresa TELTEC SOLUTIONS**	**Empresa PLUGNET**	**Empresa Planos Tecnologia**	**Empresa DriveA**	**Ata 1**	**Ata 2**	**Ata 3**	**MÉDIA**	**DESVIO PADRÃO**	**COEFICIENTE VARIAÇÃO**
6	Software de backup – licença perpétua baseada em socket com suporte por 60 meses	R$ 50.560,00	R$ 54.200,00	R$ 57.500,80	R$ 21.000,00	R$ 124.750,00	R$ 43.132,56		R$ 58.523,89	R$ 31.921,78	54,54%
7	Servidor de backup - appliance de backup com garantia e suporte por 60 meses	R$ 139.692,94	R$ 321.000,00	R$ 150.795,40	R$ 242.000,00			R$ 208.000,00	R$ 212.297,67	R$ 65.986,17	31,08%
8	Serviço de instalação e configuração da solução de backup	R$ 100.000,00	R$ 112.000,00 *	R$ 91.000,00	R$ 49.000,00				R$ 88.000,00	R$ 23.717,08	26,95%
9	Serviço de treinamento oficial do fabricante da solução de backup	R$ 8.000,00	R$ 7.500,00	R$ 9.750,00	R$ 10.080,00				R$ 8.832,50	R$ 1.103,03	12,49%

Como o coeficiente de variação dos itens 5, 6 e 7 ficaram acima de 25%, foi aplicada a técnica da média saneada citada anteriormente, onde os valores que ficam acima do Limite Superior (Média + Desvio Padrão) - *destacados em laranja* - ou abaixo do Limite Inferior (Média - Desvio Padrão) - *destacados em verde* - são expurgados e uma nova média é calculada com os valores restantes.

Na tabela abaixo os valores finais já com a média saneada:

Grupo 2 - Solução de segurança - *backup* (média saneada)											

Item	Descrição	Empresa TELTEC SOLUTIONS	Empresa PLUGNET	Empresa Planos Tecnologia	Empresa DriveA	Ata 1	Ata 2	Ata 3	MÉDIA	DESVIO PADRÃO	COEFICIENTE VARIAÇÃO
6	Software de backup – licença perpétua baseada em socket com suporte por 60 meses	R$ 50.560,00	R$ 54.200,00	R$ 57.500,80	EXCLUÍDO	EXCLUÍDO	R$ 43.132,56		R$ 51.348,34	R$ 5.341,00	10,40%
7	Servidor de backup - appliance de backup com garantia e suporte por 60 meses	EXCLUÍDO	EXCLUÍDO	R$ 150.795,40	R$ 242.000,00			R$ 208.000,00	R$ 200.265,13	R$ 37.633,68	18,79%
8	Serviço de instalação e configuração da solução de backup	R$ 100.000,00	R$ 112.000,00	R$ 91.000,00	EXCLUÍDO				R$ 101.000,00	R$ 8.602,33	8,52%
9	Serviço de treinamento oficial do fabricante da solução de backup	R$ 8.000,00	R$ 7.500,00	R$ 9.750,00	R$ 10.080,00				R$ 8.832,50	R$ 1.103,03	12,49%

**No orçamento da empresa Plugnet para o item 7, o valor de R$112.000,00 ficou apenas 0,25% maior que o Limite Superior, cerca de R$283,00, portanto mantivemos o valor considerando a sua homogeneidade/proximidade aos demais.*

As Atas citadas nas duas tabelas acima são:

- **Ata 1:** UASG: 682010 - Pregão SRP nº 11/2021 - item 2 - Grupo 1;
- **Ata 2:** UASG: 255000 - Pregão SRP nº 15/2021 - item 1, e
- **Ata 3:** UASG: 70006 - Pregão SRP nº 40/2021 - item 1.

Assim, com base nos orçamentos obtidos acima, temos as soluções viáveis demonstradas nas tabelas a seguir:

Solução Viável 1: Grupo 1 - Solução de segurança - *firewall*					

Item	Descrição do Item	Uni.	Qtde	Valor Uni.	Valor Total
1	Solução de firewall de próxima geração em appliance (Reitoria)	unidade	2	R$ 183.780,05	R$ 367.560,10
2	Solução de firewall de próxima geração em appliance (campi)	unidade	10	R$ 55.014,76	R$ 550.147,60
3	Renovação do suporte do gerenciador de firewall para 25 dispositivos	unidade	1	R$ 108.864,45	R$ 108.864,45
4	Serviço de instalação e configuração da solução de firewall - ONSITE (Campo Grande/MS)	unidade	1	R$ 37.500,00	R$ 37.500,00
5	Serviço de Projeto, Instalação e Configuração da solução de firewall - REMOTO	unidade	10	R$ 15.350,00	R$ 153.500,00
			Valor Total		**R$ 1.217.572,15**

Solução Viável 2: Grupo 2 - Solução de segurança - *backup*					
Item	**Descrição do Item**	**Uni.**	**Qtde**	**Valor Uni.**	**Valor Total**
6	Software de backup – licença perpétua baseada em socket com suporte por 60 meses	Licença por Socket	24	R$ 51.348,34	R$ 1.232.360,16
7	Servidor de backup - appliance de backup com garantia e suporte por 60 meses	Unidade	2	R$ 200.265,13	R$ 400.530,26
8	Serviço de instalação e configuração da solução de backup	Unidade	1	R$ 101.000,00	R$ 101.000,00
9	Serviço de treinamento oficial do fabricante da solução de backup	Unidade	4	R$ 8.832,50	R$ 35.330,00
			Valor Total		**R$ 1.769.220,42**

11.2 – MAPA COMPARATIVO DOS CÁLCULOS TOTAIS DE PROPRIEDADE (TCO)

Solução de segurança - Backup e Firewall	**Estimativa de TCO ao longo dos anos**					**Total**
	Ano 1	**Ano 2**	**Ano 3**	**Ano 4**	**Ano 5**	

Solução Viável 1	R$ 1.217.572,15	-	-	-	-	R$ 1.217.572,15
Solução Viável 2	R$ 1.769.220,42	-	-	-	-	R$ 1.769.220,42
TOTAL	R$ 2.986.792,57	R$ 0,00	R$ 0,00	R$ 0,00	R$ 0,00	**R$ 2.986.792,57**

12. Descrição da solução de TIC a ser contratada

12.1 - *Firewall* de próxima geração (*Next Generation Firewall – NGFW*) - Palo Alto

A solução é baseada em um equipamento de segurança de rede com recursos que vão além, quando comparado a um firewall tradicional. Seus atributos são aprimorados e permitem proteger o ambiente, por ele gerenciado, das constantes e cada vez mais atuais ameaças.

Segundo *Gartner** Os firewalls de próxima geração (NGFWs) são firewalls de inspeção profunda de pacotes que vão além da inspeção e bloqueio de porta/protocolo para adicionar inspeção em nível de aplicativo, prevenção de intrusão e trazer inteligência de fora do firewall.

Entre os recursos disponíveis na solução pode-se destacar:

- Sistemas integrados de prevenção de intrusões (IPS);
- Conscientização de identidade – controle de usuário e grupo;
- Relatórios de navegação
- Recursos de firewall padrão, como inspeção com estado;
- Controle de permissões e auditoria;
- Prevenção de intrusão integrada;
- VPN;
- Reconhecimento e controle de aplicativos para bloquear ameaças;
- Controle integrado de autenticação (*Single sign-on*);
- Fontes de inteligência sobre ameaças;
- Técnicas para lidar com as ameaças à segurança em evolução;
- Entre outros.

Conforme já citado no item 3.2 ANÁLISE DE SOLUÇÕES, a opção de manter a tecnologia já utilizada na instituição, além de ser mais fácil em termos de usabilidade e adaptabilidade para a equipe de TIC local, também se mostrou mais vantajosa financeiramente. A definição dos itens segue descrita na tabela abaixo:

	Item	Descrição	Quantidade
	1	**Solução de Firewall em Appliance Palo Alto Networks PA-460, incluindo:** • Threat Prevention; • ADV URL Filtering;	2

Grupo 1 - Solução de segurança - *Firewall*		• Suporte por 60 meses.	
	2	**Solução de Firewall Em Appliance Palo Alto Networks PA-440, incluindo:** • Threat Prevention; • ADV URL Filtering; • Suporte por 60 meses.	10
	3	**Renovação do suporte do gerenciador de *firewall* para 25 dispositivos, por 60 meses.**	1
	4	**Serviço de instalação e configuração da solução de *firewall* - ONSITE (Campo Grande/MS)**	1
	5	**Serviço de Projeto, Instalação e Configuração da solução de *firewall* - REMOTO**	10

*https://www.gartner.com/en/information-technology/glossary/next-generation-firewalls-ngfws

12.2 - Solução com servidor de armazenamento de dados e software de automatização de backup com licenciamento por socket

A solução é baseada em um equipamento (servidor de rack) com recursos específicos paraarmazenamento, processamento, redundância e alta disponibilidade, juntamente com um software responsável pela automatização e gestão do(s) backup(s).

Entre os recursos disponíveis na solução pode-se destacar:

- Realização de backups e replicação de forma segura, com garantia de proteção dos dados, de forma completa (backup full) e incremental;
- Realização de backups de máquinas virtuais sem a necessidade de interrupção do serviço;
- Compressão das cópias de segurança (backups);
- Prover testes de consistência dos backups;
- Ferramenta de gestão do armazenamento e das operações de backup com interface gráfica/web;
- Backup sintético (economia de espaço e tempo);
- Sem restrição de volume de armazenamento ou tráfego;
- Notificação via e-mail dos trabalhos.

Conforme já citado no item 9.2 ANÁLISE DE SOLUÇÕES, a opção por adquirir uma solução paga e especializada com o fornecimento de um equipamento dedicado junto ao software, que juntos possibilitam a automatização do *backup* com segurança, redundância, garantia e suporte por 60 meses, se mostrou mais vantajosa para a instituição. A definição dos itens segue descrita na tabela abaixo:

	Item	Descrição	Quantidade
Grupo 2 - Solução de Segurança - *Backup*	6	**SOFTWARE DE BACKUP – LICENÇA PERPÉTUA 5 ANOS BASEADA EM SOCKET**	24
	7	**SERVIDOR DE BACKUP – SERVIDOR DE BACKUP COM GARANTIA E SUPORTE POR 60 MESES**	2
	8	**SERVIÇO DE INSTALAÇÃO E CONFIGURAÇÃO DA SOLUÇÃO DE BACKUP**	1
	9	**SERVIÇO DE TREINAMENTO OFICIAL DO FABRICANTE DA SOLUÇÃO DE BACKUP**	4

13. Estimativa de custo total da contratação

Valor (R$): 2.986.792,57

Solução de segurança - Backup e Firewall					
Grupo 1 - Solução de segurança - *firewall*					
Item	**Descrição do Item**	**Uni.**	**Qtde**	**Valor Uni.**	**Valor Total**
1	Solução de firewall de próxima geração em appliance (Reitoria)	unidade	2	R$ 183.780,05	R$ 367.560,10
2	Solução de firewall de próxima geração em appliance (campi)	unidade	10	R$ 55.014,76	R$ 550.147,60
3	Renovação do suporte do gerenciador de firewall para 25 dispositivos	unidade	1	R$ 108.864,45	R$ 108.864,45
4	Serviço de instalação e configuração da solução de firewall - ONSITE (Campo Grande/MS)	unidade	1	R$ 37.500,00	R$ 37.500,00
5	Serviço de Projeto, Instalação e Configuração da solução de firewall - REMOTO	unidade	10	R$ 15.350,00	R$ 153.500,00

Grupo 2 - Solução de segurança - *backup*					
Item	**Descrição do Item**	**Uni.**	**Qtde**	**Valor Uni.**	**Valor Total**
6	Software de backup – licença perpétua baseada em socket com suporte por 60 meses	Licença por Socket	24	R$ 51.348,34	R$ 1.232.360,16
7	Servidor de backup - appliance de backup com garantia e suporte por 60 meses	Unidade	2	R$ 200.265,13	R$ 400.530,26
8	Serviço de instalação e configuração da solução de backup	Unidade	1	R$ 101.000,00	R$ 101.000,00
9	Serviço de treinamento oficial do fabricante da solução de backup	Unidade	4	R$ 8.832,50	R$ 35.330,00
Valor Total Estimado				**R$ 2.986.792,57**	

14. Justificativa técnica da escolha da solução

A solução escolhida é a que mais se aproxima dos requisitos definidos, ou seja, aquela que melhor atende às necessidades técnicas do requisitante dentro das especificidades e limitações citadas neste estudo, sendo viável, conforme demonstrado. A solução integra proteção de rede (com o Firewall) e proteção dos dados (com o Backup), que são dois pontos que precisam de atenção dentro da atual estrutura do órgão. Parte da solução escolhida já é utilizada pela instituição, atendendo perfeitamente ao negócio, e com os serviços de projeto, instalação, configuração e treinamento solicitados, poderemos atualizar as tecnologias já utilizadas e implantar as novas.

15. Justificativa econômica da escolha da solução

A solução escolhida, descartadas as soluções inviáveis, foi a que possui os menores valores no mapa comparativo de cálculos totais de propriedade (TCO), estimando os gastos ao longo de 60 meses.

16. Benefícios a serem alcançados com a contratação

Proporcionar a continuidade dos serviços do IFMS através da manutenção de cópias de segurança, permitindo a restauração de dados e serviços em caso de perdas e desastres tecnológicos.

Proteger a rede do IFMS e garantir a confidencialidade, integridade e disponibilidade dos dados e informações, gerenciando os riscos e ameaças que possam interferir na infraestrutura da rede.

17. Providências a serem Adotadas

Não foi identificada nenhuma providência a ser adotada previamente.

18. Declaração de Viabilidade

Esta equipe de planejamento declara **viável** esta contratação.

18.1. Justificativa da Viabilidade

A presente contratação, com a aquisição da Solução Viável 1 para o Grupo 1 e da Solução Viável 2 para oGrupo 2, busca atender perfeitamente a demanda institucional, visto todo o relato no presente Estudo Técnico Preliminar, que demonstrou que as soluções viáveis encontradas são as mais vantajosas em relação às demais, principalmente pelo fator técnico (suporte e adaptação a atual infraestrutura física e de pessoal da instituição) e também, pelo fator econômico (possuem custo menor).

19. Responsáveis

MATHEUS JARDIM GUERREIRO DA SILVA
Técnico de Tecnologia da Informação

HELDER COELHO SILVA
Analista de Tecnologia da Informação

CARLITOS FIORAVANTE VIEIRA DE OLIVEIRA
Diretor de Gestão de Tecnologia da Informação

ANEXO V - DECLARAÇÃO DE INEXISTÊNCIA DE REGISTRO DE OPORTUNIDADE

Pregão Eletrônico nº. 20/2022

A empresa _____, inscrita sob o CNPJ _____, sediada em _____, declara que não realizou nenhum tipo de registro de oportunidade junto a <empresa/fornecedor XXX>, tendo ciência que esta prática é ilegal por ferir o princípio constitucional da isonomia e da seleção da proposta mais vantajosa para a Adminsitração Pública, conforme disposto na Lei nº 8.666, de 1993.

<Local>, <dia> de <mês> de <ano>.

_____
Assinatura do representante legal