PREGÃO ELETRÔNICO

Ministério da Educação
Instituto Federal de Educação, Ciência e Tecnologia de Brasília

PREGÃO ELETRÔNICO SRP Nº 18/2022
(Processo Administrativo n.º 23098.001656.2021-46)

Torna-se público, para conhecimento dos interessados, que o INSTITUTO FEDERAL DE EDUCAÇÃO, CIÊNCIA E TECNOLOGIA DE BRASÍLIA - IFB, por meio da Coordenação Geral de Aquisições -CGAQ, sediada à SAUS QUADRA 2 LOTE 03 bloco E, Edifício Siderbrás Asa Sul – Brasília/DF, CEP 70.070-906, 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: 27/062022
Horário: 10:00h
Local: Portal de Compras do Governo Federal – https://www.gov.br/compras/pt-br
Critério de Julgamento: menor preço por 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 renovação da SOLUÇÃO ANTIVIRUS KASPERSKY ENDPOINT SECURITY FOR BUSINESS - ADVANCED pelo período de 36 (trinta e seis) meses, com serviços de instalação, suporte técnico, treinamento da equipe se necessário e garantia, conforme condições, quantidades e exigências estabelecidas neste Edital e seus anexos.**

1.2 A licitação será realizada em único item.

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

2 DO REGISTRO DE PREÇOS

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

3 DO CREDENCIAMENTO

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

3.2 O cadastro no SICAF deverá ser feito no Portal de Compras do Governo Federal, no sítio 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 (SUPRESSÃO)

4.1.3 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 *(SUPRESSÃO)*

4.3 Será permitida a participação de cooperativas, desde que apresentem modelo de gestão operacional adequado ao objeto desta licitação, com compartilhamento ou rodízio das atividades de coordenação e supervisão da execução dos serviços, e desde que os serviços contratados sejam executados obrigatoriamente pelos cooperados, vedando-se qualquer intermediação ou subcontratação.

4.3.1 Em sendo permitida a participação de cooperativas, serão estendidas a elas os benefícios previstos para as microempresas e empresas de pequeno porte quando elas atenderem ao disposto no art. 34 da Lei nº 11.488, de 15 de junho de 2007.

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

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

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

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

4.5 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.

4.6 (SUPRESSÃO)

4.6.1 *(SUPRESSÃO)*

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

4.7.1 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.

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

4.7.1.2 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.

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

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

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

4.7.5 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;

4.7.6 que a proposta foi elaborada de forma independente.

4.7.7 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;

4.7.8 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.

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

4.7.1.1 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 total do item;**

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

6.2 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, apurados mediante o preenchimento do modelo de Planilha de Custos e Formação de Preços, conforme anexo deste Edital;

6.2.1 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.

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

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

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

6.4 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 unitário do item.

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

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

7.8. *(SUPRESSÃO)*

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

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

7.11. Encerrado o prazo previsto no item anterior, o sistema abrirá oportunidade para que o autor da oferta de valor mais baixo e os das ofertas com preços até dez por cento superiores àquela possam ofertar um lance final e fechado em até cinco minutos, o que será sigiloso até o encerramento deste prazo.

7.11.1. Não havendo, pelo menos, três ofertas nas condições definidas neste item poderão os autores dos melhores lances subsequentes, na ordem de classificação, até o máximo de três, oferecer um lance final e fechado até cinco minutos, o qual será sigiloso até o encerramento deste prazo.

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

7.12.1. Não havendo lance final fechado e classificado na forma estabelecida nos itens anteriores, haverá o reinício da etapa fechada para que os demais licitantes, até no máximo de três, na ordem de classificação, possam ofertar um lance final e fechado em até cinco minutos, o qual será sigiloso até o encerramento deste prazo, observando-se, após, o item anterior.

7.13. Poderá o pregoeiro, auxiliado pela equipe de apoio, justificadamente, admitir o reinício da etapa fechada, caso nenhum licitante classificado na etapa de lance fechado atender as exigências de habilitação

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/maior desconto, 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. Será assegurado o direito de preferência previsto no artigo 3º da Lei nº 8.248, de 1991, conforme procedimento estabelecido nos artigos 5° e 8° do Decreto n° 7.174, de 2010, nos seguintes termos:

7.25.1. Após a aplicação das regras de preferência para microempresas e empresas de pequeno porte, caberá a aplicação das regras de preferência, sucessivamente, para:

7.25.1.1. bens e serviços com tecnologia desenvolvida no País e produzidos de acordo com o Processo Produtivo Básico (PPB), na forma definida pelo Poder Executivo Federal;

7.25.1.2. bens e serviços com tecnologia desenvolvida no País; e

7.25.1.3. bens e serviços produzidos de acordo com o PPB, na forma definida pelo Poder Executivo Federal, nos termos do art. 5º e 8º do Decreto 7.174, de 2010 e art. 3º da Lei nº 8.248, de 1991.

7.25.2. Os licitantes classificados que estejam enquadrados no item 7.25.1.1, na ordem de classificação, serão convocados para que possam oferecer nova proposta ou novo lance para igualar ou superar a melhor proposta válida, caso em que será declarado vencedor do certame.

7.25.3. Caso a preferência não seja exercida na forma do item 7.25.1.1, por qualquer motivo, serão convocadas as empresas classificadas que estejam enquadradas no item 7.25.1.2, na ordem de classificação, para a comprovação e o exercício do direito de preferência, aplicando-se a mesma regra para o item 7.25.1.3 caso esse direito não seja exercido.

7.25.4. 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.

7.27. 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:

7.27.1.1. por empresas brasileiras;

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

7.27.1.3. 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.

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

7.29. 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.

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

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

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

7.30. 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. (SUPRESSÃO)

8.3. (SUPRESSÃO)

8.4. (SUPRESSÃO)

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

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

8.5.2. contenha vício insanável ou ilegalidade;

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

8.5.4. apresentar preço final superior ao preço máximo fixado (Acórdão nº 1455/2018-TCU – Plenário), desconto menor do que o mínimo exigido, ou que apresentar preço manifestamente inexequível.

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

8.5.4.1.1. 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.

8.5.4.1.2. (SUPRESSÃO)

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

8.7. (SUPRESSÃO)

8.8. (SUPRESSÃO)

8.8.1. (SUPRESSÃO)

8.8.2. (SUPRESSÃO)

8.8.3. (SUPRESSÃO)

8.9. 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.

8.9.1. 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.

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

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

8.10.2. (SUPRESSÃO)

8.11. (SUPRESSÃO)

8.12. (SUPRESSÃO)

8.13. (SUPRESSÃO)

8.13.1. (SUPRESSÃO)

8.13.2. (SUPRESSÃO)

8.14. 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.

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

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

8.17. 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.

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

8 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 02 (duas) horas, sob pena de inabilitação.

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

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

9.6. Se o licitante for a matriz, todos os documentos deverão estar em nome da matriz, e se o licitante for a filial, todos os documentos deverão estar em nome da filial, exceto 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 a participante sucursal, filial ou agência;

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

9.8.6. decreto de autorização, em se tratando de sociedade empresária estrangeira em funcionamento no País;

9.8.7. *(SUPRESSÃO)*

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

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

9.9. **Regularidade fiscal e trabalhista:**

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

9.9.2. prova de regularidade fiscal perante a Fazenda Nacional, mediante apresentação de certidão expedida conjuntamente pela Secretaria da Receita Federal do Brasil (RFB) e pela Procuradoria-Geral da Fazenda Nacional (PGFN), referente a todos os créditos tributários federais e à Dívida Ativa da União (DAU) por elas administrados, inclusive aqueles relativos à Seguridade Social, nos termos da Portaria Conjunta nº 1.751, de 02/10/2014, do Secretário da Receita Federal do Brasil e da Procuradora-Geral da Fazenda Nacional.

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

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

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

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

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

9.9.8. *(SUPRESSÃO)*

9.10. **Qualificação Econômico-Financeira:**

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

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

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

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

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

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

9.11. **Qualificação Técnica:**

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

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

9.11.1.1.1. **Comprovação de prestação de serviços de entrega, instalação, configuração, treinamento e suporte técnico referentes ao objeto da contratação;**

9.11.1.1.2. **A empresa licitante deverá apresentar atestado(s) que comprove, no mínimo, atendimento à 50% dos quantitativos previstos para o item pretendido**

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.

9.11.6. (SUPRESSÃO)

9.11.7. 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.

9.11.8. *(SUPRESSÃO)*

9.11.9. A LICITANTE deve anexar à proposta de preço uma declaração que manterá em seu corpo funcional, durante todo o período de suporte contratado, equipe especializada contendo, no mínimo 02 (dois) profissionais treinados e com certificação máxima disponível pelo fabricante da solução ofertada, podendo comprovar através de certificados emitidos pelo fabricante.

9.11.10. (SUPRESSÃO)

9.11.10.1. *(SUPRESSÃO)*

8.12. Em relação às licitantes cooperativas será, ainda, exigida a seguinte documentação complementar:

8.12.1. A relação dos cooperados que atendem aos requisitos técnicos exigidos para a contratação e que executarão o contrato, com as respectivas atas de inscrição e a comprovação de que estão domiciliados na localidade da sede da cooperativa, respeitado o disposto nos arts. 4º, inciso XI, 21, inciso I e 42, §§2º a 6º da Lei n. 5.764 de 1971;

8.12.2. A declaração de regularidade de situação do contribuinte individual – DRSCI, para cada um dos cooperados indicados;

8.12.3. A comprovação do capital social proporcional ao número de cooperados necessários ao fornecimento da solução;

8.12.4. O registro previsto na Lei n. 5.764/71, art. 107;

8.12.5. A comprovação de integração das respectivas quotas-partes por parte dos cooperados que executarão o contrato; e

8.12.6. Os seguintes documentos para a comprovação da regularidade jurídica da cooperativa: a) ata de fundação; b) estatuto social com a ata da assembleia que o aprovou; c) regimento dos fundos instituídos pelos cooperados, com a ata da assembleia; d) editais de convocação das três últimas assembleias gerais extraordinárias; e) três registros de presença dos cooperados que executarão o contrato em assembleias gerais ou nas reuniões seccionais; e f) ata da sessão que os cooperados autorizaram a cooperativa a contratar o objeto da licitação;

8.12.7. A última auditoria contábil-financeira da cooperativa, conforme dispõe o art. 112 da Lei n. 5.764/71 ou uma declaração, sob as penas da lei, de que tal auditoria não foi exigida pelo órgão fiscalizador.

8.13. (SUPRESSÃO)

8.13.1. (SUPRESSÃO)

8.13.2. (SUPRESSÃO)

8.13.3. (SUPRESSÃO)

8.13.4. (SUPRESSÃO)

8.13.4.1. (SUPRESSÃO)

8.13.5. (SUPRESSÃO)

8.13.6. (SUPRESSÃO)

8.13.7. (SUPRESSÃO)

8.13.8. (SUPRESSÃO)

8.14. 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.

8.15. 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.

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

8.16. 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.

8.17. 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.

8.18. 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.

8.19. 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.

8.20. 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.

8.21. (SUPRESSÃO)

8.21.1. (SUPRESSÃO)

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

9. *(SUPRESSÃO)*

9.12. *(SUPRESSÃO)*

9.13. *(SUPRESSÃO)*

9.14. *(SUPRESSÃO)*

10. DO ENCAMINHAMENTO DA PROPOSTA VENCEDORA

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

10.12.1. 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.

10.12.2. (SUPRESSÃO)

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

10.13. 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.

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

10.14. 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).

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

10.15. 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.

10.16. 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.

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

11. DOS RECURSOS

11.12. 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.

11.13. 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.

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

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

11.13.3. 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.

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

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

13. DA REABERTURA DA SESSÃO PÚBLICA

13.1. A sessão pública poderá ser reaberta:

13.1.1. 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.

13.1.2. 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.

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

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

13.2.2. 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.

14. DA ADJUDICAÇÃO E HOMOLOGAÇÃO

14.1. 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.

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

15. DA GARANTIA DE EXECUÇÃO

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

16. DA ATA DE REGISTRO DE PREÇOS

15.2 Homologado o resultado da licitação, terá o adjudicatário o prazo de 03 (três) 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.

15.3 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 03 (três) dias, a contar da data de seu recebimento, **sendo admitida assinatura digital da mesma. (INCLUSÃO)**

15.4 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.

15.5 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.

15.6 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;

17. DO TERMO DE CONTRATO OU INSTRUMENTO EQUIVALENTE

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

17.2. O adjudicatário terá o prazo de 03 (três) 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.

17.2.1. 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 03 (três) dias úteis, a contar da data de seu recebimento ou da disponibilização do acesso ao sistema de processo eletrônico.

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

17.3. (SUPRESSÃO)

17.3.1. (SUPRESSÃO)

17.3.2. (SUPRESSÃO)

17.3.3. (SUPRESSÃO)

17.4. O prazo de vigência da contratação é o previsto no instrumento contratual

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

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

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

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

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

18. DO REAJUSTAMENTO EM SENTIDO GERAL

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

19. DO MODELO DE GESTÃO DO CONTRATO

19.1. 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.

20. DAS OBRIGAÇÕES DA CONTRATANTE E DA CONTRATADA

20.1. 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.

21. DO PAGAMENTO

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

21.1.1. 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.

22. DAS SANÇÕES ADMINISTRATIVAS.

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

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

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

22.1.3. apresentar documentação falsa;

22.1.4. deixar de entregar os documentos exigidos no certame;

22.1.5. ensejar o retardamento da execução do objeto;

22.1.6. não mantiver a proposta;

22.1.7. cometer fraude fiscal;

22.1.8. comportar-se de modo inidôneo;

22.2. 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.

22.3. 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.

22.4. 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:

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

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

22.4.3. 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;

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

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

22.4.5. 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;

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

22.6. 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.

22.7. 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.

22.8. 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.

22.9. 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.

22.10. 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.

22.11. 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.

22.12. As penalidades serão obrigatoriamente registradas no SICAF.

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

23. DA FORMAÇÃO DO CADASTRO DE RESERVA

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

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

23.3. 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.

23.4. 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.

24. **DA IMPUGNAÇÃO AO EDITAL E DO PEDIDO DE ESCLARECIMENTO**

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

24.2. **A impugnação poderá ser realizada por forma eletrônica, pelo e-mail cdli.cbra@ifb.edu.br, ou por petição dirigida ou protocolada no endereço** SGAN, Módulos D, E, F e G - Asa Norte, Brasília - CEP: 70.830-450**, setor de Licitações.**

24.3. 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.

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

24.5. 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.

24.6. 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

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

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

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

25. **DAS DISPOSIÇÕES GERAIS**

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

25.2. 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.

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

25.4. 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.

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

25.6. 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.

25.7. 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.

25.8. 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.

25.9. 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.

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

25.11. **O Edital está disponibilizado, na íntegra, no endereço eletrônico www.ifb.edu.br/licitacoes, e também poderá ser lido e/ou obtido no endereço** SGAN, Módulos D, E, F e G - Asa Norte, Brasília - CEP: 70.830-450 **nos dias úteis, no horário das 09:00. horas às 18:00 horas, mesmo endereço e período no qual os autos do processo administrativo permanecerão com vista franqueada aos interessados**.

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

25.12.1. ANEXO I - Termo de Referência;

25.12.2. ANEXO II – Minuta de Ata de Registro de Preços;

25.12.3. ANEXO III – Minuta de Termo de Contrato;

25.12.4. ANEXO IV – Modelo de Proposta;

25.12.5. ANEXO V – Termo de Compromisso de Manutenção de Sigilo;

25.12.6. ANEXO VI – Termo de Ciência.

Brasília, 13 de junho de 2022.

RODRIGO MAIA DIAS LEDO

Ordenador de Despesas

MINISTÉRIO DA EDUCAÇÃO

Instituto Federal de Educação, Ciência e Tecnologia de Brasília

Anexo <XXX> do Edital

TERMO DE REFERÊNCIA

Processo Administrativo nº 23098.001656.2021-46

Histórico de Revisões

Data	Versão	Descrição	Autor
24/12/2021	1.0	Finalização da primeira versão do documento	Equipe de planejamento da contratação
28/12/2021	1.1	Revisão e finalização do documento	Equipe de planejamento da contratação
31/12/2021	1.2	Revisão solicitada pela CGAQ	Equipe de planejamento da contratação
04/01/2022	1.3	Revisão solicitada pelo Diretor de TIC	Equipe de planejamento da contratação
01/04/2022	1.4	Revisão solicitada pela CGAq quanto aos requisitos da contratação	Equipe de planejamento da contratação
19/04/2022	1.5	Alteração solicitada pela CGAq quanto prazo descrito no item 10.1	Equipe de planejamento da contratação

DIRETORIA DE TECNOLOGIA DA INFORMAÇÃO E COMUNICAÇÃO – DTIC

TERMO DE REFERÊNCIA

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

Conforme arquivo "4-termo-de-referencia-ou-projeto-basico-v2-0.odt", atualizado em 01/06/2021, e extraído do sítio https://www.gov.br/governodigital/pt-br/contratacoes/templates-e-listas-de-verificaca em 17/12/2021.

1. OBJETO DA CONTRATAÇÃO

1.1 Esta licitação tem por objeto o registro de preços para contratação de empresa especializada para prestação de serviços de renovação da SOLUÇÃO ANTIVIRUS KASPERSKY ENDPOINT SECURITY FOR BUSINESS - ADVANCED pelo período de 36 (trinta e seis) meses, com serviços de instalação, suporte técnico, treinamento da equipe se necessário e garantia conforme condições, quantidades e exigências estabelecidas neste instrumento.

2. DESCRIÇÃO DA SOLUÇÃO DE TIC

2.1 Bens e serviços que compõem a solução

Id.	Descrição do Bem ou Serviço	Código CATMAT/CATSER	Quantidade	Métrica ou Unidade
1	Licença Kaspersky Endpoint Security for Business Advanced com serviços de instalação, suporte técnico, treinamento da equipe se necessário e garantia, pelo período de 36 (trinta e seis) meses.	350949	4.402	**Unid.**

2.2 Finalidade da Solução

Item	Detalhamento da finalidade da solução
1	Software de Antivírus, para proteção de todas máquinas administrativas e de laboratórios contra pragas digitais. Garantir a segurança dos dados do parque computacional.

3. DA JUSTIFICATIVA

3.1 Contextualização e Justificativa da Contratação

3.1.1. O Instituto Federal de Brasília - IFB é uma instituição pública que oferece Educação Profissional gratuita, na forma de cursos e programas de formação inicial e continuada de trabalhadores (FIC), educação profissional técnica de nível médio e educação profissional tecnológica de graduação e de pós-graduação, articulados a projetos de pesquisa e extensão, cuja missão é oferecer ensino, pesquisa e extensão no âmbito da Educação Profissional e Tecnológica, por meio da inovação, produção e difusão de conhecimentos, contribuindo para a formação cidadã e o desenvolvimento sustentável, comprometidos com a dignidade humana e a justiça social.

3.1.2. A instituição é composta por uma Reitoria e 10 (dez) campi distribuídos pelo Distrito Federal (DF): Brasília, Ceilândia, Estrutural, Gama, Planaltina, Recanto das Emas, Riacho Fundo, Samambaia, São Sebastião e Taguatinga. Essa estrutura multicampi faculta ao IFB fixar-se em vários eixos tecnológicos, diversificando seu atendimento, em conformidade com a vocação econômica das regiões administrativas do DF.

3.1.3. Criado em dezembro de 2008, por meio da lei nº 11.892, passando a compor a Rede Federal de Educação Profissional, Científica e Tecnológica existente em todo o Brasil, o IFB vem, desde a sua criação, experimentando um processo de maturidade no qual exige grande necessidade de modernização para suportar o atual ritmo de trabalho e o nível das atividades requeridas para assegurar o cumprimento de sua missão com qualidade e de forma adequada.

3.1.4. Missão essa que é oferecer ensino, pesquisa e extensão no âmbito da Educação Profissional e Tecnológica, por meio da inovação, produção e difusão de conhecimentos, contribuindo para a formação cidadã e o desenvolvimento sustentável, comprometidos com a dignidade humana e a justiça social.

3.1.5. Dessa forma, tanto no âmbito Federal quanto no âmbito Distrital, o IFB desempenha um papel de destaque na oferta de Educação Profissional e Tecnológica, pelo qual vem sendo cobrado quanto à agilidade no cumprimento de suas ações, bem como pela necessidade de dispor de instrumentos e recursos que possam dar suporte, continuidade ou ainda, trazer inovação aos processos acadêmicos, aos de ensino-aprendizagem e aos administrativos.

3.1.6. Assim, o Plano Diretor de Tecnologia da Informação e Comunicação – PDTIC 2021-2023, tem por objetivo assegurar que as metas e objetivos de TIC estejam alinhados aos objetivos e planejamento estratégico do IFB, bem como, à Estratégia de Governança Digital - EGD.

3.1.7. Nesse sentido, a aquisição de um licenciamento de antivírus tem por objetivo prevenir que os computadores do Instituto Federal de Brasília (das áreas administrativas, acadêmicas e dos laboratórios de informática) sejam contaminados por vírus, malwares e suas variantes, e também de ameaças cibernéticas distintas que podem colocar em risco o sigilo, a integridade e a disponibilidade das informações institucionais. Com a aumento do trabalho remoto, aulas on-line, o grande volume de utilização de e-mails, acesso às páginas de internet, aos dados acadêmicos do estudante, aos fomentos e às pesquisas dos docentes, a aquisição de licenças de antivírus é necessária para oferecer um mínimo de segurança à infraestrutura de rede de computadores do Instituto. A aquisição propõe uma maior proteção aos computadores de trabalho e de laboratório, bem como aos servidores de aplicação que sustentam os serviços essenciais prestados pela instituição, resguardando-a de problemas que possam vir a prejudicar sua atividade-fim.

3.1.8. Ou seja, além das razões supracitadas e daquelas expostas no Ofício 06/2021 CITIC/DTIC/RIFB/IFBRASILIA, a natureza sensível das informações elaboradas ou tramitadas pelo Instituto Federal de Brasília – IFB impõe severos requisitos de confidencialidade, integridade, autenticidade e disponibilidade dessas informações, principalmente, frente à preocupação com o crescente número de ataques de ransomwares em órgãos da Administração Pública Federal nos dois últimos anos e se considerada a realidade que se impôs com a Pandemia da Covid-19 de trabalho remoto, na qual houve aumento do uso dos dispositivos institucionais e pessoais de forma remota. Essa nova forma de atuação exige da Instituição uma atenção maior com a Segurança da Informação e com o que a Lei Geral de Proteção de Dados (LGPD) recomenda.

3.1.9. Portanto, quando se trata de tecnologia e de segurança da informação, sempre existe a necessidade de adquirir produtos com sistemas mais avançados de detecção de ataques virtuais ou quaisquer outros programas maliciosos pulverizados pela internet. Sendo assim, visando um nível mais avançado de proteção de todos os ativos (servidores, estações de trabalho) do Instituto Federal de Brasília – IFB faz-se imperiosa a atualização da versão da solução do antivírus do IFB para o Kaspersky Endpoint Security for Business Advanced, que é uma atualização do sistema atual (Kaspersky Endpoint Security for Business Select), com melhoramento de diversas funcionalidades do antivírus, como apresentada na tabela comparativa abaixo:

COMPARATIVO DAS VERSÕES KASPERSKY SECURITY FOR BUSINESS SELECT X ADVANCED			
CARACTERÍSTICAS / FUNCIONALIDADES		**Kaspersky Endpoint Security for Business Select**	**Kaspersky Endpoint Security for Business Advanced**
	Oferece segurança multicamadas:		

	Mecanismo antimalware que combina segurança com base em assinatura, heurística e análise comportamental e tecnologias assistidas em nuvem para proteger a instituição contra ameaças conhecidas, desconhecidas e avançadas. Pode defender qualquer combinação de desktops e laptops Mac, Linux e Windows.	**X**	**X**
	Atualização da segurança: Oferece atualizações de banco de dados com muito mais frequência do que qualquer outro fornecedor de segurança. Além disso, utiliza várias tecnologias de segurança avançadas para garantir o fornecimento de taxas de detecção bastante aprimoradas com redução do tamanho das atualizações, para que uma porção maior da largura de banda para comunicação esteja disponível para outras tarefas.	**X**	**X**
	Proteção contra ameaças avançadas e desconhecidas: Quando um novo item de malware é revelado ao mundo, há um período de alto risco. Para oferecer proteção de hora zero contra essas ameaças, as tecnologias e a inteligência contra ameaças da Kaspersky Lab estão em constante evolução para garantir que a instituição fique protegida contra as novas ameaças, até mesmo as mais sofisticadas.	**X**	**X**
Proteção de desktops e	*Detecção de comportamento suspeito:* Sempre que um aplicativo é inicializado na rede corporativa, o módulo Inspetor do Sistema monitora seu comportamento. Se um comportamento suspeito for detectado, o Inspetor do Sistema bloqueará automaticamente o aplicativo. Além disso, como o Inspetor do Sistema mantém um registro dinâmico do sistema operacional, do registro etc., ele reverte automaticamente as ações mal-intencionadas que o malware implementou antes de ser bloqueado.	**X**	**X**

laptops Windows, Linux e Mac	*Proteção contra explorações:* A tecnologia Automatic Exploit Prevention (AEP) inovadora ajuda a garantir que um malware não possa explorar as vulnerabilidades dos sistemas operacionais ou aplicativos em execução na rede. A AEP monitora especificamente os aplicativos mais usados como alvo, como Adobe Reader, Internet Explorer, Microsoft Office, Java e muitos outros, para oferecer uma camada extra de proteção e monitoramento de segurança contra ameaças desconhecidas.	**X**	**X**
	Controle de aplicativos e conectividade: Para alguns aplicativos, mesmo que os aplicativos possam não ser classificados como mal-intencionados, suas atividades podem ser consideradas de alto risco. Em muitos casos, é aconselhável que essas atividades sejam restritas. O Host-Based Intrusion Prevention System (HIPS) restringe as atividades no endpoint, de acordo com o "nível de confiança" atribuído ao aplicativo. O HIPS funciona em conjunto com o firewall pessoal em nível de aplicativo, que restringe a atividade de rede.	**X**	**X**
	Bloqueio de ataques à rede: A tecnologia Network Attack Blocker detecta e monitora atividades suspeitas na rede corporativa e permite que se pré-configure a forma como os sistemas responderão se for encontrado um comportamento suspeito.	**X**	**X**
	Utilização do poder da nuvem para uma segurança ainda melhor: Com milhões de usuários deixando o Kaspersky Security Network (KSN) com base na nuvem recebendo dados sobre comportamento suspeito em seus computadores, a instituição poderá se beneficiar de proteção aprimorada contra os malwares mais recentes. Esse fluxo de dados em tempo real garante que seus clientes	**X**	**X**

	possam se beneficiar de uma resposta rápida a novos ataques e ajuda a reduzir a incidência de "falsos positivos".		
Proteção de servidores de arquivos	*Proteção de ambientes heterogêneos:* Protege servidores de arquivos que executam Windows, Linux ou FreeBSD. Os processos de verificação otimizados ajudam a garantir um impacto mínimo no desempenho de seus servidores. Além de proteger servidores de cluster, também protege servidores de terminal Microsoft e Citrix.	**X**	**X**
	Garantia de proteção confiável: No caso de um dos servidores de arquivos apresentar uma falha, as tecnologias de segurança serão automaticamente reinicializadas assim que o servidor de arquivos for reiniciado.	**X**	**X**
	Aumento da capacidade de gerenciamento: Cada minuto gasto com a administração e a geração de relatórios poderia ser dedicado a atividades estrategicamente importantes. É por isso que a solução fornece um console centralizado que permite gerenciar a segurança em todos os endpoints (servidores de arquivos, estações de trabalho e dispositivos móveis) e facilita a geração de relatórios detalhados.	**X**	**X**
	Listas brancas dinâmicas para complementar a segurança: O fornecedor investiu na criação de seu próprio Laboratório de listas brancas, que verifica os riscos de segurança de aplicativos. O banco de dados de aplicativos incluídos na lista branca contém mais de 1,3 bilhão de arquivos exclusivos e está crescendo em mais de 1 milhão de arquivos por dia. O Controle de aplicativos e Whitelist dinâmico torna mais fácil executar uma política de Default Deny que bloqueia todos os aplicativos, a menos que eles estejam em	**X**	**X**

	sua whitelist. Numa implementação ou atualização de uma política de Negação Padrão, o novo modo de teste permitirá configurar a política em um ambiente de teste, para que se possa verificar se a política está configurada corretamente, antes da "entrada em operação".		
Controle de aplicativos, dispositivos e acesso à Internet	*Prevenção da conexão de dispositivos não autorizados:* As ferramentas de Controle de dispositivos facilitam o gerenciamento dos dispositivos que têm permissão para acessar sua rede corporativa de TI. Pode-se configurar controles com base na hora do dia, na localização geográfica ou no tipo de dispositivo. Pode-se também alinhar os controles com o Active Directory – para administração granular e atribuição de política. Os administradores também podem usar máscaras na criação de regras de controle de dispositivos, para que vários dispositivos possam ser facilmente incluídos em listas brancas para uso.	**X**	**X**
	Monitoramento e controle do acesso à Internet: As ferramentas de Controle da Web permitem configurar políticas de acesso à Internet e monitorar o uso da Internet. É fácil proibir, limitar, permitir ou auditar as atividades dos usuários em sites individuais ou em categorias de sites, como sites de jogos, de apostas ou de redes sociais. Os controles de localização geográfica e de hora do dia podem ser alinhados com o Active Directory – para ajudar na administração e na definição de políticas.	**X**	**X**
	Possibilidade de controlar todas as funções em um único console: O Kaspersky Endpoint Security for Business | Advanced inclui o Kaspersky Security Center, um único console de gerenciamento unificado que garante a visibilidade e o controle de todas as tecnologias de segurança de endpoints da Kaspersky Lab que estiver		**X**

Centralização das tarefas de gerenciamento	executando. O Kaspersky Security Center permite gerenciar a segurança dos dispositivos móveis, laptops, desktops, servidores de arquivos, máquinas virtuais e muito mais, com a conveniência de um console de "painel único".		
	Oferece um nível mais alto de integração: Como o código altamente integrado resulta em produtos que proporcionam segurança, desempenho e capacidade de gerenciamento maiores, toda a funcionalidade de proteção de endpoint está contida na mesma base de códigos, para que não ocorra nenhum problema de incompatibilidade com o qual a equipe de TI da instituição tenha que lidar. Em vez disso, ela se beneficia com as tecnologias de segurança integradas com perfeição que fazem mais para proteger seu ambiente de TI, enquanto o gerenciamento centralizado economiza tempo.	**X**	**X**
	Segurança de dispositivos móveis robusta: O antiphishing oferece proteção contra sites que tentam roubar informações ou detalhes de identidade, e o antispam ajuda a filtrar chamadas e textos indesejados. As ferramentas de controle flexíveis permitem bloquear a execução de aplicativos não autorizados e o acesso a sites perigosos. O rastreamento e o bloqueio de incidentes são detectados automaticamente, e os dispositivos são bloqueados.		**X**
	Separação de dados corporativos e pessoais: A tecnologia de "empacotamento de aplicativos" permite configurar contêineres especiais em cada dispositivo. Os aplicativos corporativos são armazenados nos contêineres – totalmente separados dos dados pessoais do usuário. É possível aplicar a criptografia a todos os dados conteinerizados e impedir que os dados sejam copiados e colados fora do contêiner. Além disso, pode-se solicitar		**X**

Proteção de dispositivos móveis*	autorização de usuário adicional antes de os aplicativos conteinerizados terem permissão para serem executados. Se um servidor sair da instituição, o recurso Limpeza seletiva operado remotamente permitirá a exclusão do contêiner corporativo, sem a exclusão das configurações e dos dados pessoais do proprietário do dispositivo.		
	Suporte a plataformas comuns de MDM: Com os recursos de gerenciamento de dispositivos móveis (MDM) aprimorados, fica fácil aplicar as políticas de MDM de grupo ou individuais aos dispositivos Microsoft Exchange ActiveSync e iOS MDM, através de uma única interface. O suporte para Samsung KNOX permite gerenciar várias configurações de dispositivos Samsung.X		**X**
*Alguns recursos não estão disponíveis para algumas das plataformas móveis suportadas.	*Bloqueio, limpeza e localização de dispositivos ausentes:* Os recursos de segurança operados remotamente ajudam a proteger dados corporativos nos dispositivos ausentes. Os administradores e os usuários podem bloquear o dispositivo, excluir dados corporativos e identificar sua localização. Se um ladrão alterar o cartão SIM, o recurso Verificação do Chip enviará o novo número de telefone, para que você possa ainda executar os recursos antirroubo. O suporte a Google Cloud Messaging (GCM) ajuda a garantir que os telefones Android recebam comandos antirroubo rapidamente.		**X**
	Portal de autoatendimento: O Portal de autoatendimento facilita a ativação de dispositivos móveis pessoais na rede corporativa. Além disso, o portal oferece aos usuários acesso remoto aos principais recursos antirroubo, para que os usuários possam dar uma resposta rápida à perda de um dispositivo e reduzir o risco de perda de dados, sem sobrecarregar os		**X**

	administradores.		
	Redução da sobrecarga sobre os administradores de TI: Um console centralizado único permite gerenciar dispositivos móveis (e sua segurança) e facilita a aplicação de políticas consistentes em diferentes plataformas móveis. Além disso, o Console da Web permite gerenciar os dispositivos móveis e sua segurança, além da segurança de outros endpoints, de qualquer lugar onde você possa estar on-line.		**X**
Gerenciamento de sistemas	Gerenciamento de vulnerabilidades e correções: Detecção e priorização automatizadas de vulnerabilidades do SO e de aplicativos, combinadas com a rápida distribuição automatizada de correções e atualizações.		**X**
Inventários de hardware e software e gerenciamento de licenças	Identificação, visibilidade e controle (incluindo bloqueio), juntamente com o gerenciamento de uso da licença, fornecem informações sobre todos os softwares e hardwares implementados por todo o ambiente, incluindo dispositivos removíveis. Estão disponíveis também: gerenciamento de licenças de software e hardware, detecção de dispositivos convidados, controles de privilégios e provisionamento de acesso.		**X**
Criptografia Poderosa Proteção de dados	Criptografia dos arquivos / pastas (FLE) e do disco completo (FDE) pode ser aplicada aos endpoints. O suporte para o "modo portátil" garante a administração de criptografia em todos os dispositivos que saem dos domínios administrativos.		**X**
Conexão flexível do usuário	Autenticação pré-inicialização (Pre-boot authentication - PBA) para aumentar a segurança que inclui login único opcional para transparência do usuário. Também está disponível a autenticação com base em dois fatores ou em token.		**X**

Criação de políticas Integradas	Integração única de criptografia com controles de aplicativos e dispositivos fornece uma camada adicional de segurança aprimorada e facilidade administrativa.		**X**
Controle de acesso com base em função (Role Based Access Control — RBAC)	Responsabilidades administrativas podem ser atribuídas através de redes complexas, com exibição do console personalizada de acordo com as funções e direitos atribuídos.		**X**
Implementação do sistema operacional	Armazenamento e implementação de imagens "golden" do SO a partir de um local centralizado, incluindo suporte a UEFI.		**X**
Integração SIEM	Suporte para sistemas IBM® QRadar e HP ArcSight SIEM.		**X**
Distribuição e solução de problemas de software	Implementação e aplicação remotas do software e atualização do SO disponível por demanda ou programada. A solução de problemas remota com economia de tempo e a distribuição eficiente de software são suportadas através da tecnologia Multicast.		**X**

3.1.10. Vale destacar que, segundo o levantamento orçamentário realizado no estudo técnico preliminar, a atualização da solução de antivírus para a versão mais avançada não fere o previsto no Plano Diretor de Tecnologia da Informação e Comunicação do IFB para o triênio 2021-2023, uma vez que neste consta a previsão de valor unitário de licenciamento de aproximadamente de R$ 140,63 (cento e quarenta reais e sessenta e três centavos), e o valor médio encontrado no estudo técnico e considerado neste Termo de Referência foi de R$ 108,40 (Cento e oito reais e quarenta centavos).

3.1.11. Outros fatores preponderantes para definição da solução a ser contratada:
3.1.12. As Especificações técnicas Constam no Anexo I deste Termo de Referência.

3.2 Do Alinhamento aos Instrumentos de Planejamento Institucionais

3.2.1. Dispor de licenças em formato digital de solução em programa informático de combate a vírus cibernéticos, antivírus, que tenha a competência de detectar, monitorar e combater quaisquer atividades relacionadas à softwares maliciosos que venham ou possam vir a causar danos ao parque computacional do Instituto Federal de Brasília.

3.2.2. Atualmente, há tanto um aumento exponencial de equipamentos e soluções digitais, quanto, equitativamente, o de riscos em sua utilização. Por meio de equipamentos comprometidos ou aplicações vulneráveis, dados sensíveis podem ser expostos, usuários podem ser ludibriados e graves consequências podem emergir.

3.2.3. Dentre as diversas formas de ameaças digitais, existem tipos específicos de aplicações maliciosas, dentre elas podem-se citar *worms*, *trojans*, *spywares*, *ransomwares*, *rootkits*, *keyloggers*, *adwares*, *browser hijackers*, *phishing*, entre outros.

3.2.4. Com a massificação do uso de soluções digitais advindo ao ambiente institucional, necessita-se de solução capaz de monitorar, identificar e proteger equipamentos informáticos, a fim de assegurar integridade dos dados e oferecer o mínimo de segurança cibernética necessária aos usuários do IFB que fazem uso de equipamentos da instituição. Visto que o licenciamento atual finda em 03 de janeiro de 2022, surge a necessidade de se adquirir nova solução para auxiliar no combate a possíveis riscos.

3.2.5. A necessidade em questão está diretamente alinhada com o Plano de Desenvolvimento Institucional 2021-2023, com o Plano Diretor de Tecnologia da Informação e Comunicação vigente para o período 2021 - 2023, com a Estratégia de Governo Digital e com o Plano Anual de Contratações 2021, conforme a apresentando a seguir:

ALINHAMENTO AOS PLANOS ESTRATÉGICOS	
ID	**Objetivos Estratégicos Institucionais**
OE 1.1	Assegurar a oferta de cursos de Educação Profissional e Tecnológica alinhados às necessidades de qualificação do mundo do trabalho
OE 3.3	Fomentar e aprimorar o uso da tecnologia da informação e comunicação
ID	**Objetivos Estratégicos da EGD**
OE 2	Avaliação de satisfação nos serviços digitais
OE 11	Garantia da segurança das plataformas de governo digital e de missão crítica

ALINHAMENTO AO PDTIC 2021 - 2023			
Objetivo Estratégico 3: *Prover a infraestrutura de TIC, a conectividade, a segurança da informação e comunicação*			
ID	**Ação do PDTIC**	**ID**	**Meta do PDTIC associada**
A.3.2.E1.1.1	Apoiar o processo de contratação da solução de Software de Antivírus	M 3.2.E1	Instruir 100% dos processos de aquisição/ contratação de TIC aprovadas no PDTIC 2021-2023

ALINHAMENTO AO PAC 2021

Item	Descrição
100	LICENCIAMENTO DE DIREITOS PERMANENTES DE USO DE SOFTWARE PARA ESTAÇÃO DE TRABALHO

3.3 Da Estimativa da Demanda

3.3.1. Diante da análise quantitativa realizada no estudo técnico preliminar, constata-se que, para fins de um processo de aquisição de renovação de licenças de software de antivírus com upgrade de versão, faz-se necessário o seguinte quantitativo de licenças, distribuídos por campi e reitoria, para que a solução atenda a demanda da instituição:

Solução	Quantitativo de Licenças por Campi / Reitoria CATMAT - 350949		
	Unidade		Quantidade de Licenças
Kaspersky Endpoint Security for Business Advanced com serviços de instalação, suporte técnico, treinamento da equipe se necessário e garantia, pelo período de 36 (trinta e seis) meses.	**REIT**	**Reitoria**	**150**
	CCEI	**Campus Ceilândia**	**270**
	CEST	**Campus Estrutural**	**250**
	CGAM	**Campus Gama**	**520**
	CPLA	**Campus Planaltina**	**200**
	CSAM	**Campus Samambaia**	**370**
	CSSB	**Campus São Sebastião**	**520**
	CTAG	**Campus Taguatinga**	**520**
	CBRA	**Campus Brasília**	**727**
	CREM	**Campus Recanto das Emas**	**320**

	CRFD	**Campus Riacho Fundo**	**195**
	Total de Licenças		**4.042**

3.4 Do Não Parcelamento da Solução de TIC

3.4.1. A aquisição das licenças, deverá ser realizada em única parcela no que tange a compra. Uma vez que o mercado oferece diversas empresas na área de TI, com capacidade de atender a esta demanda.

3.5 Dos Resultados e Benefícios a Serem Alcançados

3.5.1. O resultado desejado com a contratação é manter a disponibilidade, a integridade e a confiabilidade dos dados e a continuidade dos serviços prestados pelo Instituto Federal de Brasília, de acordo com as diretrizes de segurança da informação definidas pela Instituição conforme preconizam as boas práticas e a Administração Pública Federal.

3.5.2. Assim, o IFB terá o seu parque computacional minimamente preparado tanto para sustentar o trabalho administrativo quanto para dar condições ao aprendizado prático, por meio das atividades de laboratório, com suporte ferramental tecnológico, diminuindo o analfabetismo digital ao mesmo tempo em que eleva o nível de profissional que será entregue ao mercado de trabalho.

3.5.3. Dessa forma, espera-se com a contratação:

3.5.3.1. Manter o sistema de segurança do parque computacional do IFB;

3.5.3.2. Evitar novos gastos com o processo de configuração inicial caso fosse adquirido um novo software;

3.5.3.3. Manter as atividades administrativas e educacionais desenvolvidas nos Campi /Reitoria do IFB;

3.5.3.4. Deixar o IFB mais próximo daquilo que é preconizado pela LGPD.

4. ESPECIFICAÇÃO DOS REQUISITOS DA CONTRATAÇÃO

4.1 Dos Requisitos de Negócio

4.1.1 A presente contratação orienta-se pela proteção de todas máquinas administrativas e de laboratórios contra pragas digitais para garantir a segurança dos dados do parque computacional. Está alinhado ao Planejamento Estratégico Institucional, especificamente com os objetivos estratégicos "Assegurar a oferta de cursos de Educação Profissional e Tecnológica alinhados às necessidades de qualificação do mundo do trabalho" e "Fomentar e aprimorar o uso da tecnologia da informação e comunicação".

4.2 Dos Requisitos de Capacitação

4.2.1. Faz parte do escopo da contratação a realização de capacitação técnica mínima necessária na utilização dos recursos relacionados ao objeto da presente contratação.

4.2.4. A CONTRATADA deve prestar as informações e os esclarecimentos que venham a ser solicitados pela CONTRATANTE acerca do fornecimento ou de características técnicas da solução em até 24 horas corridas, por intermédio do preposto designado para acompanhamento do contrato, a contar de sua solicitação.

4.3 Dos 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. A contratação em questão, não incide nas hipóteses vedadas pelos artigos 3º e 4º da IN SGD/ME nº 1/2019,

"Art. 3º Não poderão ser objeto de contratação:

I. *- mais de uma solução de TIC em um único contrato, devendo o órgão ou entidade observar o disposto nos §§ 2º e 3º do art. 12; e*

II. *- o disposto no art. 3º do Decreto nº 9.507, de 2018, inclusive gestão de processos de TIC e gestão de segurança da informação.*

Parágrafo único. O apoio técnico aos processos de gestão, de planejamento e de avaliação da qualidade das soluções de TIC poderá ser objeto de contratação, desde que sob supervisão exclusiva de servidores do órgão ou entidade.

Art. 4º Nos casos em que a avaliação, mensuração ou apoio à fiscalização da solução de TIC seja objeto de contratação, a contratada que provê a solução de TIC não poderá ser a mesma que a avalia, mensura ou apoia a fiscalização."

4.3.3. Cabe também registrar que o presente Termo de Referência foi elaborado a partir da observação dos guias, manuais e modelos publicados pelo órgão central do SISP em consonância com o §2° do art. 8° da Instrução Normativa n° 01/2019/SGD/ME, o qual estabelece:

"§ 2º As contratações de soluções de TIC devem atender às normas específicas dispostas no ANEXO e observar os guias, manuais e modelos publicados pelo Órgão Central do SISP.

4.4 Dos Requisitos de Manutenção - Acordo de Nível de Serviço (ANS)

4.4.1. Durante o período de vigência do contrato o CONTRATANTE terá direito, sem ônus adicional, a todas as atualizações de versão e releases dos softwares e firmwares que fazem parte da solução ofertada.

4.4.2. A CONTRATADA deverá manter o serviço de suporte técnico, disponível para a abertura e acompanhamento de chamados em tempo integral, 24 (vinte e quatro) horas por dia, 7 (sete) dias por semana, todos os dias do ano, inclusive sábados, domingos e feriados, com início de atendimento e prazo de solução de acordo com o nível de severidade exigido para o caso, conforme os índices de criticidade abaixo:

Criticidade	Descrição	Prazo Máximo de Atendimento	Prazo Máximo de Restauração de Serviço
	Sistema parado ou produto inoperante	Em até 2 horas deve ter um técnico do fornecedor On-site.	Em até 8 horas

Severidade 1 (Alta)	com impacto na operações críticas de negócio. Exemplos: Servidor de produção ou outro sistema inicial está inativo. Parte substancial dos dados essenciais corre risco de perda ou corrupção. Operações relacionadas ao negócio foram afetadas, falha que compromete a integridade geral do sistema ou dos dados.	Em até 15 min. Um Engenheiro de Suporte do fabricante deve iniciar o atendimento através de transferência ao telefone. Representante técnico especialista do suporte deve estar disponível 24x7 e ser automaticamente notificado na abertura do caso.	Entrega da Solução em até 6 dias.
Severidade 2 (Média/Alta)	Alto impacto no ambiente de produção ou grande restrição de funcionalidade. Exemplo: Ocorreu um problema no qual um recurso importante foi gravemente danificado. As operações podem continuar de forma limitada, embora a produtividade em longo prazo possa ser afetada negativamente.	Em até 4 horas deve ter um técnico do fornecedor On-site.	Em até 16 horas
		Em até 2 horas um Engenheiro de Suporte do fabricante deve iniciar o atendimento através de transferência ao telefone ou retorno de chamada. Representante técnico especialista do suporte deve estar disponível 24x7 e ser automaticamente notificado na abertura do caso.	Entrega da Solução em até 10 dias.
Severidade 3 (Média/Baixa)	O defeito não gera impacto ao negócio. Exemplo: Ocorreu um erro que causou impacto negativo limitado na operações.	Em até 8 horas deve ter um técnico do fornecedor On-site.	Em até 24 horas
		Em até 6 horas um Engenheiro de Suporte do fabricante entra em contato.	Entrega da Solução em até 15 dias ou na próxima atualização do Software.
	O problema é pequeno, ou de	Em até 12 horas um técnico do fornecedor entra em contato.	Em até 72 horas

Severidade 4 (Baixa)	documentação. Exemplos: O problema não afetou as operações da contratante negativamente; Encaminhamento de solicitações e ou sugestões para novos recursos ou aprimoramento do software licenciado.	No mesmo dia ou no próximo dia útil comercial	Entrega da Solução em até 20 dias ou considerado para as próximas atualizações do Software

4.4.3. O suporte poderá ser realizado a distância (atendimento remoto), por quaisquer meios seguros de comunicação, incluindo, telefone (0800), internet, e-mail ou "on-site" (presencial).

4.4.4. Será disponibilizado canal de atendimento e chamado técnico 24 (vinte e quatro) horas por dia, 7 (sete) dias por semana através de site na Internet e/ou canal telefônico gratuito 0800.

4.4.5. A CONTRATADA deverá fazer análises dos chamados e enviar recomendações de possíveis treinamentos necessários ao desenvolvimento da equipe da CONTRATANTE.

4.4.6. A CONTRATADA deverá apresentar relatório contendo as ações adotadas para a solução do problema.

4.4.7. A CONTRATADA deverá disponibilizar à CONTRATANTE serviço de atendimento remoto de um Gestor do contrato de Suporte, responsável este que será o ponto focal de todas as necessidades de suporte da CONTRATANTE para casos de escalações ou problemas de atendimento do Suporte Técnico. Caso a CONTRATADA tenha seus laboratórios em outros países que não seja o território nacional, o Gestor deverá ter fluência na língua para facilitar a comunicação entre as partes.

4.5 Dos Requisitos Temporais

4.5.1. O prazo de fornecimento e ativação das licenças, será de até 20 (vinte) dias corridos,a contar do recebimento da Ordem de Serviço (OS) Anexo VI do TR, emitida pela CONTRATANTE, podendo ser prorrogada, excepcionalmente, por até igual período, desde que justificado previamente pela CONTRATADA e autorizado pela CONTRATANTE..

4.5.2. As licenças descritas neste documento deverão ser entregues, preferencialmente, de forma eletrônica com links para download dos softwares, bem como as respectivas documentações dos softwares adquiridos em formato impresso ou digital.

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

4.6 Dos Requisitos de Segurança e Privacidade

4.6.1. A CONTRATADA deverá obedecer aos procedimentos operacionais adotados pela CONTRATANTE, no tocante à segurança e privacidade;

4.6.2. 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.

4.6.3. 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 Dos Requisitos Sociais, Ambientais e Culturais

4.7.1. A documentação e os manuais da solução deverão ser apresentados no idioma Português (Brasil), eventualmente poderão ser apresentados em inglês. Todos os contatos para gerenciamento de chamados e suporte técnico deverão ser realizados em Português (Brasil).

4.8 Dos Requisitos de Arquitetura Tecnológica

4.8.1. A arquitetura tecnológica da solução deverá observar os requisitos específicos de cada item de acordo com as especificações técnicas constante no ANEXO I deste Termo de Referência.

4.9 Dos Requisitos de Projeto e de Implementação

4.9.1. A Contratada deverá apresentar o projeto de instalação que deverá ser aprovado pela CONTRATANTE. O projeto deverá incluir uma proposta de cronograma.

4.9.2. Após a aprovação do projeto de instalação, a empresa vencedora procederá com a instalação da solução para a realização dos testes de funcionamento, na presença e supervisão de técnicos da Coordenação de Infraestrutura de TIC do CONTRATANTE, sendo, posteriormente, aferido e testado o seu perfeito funcionamento.

4.9.3. Compreende-se, nesta etapa, a instalação de softwares e aplicativos pela CONTRATADA, bem como a migração das configurações existentes na CONTRATANTE, caso haja, para implementação da solução.

4.10 Dos Requisitos de Implantação

4.10.1. Não se aplica para o objeto da presente contratação.

4.11 Dos Requisitos de Garantia e Manutenção

4.11.1. O período de licenciamento do software será de 36 (trinta e seis) meses, com suporte técnico remoto de 08 (oito) por horas por dia, (cinco) dias por semana. Durante o período de licenciamento o fabricante deve garantir o funcionamento do software, com suporte técnico prestado em caso de falha.

4.11.2. A garantia da solução deverá cobrir, em toda vigência do licenciamento, a atualização de versões, releases, componentes (bibliotecas, filtros, etc.) e módulos dos produtos. Todos os produtos deverão ter o mesmo período de licenciamento.

4.11.3. A CONTRATADA deverá disponibilizar ao IFB mecanismos para que os técnicos do Órgão possam solicitar diretamente ao fabricante as mídias ou as autorizações para download das versões/atualizações, 36 meses de suporte prestado diretamente pelo fabricante.

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

4.11.5. O acionamento do serviço de assistência técnica em GARANTIA deverá estar disponível preferencialmente por meio de central telefônica DDG (0800), diretamente via website do fabricante ou do fornecedor), Correio Eletrônico (e-mail do fabricante ou do fornecedor), em língua portuguesa (Português-BR), para

operacionalização da abertura de chamados e fornecimento de número de protocolo a fim de realizar o acompanhamento e monitoramento das solicitações.

4.11.6. 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.

4.11.7. 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.

4.11.8. Os atendimentos técnicos deverão ser registrados, cabendo à CONTRATADA apresentar RELATÓRIO DE VISITA TÉCNICA (ou equivalente), nele constando a descrição clara dos problemas identificados e os procedimentos adotados para a sua resolução, além de outras informações que se façam necessárias.

4.11.9. 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.

4.11.10. Nos casos em que não for possível solucionar problemas remotamente e/ou por telefone, para fins de atendimento técnico presencial, a CONTRATADA deverá observar o cumprimento dos prazos máximos de solução estipulados neste documento, cuja contagem se iniciará a partir do registro da solicitação do serviço de assistência técnica

4.12 Dos Requisitos de Experiência Profissional

4.12.1. Os profissionais componentes da equipe de implantação da solução por parte da CONTRATADA deverão ser devidamente qualificados pelo fabricante da solução ou pela Contratada.

4.12.2. A comprovação deverá ser feita através da apresentação de certificados de capacitação emitidos em nome do profissional

4.13 Dos Requisitos de Formação da Equipe

4.13.1. A CONTRATADA deverá possuir em seu quadro funcional pelo menos 02 (dois) profissionais treinados e com certificação máxima disponível pelo fabricante da solução ofertada, podendo comprovar por meio de certificados emitidos pelo fabricante e cópia da carteira de trabalho. Esta solicitação visa garantir que a CONTRATADA tenha plenas condições de elaborar/acompanhar o processo de instalação/configuração do objeto da licitação, juntamente com o profissional designado pela CONTRATANTE, assim como manter o nível de suporte técnico necessário durante toda a vigência do contrato.

4.13.2. A Contratada será responsável pelo fornecimento do software e gestão dos recursos humanos e materiais necessários para a prestação do suporte técnico.

4.14 Dos Requisitos de Metodologia de Trabalho

4.14.1. O fornecimentos da solução está condicionado ao recebimento pela CONTRATADA de Ordem de Serviço (OS) - Anexo VI do TR, emitida pela CONTRATANTE.

4.14.2. A CONTRATADA deve prestar serviço de assistência técnica para a solução objeto desta contratação no local original de fornecimento do produto constante da OS, conforme condições prevista na sessão específica de assistência técnica deste Termo de Referência.

4.14.3. A CONTRATADA deve fornecer meios para contato e registro de ocorrências do funcionamento do serviço contratado, da seguinte forma: com funcionamento 24 horas por dia e 7 dias

por semana de maneira eletrônica e por via telefônica.

4.14.4. O andamento do fornecimento da solução deve ser acompanhado pela CONTRATADA, que dará ciência de eventuais acontecimentos à CONTRATANTE.

4.14.5. A Contratante será a responsável pela verificação da aderência aos padrões de qualidade exigidos dos produtos entregues.

4.14.6. A Contratada será responsável pelo fornecimento do software e gestão dos recursos humanos e materiais necessários para a prestação do suporte técnico.

4.14.7. O fornecimento das licenças, será feito por meio de acesso ao site do fabricante, a área de acesso exclusivo da CONTRATANTE, por meio de credenciais específicas, e verificação das licenças e quantidades disponibilizadas frente à quantidade e tipos de licenças constantes da Ordem de Serviço.

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

4.15 Dos Requisitos de Segurança da Informação e Privacidade

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 IFB durante a prestação dos serviços.

4.15.4. A Contratada deverá obedecer aos procedimentos operacionais adotados pela contratante, no tocante à segurança e privacidade.

4.15.5. A Contratada deverá respeitar a Política de Segurança da Informação e Comunicações (POSIC) do Instituto Federal de Brasília bem como demais políticas e normas internas que poderão ser instituídas durante a vigência do contrato.

4.15.6. 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.

4.15.7. A Contrata deverá 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.

4.15.8. A Contratada deverá 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.

4.15.9. 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 III. A Contratada deverá providenciar a assinatura do Termo de Ciência, disponível no ANEXO IV, por todos os seus colaboradores que estejam relacionados com a execução do projeto.

4.15.10. O Termo de Compromisso e o Termo de Ciência deverão ser entregues assinados durante a reunião inicial.

4.15.11. 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.

4.16 Dos Outros Requisitos Aplicáveis

4.16.1. Nos termos do Capítulo V (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 Dos Deveres e Responsabilidades da CONTRATANTE

5.1.1. 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, posterior, recebimento definitivo.

5.1.2. Observar e fazer cumprir fielmente o que estabelece este Termo de Referência, em particular no que se refere aos níveis mínimos de serviço especificados.

5.1.3. Exigir o cumprimento de todas as obrigações assumidas pela CONTRATADA, de acordo com as cláusulas contratuais avençadas.

5.1.4. Providenciar as assinaturas pela CONTRATADA no Termo de Compromisso de Manutenção de Sigilo e Respeito às Normas de Segurança e no Termo de Ciência da Declaração de Manutenção de Sigilo.

5.1.5. Garantir, quando necessário, o acesso dos empregados da CONTRATADA às dependências da CONTRATANTE, para execução dos serviços referentes ao objeto contratado, após o devido cadastramento dos referidos empregados.

5.1.6. Prestar as informações e esclarecimentos relativos ao objeto desta contratação que venham a ser solicitado pelo preposto da CONTRATADA.

5.1.7. Nomear Gestor e Fiscais Técnico, Administrativo e Requisitante do contrato para acompanhar e fiscalizar a execução do contrato.

5.1.8. Acompanhar e fiscalizar o cumprimento das obrigações da CONTRATADA, por intermédio de 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.

5.1.9. Dirimir as dúvidas que surgirem no curso da prestação dos serviços por intermédio do Gestor ou fiscal do Contrato designados para tanto.

5.1.10. Encaminhar formalmente a demanda por meio de Ordem de Serviço, de acordo com os critérios estabelecidos neste Termo de Referência.

5.1.11. Receber o objeto fornecido pela contratada que esteja em conformidade com a proposta aceita e as especificações deste TR, conforme inspeções realizadas.

5.1.12. Realizar, no momento da licitação e sempre que possível, diligências e/ou Teste de Homologação da Amostra com o LICITANTE classificado provisoriamente em primeiro lugar, para fins de comprovação de atendimento das especificações técnicas, exigindo, no caso do fornecimento de bens, a descrição em sua proposta da marca e modelo dos bens ofertados.

5.1.13. Notificar a CONTRATADA por escrito da ocorrência de eventuais imperfeições, falhas ou irregularidades verificadas no objeto fornecido, fixando prazo para que seja substituído, reparado ou corrigido; certificando-se que as soluções por ela propostas sejam as mais adequadas.

5.1.14. Efetuar o pagamento à CONTRATADA no valor correspondente ao fornecimento do objeto, de acordo com as condições contratuais, no prazo e condições estabelecidas neste Termo de Referência, e no caso de cobrança indevida, glosar os valores considerados em desacordo com o contrato.

5.1.15. Após a notificação da glosa, a CONTRATADA terá prazo de 15 dias corridos para questionar os valores glosados, sob pena de aceitação da glosa.

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

5.1.17. Não praticar atos de ingerência na administração da CONTRATADA, tais como:

5.1.17.1. 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;

direcionar a contratação de pessoas para trabalhar nas empresas contratadas;

5.1.17.2 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.

5.1.18. Fornecer por escrito as informações necessárias para o desenvolvimento do objeto do contrato.

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

5.1.20. 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.

5.1.21. Aplicar à CONTRATADA as sanções administrativas regulamentares e contratuais cabíveis, comunicando ao órgão gerenciador da Ata de Registro de Preços, quando aplicável, assegurando à CONTRATADA a ampla defesa e o contraditório.

5.1.22. Liquidar o empenho e efetuar o pagamento à CONTRATADA, dentro dos prazos preestabelecidos em contrato.

5.1.23. Comunicar à CONTRATADA todas e quaisquer ocorrências relacionadas com o fornecimento da solução de TIC.

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

5.2 Dos Deveres e Responsabilidades da CONTRATADA

5.2.1. Cumprir todas as obrigações constantes no Edital, seus anexos e sua proposta, assumindo como exclusivamente seus os riscos e as despesas decorrentes da boa e perfeita execução do objeto.

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

5.2.3. O objeto deve estar acompanhado do manual do usuário, com uma versão em português e da relação da rede de assistência técnica autorizada.

5.2.4. Responsabilizar-se pelos vícios e danos decorrentes do objeto, de acordo com os artigos 12, 13 e 17 a 27, do Código de Defesa do Consumidor (Lei nº 8.078, de 11 de setembro de 1990).

5.2.5. Comunicar à CONTRATANTE, no prazo máximo de 72 (setenta e duas) horas que antecede a data da entrega, os motivos e justificativas que impossibilitem o cumprimento do prazo previsto, com a devida comprovação.

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

5.2.7. Executar o objeto do certame em estreita observância dos ditames estabelecido pela Lei nº 13.709, de 14 de agosto de 2018 (Lei Geral de Proteção de Dados Pessoais - LGPD).

5.2.8. A Contratada deverá disponibilizar em até 10 (dez) dias úteis da assinatura do contrato, preferencialmente, em sítio eletrônico as informações referentes ao encarregado da credenciada responsável pela proteção de dados em relação ao objeto deste Termos de Referência, nos termos do art. 41 da Lei nº 13.709, de 2018.

5.2.9. Executar o objeto contratual conforme especificações deste Termo de Referência e de sua proposta, com a alocação dos empregados necessários ao perfeito cumprimento das cláusulas contratuais.

5.2.10. Fornecer a solução contratada, na qualidade e quantidade adequadas especificadas neste Termo de Referência e em sua proposta.

5.2.11. Fornecer, sempre que solicitado, amostra para a realização de Homologação do Bem para fins de comprovação de atendimento das especificações técnicas.

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

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

5.2.14. 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.

5.2.15. Prestar as informações e os esclarecimentos que venham a ser solicitados pela Contratante por intermédio de preposto designado para acompanhamento do contrato nos seguintes prazos, a contar de sua solicitação em até 2 dias úteis.

5.2.16. Indicar formalmente e por escrito, no prazo máximo de 5 dias úteis após a assinatura do contrato, junto à CONTRATANTE, um preposto idôneo com poderes de decisão para representar a CONTRATADA, principalmente no tocante à eficiência e agilidade da execução do objeto deste Termo de Referência, e que deverá responder pela fiel execução do contrato.

5.2.17. Na hipótese de afastamento do preposto definitivamente ou temporariamente, a CONTRATADA deverá comunicar ao Gestor do Contrato por escrito o nome e a forma de comunicação de seu substituto até o fim do próximo dia útil.

5.2.18. Ter conhecimento do Gestor do Contrato, bem como outros servidores que forem indicados pela CONTRATANTE, para realizar as solicitações relativas aos contratos a serem firmados.

5.2.19. Apresentar Nota Fiscal/Fatura com a descrição dos bens fornecidos, nas condições deste Termo de Referência, como forma de dar início ao processo de pagamento pela CONTRATANTE.

5.2.20. Atender prontamente quaisquer orientações e exigências da Equipe de Fiscalização do Contrato, inerentes à execução do objeto contratual.

5.2.21. Assumir as responsabilidades pelos encargos fiscais e comerciais resultantes da adjudicação da licitação oriunda deste Termo de Referência.

5.2.22. Responsabilizar-se pelo cumprimento por todas as obrigações trabalhistas, sociais, previdenciárias, tributárias e as demais previstas em legislação específica, cuja inadimplência não transfere a responsabilidade à CONTRATANTE.

5.2.23. Assumir inteira responsabilidade técnica e operacional do objeto contratado, não podendo, sob qualquer hipótese, transferir a outras empresas a responsabilidade por quaisquer problemas relacionados ao fiel cumprimento do contrato.

5.2.24. Caso o problema de funcionamento do bem e ou serviço detectado tenha a sua origem fora do escopo do objeto contratado, a CONTRATADA repassará para a CONTRATANTE as informações técnicas com a devida análise fundamentada que comprovem o fato, sem qualquer ônus para a CONTRATANTE.

5.3 Dos 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:

5.3.3.1. as formas de comunicação entre os envolvidos, a exemplo de ofício, telefone, e-mail, ou sistema informatizado, quando disponível; e

5.3.3.2. 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

5.3.4.3. 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 Rotina 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 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.

6.1.1.3. A pauta desta reunião observará, pelo menos:

6.1.1.3.1. 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.

6.1.1.3.2. Apresentação das declarações/certificados do fabricante, comprovando que o produto ofertado possui a garantia solicitada neste termo de referência.

6.1.2 DA EXECUÇÃO DO CONTRATO

6.1.2.1. O gestor do contrato emitirá a Ordem de serviço (OS) Anexo VI do TR, para a entrega dos bens desejadosAs licenças descritas neste documento deverão ser entregues, preferencialmente, de forma eletrônica com links para download dos softwares, bem como as respectivas documentações dos softwares adquiridos em formato impresso ou digital.

6.1.2.2. 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.

6.1.2.3. Os bens poderão ser rejeitados, no todo ou em parte, quando em desacordo com as especificações constantes neste Termo de Referência e na proposta, devendo ser substituídos no prazo de 10 (dez) dias corridos, a contar da notificação da contratada, às suas custas, sem prejuízo da aplicação das penalidades.

6.1.2.4. O recebimento provisório será realizado pelo FISCAL TÉCNICO do CONTRATO quando da entrega do OBJETO resultante da ORDEM DE SERVIÇO 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 no item 7.1 deste Termo de Referência.

6.1.2.5. 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:

6.1.2.6.1. A avaliação da qualidade realizada a partir da aplicação de listas de verificação e de acordo com os critérios de aceitação definidos em CONTRATO;

6.1.2.6.2. Verificação de aderências aos requisitos e especificações técnicas;

6.1.2.6.3. Identificação de eventuais não conformidade com os termos contratuais;

6.1.2.6.4. Verificação de aderência aos termos contratuais, a cargo do Fiscal Administrativo do CONTRATO;

6.1.2.6.5. Verificação da manutenção das condições classificatórias referentes à pontuação obtida e à habilitação técnica, a cargo dos Fiscais Administrativo e Técnico do CONTRATO;

6.1.2.6.6. Encaminhamento à CONTRATADA das eventuais demandas de correção, a cargo do GESTOR do CONTRATO ou, por delegação de competência, do Fiscal Técnico do CONTRATO;

6.1.2.6.7. 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.

6.1.2.12. 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.

6.2 **Quantidade Mínima de Bens ou Serviços para Comparação e Controle**

6.2.1. Nos termos do art. 67 Lei nº 8.666, de 1993, será designado representante para acompanhar e fiscalizar a entrega dos bens, anotando em registro próprio

todas as ocorrências relacionadas com a execução e determinando o que for necessário à regularização de falhas ou defeitos observados.

6.2.2. A fiscalização de que trata este item não exclui nem reduz a responsabilidade da CONTRATADA, inclusive perante terceiros, por qualquer irregularidade, ainda que resultante de imperfeições técnicas ou vícios redibitórios, e, na ocorrência desta, não implica em corresponsabilidade da Administração ou de seus agentes e prepostos, de conformidade com o art. 70 da Lei nº 8.666, de 1993.

6.2.3. O representante da Administração anotará em registro próprio todas as ocorrências relacionadas com a execução do contrato, indicando dia, mês e ano, bem como o nome dos funcionários eventualmente envolvidos, determinando o que for necessário à regularização das falhas ou defeitos observados e encaminhando os apontamentos à autoridade competente para as providências cabíveis.

6.2.4. Quantidade mínima de bens ou serviços para comparação e controle:

6.2.4.1. As quantidades estimadas por localidade constam no item 3.3.1 deste Termo de Referência. Tais quantitativos serão consolidados e definidos após a Intenção de Registro de Preços (IRP) que será realizada a fim de definir a volumetria dessa contratação.

6.3 Mecanismos Formais de Comunicação

6.3.1. São definidos como mecanismos formais de comunicação, entre a CONTRATANTE e a CONTRATADA, os seguintes: Ordem de Serviço; Ata de Reunião; Ofício; Sistema de abertura de chamados; E-mails e Cartas.

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 III e IV.

7. MODELO DE GESTÃO DE CONTRATO

7.1 Critérios De Aceitação

7.1.1. A avaliação das entregas realizadas será feita mediante verificação da aderência às políticas, normas, padrões, procedimentos e processos em vigor no ambiente do CONTRATANTE. Assim, de modo geral, os serviços entregues serão avaliados segundo os critérios de qualidade, completude, consistência e forma, considerando:

7.1.1.1. *Critério de Qualidade:* os serviços serão avaliados com base em sua conformidade com relação às especificações técnicos e os níveis mínimos de serviço estabelecidos pelo CONTRATANTE, conforme a aplicabilidade para cada item da solução;

7.1.1.2. *Critério de Completude:* os serviços serão avaliados com base em sua completude em relação a etapas, tarefas ou resultados definidos pelo CONTRATANTE

7.1.1.3. *Critério de Consistência*: serão considerados inconsistentes os serviços que apresentarem desconformidade em relação aos processos internos do CONTRATANTE; e

7.1.1.4. *Critério de Forma:* os serviços serão avaliados no que tange à conformidade com padrões pré-estabelecidos pelo CONTRATANTE. Serão considerados em desacordo todos os serviços entregues com não conformidades relacionadas à padrões, formas de entrega e outras inadequações de natureza técnica definidos pela CONTRATANTE

7.1.2. Bens e/ou Serviços que não atendam às especificações e/ou aos níveis mínimos de qualidade e/ou serviços inconsistentes e/ou bens/serviços incompletos serão rejeitados. Serviços desformatados poderão ser aceitos com restrição, implicando compromisso da CONTRATADA em solucionar as restrições impreterivelmente no tempo determinado pelo CONTRATANTE, sob pena de não recebimento (rejeição) e/ou aplicação de sanções previstas em CONTRATO.

7.1.3. Orientações adicionais quanto à completude, consistência e forma serão disponibilizadas pelo CONTRATANTE no momento adequado, assim como as exigências concernentes à etapas, tarefas e documentação técnica serão fixadas em termo hábil (em ORDEM DE SERVIÇO, por exemplo).

7.2 Procedimentos de Teste e Inspeção

7.2.1. A inspeção da solução fornecida será realizada por meio de comparação das especificações constantes dos prospectos do fabricante da solução.

7.2.2. Ao CONTRATANTE reserva-se o 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 são indicadores mensuráveis estabelecidos pelo órgão/entidade para aferir objetivamente os resultados pretendidos com a contratação. São considerados para a presente contratação os seguintes indicadores:

IAE – INDICADOR DE ATRASO DE ENTREGA DE OS		
Tópico	**Descrição**	
Finalidade	Medir o tempo de atraso na entrega dos produtos e serviços constantes na Ordem de Serviço.	
Meta a cumprir	**IAE < = 0**	A meta definida visa garantir a entrega dos produtos e serviços constantes nas Ordens de Serviço dentro do prazo previsto.
Instrumento de medição	Através das ferramentas disponíveis para a gestão de demandas, por controle próprio da Contratante e lista de Termos de Recebimento Provisório e Definitivo emitidos.	
Forma de acompanhamento	A avaliação será feita conforme linha de base do cronograma registrada na OS. Será subtraída a data de entrega dos produtos da OS (desde que o fiscal técnico reconheça aquela data, com registro em Termo de Recebimento Provisório) pela data de início da execução da OS.	
Periodicidade	Mensalmente, para cada Ordem de Serviço encerrada e com Termo de Recebimento Definitivo.	
	IAE = $\frac{TEX - TEST}{TEST}$	

Mecanismo de Cálculo (métrica)	Onde: **IAE** – Indicador de Atraso de Entrega da OS; **TEX** – Tempo de Execução – corresponde ao período de execução da OS, da sua data de início até a data de entrega dos produtos da OS. A data de início será aquela constante na OS; caso não esteja explícita, será o primeiro dia útil após a emissão da OS. A data de entrega da OS 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 OS 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 OS – constante na OS, conforme estipulado no Termo de Referência.
Observações	Obs1: Serão utilizados dias úteis na medição. Obs2: Os dias com expediente parcial no órgão/entidade serão considerados como dias úteis no cômputo do indicador. Obs3: Não se aplicará este indicador para as OS 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 OS.

7.4 DAS SANÇÕES ADMINISTRATIVAS E PROCEDIMENTOS PARA RETENÇÃO OU GLOSA NO PAGAMENTO

7.4.1. A licitante que, convocada dentro do prazo de validade da sua proposta, não assinar a Ata ou o Contrato, deixar de entregar documentação exigida no Edital, apresentar documentação falsa, não mantiver a proposta, fraudar na execução do contrato, comportar-se de modo inidôneo, fizer declaração falsa ou cometer fraude fiscal ficará impedida de licitar e de contratar com a União e será descredenciado no SICAF, pelo prazo de até 5 (cinco) anos, sem prejuízo das multas e demais cominações legais.

7.4.2. Pela recusa em assinar a Ata, o Contrato, ou retirar a Nota de Empenho, no prazo máximo de 5 (cinco) dias úteis, após a regular convocação, a licitante poderá ser penalizada com multa no percentual de 5% (cinco por cento), calculada sobre o valor total estimado do Contrato, sem prejuízo da aplicação de outras sanções previstas no parágrafo anterior.

7.4.3. Comete infração administrativa nos termos da Lei nº 10.520, de 17 de julho de 2002, a CONTRATADA que:

7.4.3.1. Não executar total ou parcialmente qualquer das obrigações assumidas em decorrência da contratação;

7.4.3.2. ensejar o retardamento da execução do objeto;

7.4.3.3. falhar ou fraudar na execução do contrato;

7.4.3.4. comportar-se de modo inidôneo; Ou

7.4.3.5. cometer fraude fiscal.

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

7.4.4.1. Advertência por escrito, quando do não cumprimento de quaisquer das obrigações contratuais consideradas faltas leves, assim entendidas aquelas que não acarretam prejuízos significativos para o serviço contratado.

7.4.4.2. Multa, quando do não cumprimento de quaisquer das obrigações contratuais consideradas faltas moderadas ou graves, assim entendidas aquelas que acarretam prejuízos para o serviço contratado.

7.4.4.3. As penalidades de multa decorrentes de fatos diversos serão consideradas independentes entre si.

7.4.4.4. 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.

7.4.4.5. Sanção de impedimento de licitar e contratar com órgãos e entidades da União, com o consequente descredenciamento no SICAF pelo prazo de até cinco anos.

7.4.4.6. 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.

7.4.5. As sanções previstas nos subitens 7.4.4.1, 7.4.4.4, 7.4.4.5 e 7.4.4.6 poderão ser aplicadas à CONTRATADA juntamente com as de multa, descontando-a dos pagamentos a serem efetuados.

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

7.4.6.1. tenham sofrido condenação definitiva por praticar, por meio dolosos, fraude fiscal no recolhimento de quaisquer tributos;tenham praticado atos ilícitos visando a frustrar os objetivos da licitação;

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

7.4.7. 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.

7.4.8. 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.

7.4.9. Caso a CONTRATANTE determine, a multa deverá ser recolhida no prazo máximo de 10 (dez) dias úteis, a contar da data do recebimento da comunicação enviada pela autoridade competente.

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

7.4.11. 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.

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

7.4.13. 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 2013, seguirão seu rito normal na unidade administrativa.

7.4.14. O processamento do Processo Administrativo de Responsabilização (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.

7.4.15. As penalidades serão obrigatoriamente registradas no SICAF.

Id	Ocorrência	Glosa/Sanção
1	Não comparecer injustificadamente à Reunião Inicial.	Advertência. Em caso de reincidência, 0,5% sobre o valor total do Contrato.
2	Quando convocado dentro do prazo de validade da sua proposta, não celebrar o Contrato, deixar de entregar ou apresentar documentação falsa exigida para o certame, ensejar o retardamento da execução de seu objeto, não manter a proposta, falhar ou fraudar na execução do Contrato, comportar-se de modo inidôneo ou cometer fraude fiscal.	A Contratada ficará impedida de licitar e contratar com a União, Estados, Distrito Federal e Municípios e, será descredenciada no SICAF, ou nos sistemas de cadastramento de fornecedores a que se refere o inciso XIV do art. 4º da Lei nº 10.520/2002, pelo prazo de até 5 (cinco) anos, sem prejuízo das demais cominações legais, e multa de 5% do valor da contratação.
3	Ter praticado atos ilícitos visando frustrar os objetivos da licitação.	A Contratada será declarada inidônea para licitar e contratar com a Administração.
4	Demonstrar não possuir idoneidade para contratar com a Administração em virtude de atos ilícitos praticados.	Suspensão temporária de 6 (seis) meses para licitar e contratar com a Administração, sem prejuízo da Rescisão Contratual.
5	Não executar total ou parcialmente os serviços previstos no objeto da contratação.	Suspensão temporária de 6 (seis) meses para licitar e contratar com a Administração, sem prejuízo da Rescisão Contratual.
6	Suspender ou interromper, salvo motivo de força maior ou caso fortuito, os serviços solicitados, por até de 30 dias, sem comunicação formal ao gestor do Contrato.	Multa de 5% sobre o valor total do Contrato. Em caso de reincidência, configura-se inexecução total do Contrato por parte da empresa, ensejando a rescisão contratual unilateral.

7	Suspender ou interromper, salvo motivo de força maior ou caso fortuito, os serviços solicitados, por mais de 30 (trinta) dias, sem comunicação formal ao gestor do contrato.	Contratada será declarada inidônea para licitar e contratar com a Administração, sem prejuízo da Rescisão Contratual.
8	Não prestar os esclarecimentos imediatamente, referente à execução dos serviços, salvo quando implicarem em indagações de caráter técnico, hipótese em que serão respondidos no prazo máximo estabelecido neste Termo de Referência	Advertência. Em caso de reincidência, 0,5% sobre o valor total do Contrato.
12	Comprometer intencionalmente o sigilo das informações armazenadas nos sistemas da contratante.	A Contratada será declarada inidônea para licitar ou contratar com a Administração Pública, sem prejuízo às penalidades decorrentes da inexecução total ou parcial do contrato, o que poderá acarretar a rescisão do Contrato, sem prejuízo das demais penalidades previstas na Lei nº 8.666, de 1993.
13	Não atender ao indicador de nível de serviço IAE (Indicador de Atraso de Entrega de OS)	Glosa de 0,33% de atraso sobre o valor de cada licença e/ou serviço em atraso até o limite de 10% para valores do indicador IAL de 0,1 a 0,30.
		Multa de 2% sobre o valor OS, sem prejuízo da aplicação da glosa definida na faixa anterior para valores do indicador IAL acima de 0,30.
14	Não cumprir qualquer outra obrigação contratual não citada nesta tabela.	Advertência. Em caso de reincidência ou configurado prejuízo aos resultados pretendidos com a contratação, aplica-se multa de 0,5% do valor total do Contrato.

7.5 DO PAGAMENTO

7.5.1. O pagamento será efetuado pela CONTRATANTE no prazo de 30 dias corridos, contados do recebimento da Nota Fiscal/Fatura, por meio de ordem bancária, para crédito em banco, agência e conta corrente indicados pelo contratado.

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

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

7.5.4. A emissão da Nota Fiscal/Fatura será precedida do recebimento definitivo do serviço, conforme previsto neste Termo de Referência.

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

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

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

7.5.8. O setor competente para proceder o pagamento deve verificar se a Nota Fiscal/Fatura apresentada expressa os elementos necessários e essenciais do documento, tais como: o prazo de validade; a data da emissão; os dados do contrato e do órgão contratante; o período de prestação dos serviços; o valor a pagar; e eventual destaque do valor de retenções tributárias cabíveis.

7.5.9. Nos termos do item 1, do Anexo VIII-A da Instrução Normativa SEGES/MP nº 05, de 2017, será efetuada a retenção ou glosa no pagamento, proporcional à irregularidade verificada, sem prejuízo das sanções cabíveis, caso se constate que a CONTRATADA:

7.5.9.1. não produziu os resultados acordados;

7.5.9.2. deixou de executar as atividades contratadas, ou não as executou com a qualidade mínima exigida;

7.5.9.3. deixou de utilizar os materiais e recursos humanos exigidos para a execução do serviço, ou utilizou-os com qualidade ou quantidade inferior à demandada.

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

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

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

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

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

7.5.15. Persistindo a irregularidade, a CONTRATANTE deverá adotar as medidas necessárias à rescisão contratual nos autos do processo administrativo correspondente, assegurada à CONTRATADA a ampla defesa.

7.5.16. Havendo a efetiva execução do objeto, os pagamentos serão realizados normalmente, até que se decida pela rescisão do contrato, caso a contratada não

regularize sua situação junto ao SICAF.

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

7.5.18. Quando do pagamento, será efetuada a retenção tributária prevista na legislação aplicável, em especial a prevista no artigo 31 da Lei 8.212, de 1991, nos termos do item 6 do Anexo XI da IN SEGES/MP n. 5/2017, quando couber.

7.5.19. É vedado o pagamento, a qualquer título, por serviços prestados ou fornecimento de bens, à empresa privada que tenha em seu quadro societário servidor público da ativa do órgão CONTRATANTE, com fundamento na Lei de Diretrizes Orçamentárias vigente.

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

EM = I x N x VP, sendo:

EM = Encargos moratórios;
N = Número de dias entre a data prevista para o pagamento e a do efetivo pagamento;

VP = Valor da parcela a ser paga.

I = Índice de compensação financeira diário= ,00016438, assim apurado:

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

8. ESTIMATIVA DE PREÇOS DA CONTRATAÇÃO

Solução	Quantitativo de Licenças por Campi / Reitoria CATMAT - 350949				
	Unidade		Quantidade de Licenças	Valor Unitário R$	Valor Total R$
Kaspersky Endpoint	REIT	Reitoria	150	108,40	16.260,00
	CCEI	Campus Ceilândia	270	108,40	29.268,00
	CEST	Campus Estrutural	250	108,40	27.100,00

Security for Business Advanced com serviços de instalação, suporte técnico, treinamento da equipe se necessário e garantia, pelo período de 36 (trinta e seis) meses.	CGAM	Campus Gama	520	108,40	56.368,00
	CPLA	Campus Planaltina	200	108,40	21.680,00
	CSAM	Campus Samambaia	370	108,40	40.108,00
	CSSB	Campus São Sebastião	520	108,40	56.368,00
	CTAG	Campus Taguatinga	520	108,40	56.368,00
	CBRA	Campus Brasília	727	108,40	78.806,80
	CREM	Campus Recanto das Emas	320	108,40	34.688,00
	CRFD	Campus Riacho Fundo	195	108,40	21.138,00
	Total de Licenças		**4.042**		**438.152,80**

9. ADEQUAÇÃO ORÇAMENTÁRIA E CRONOGRAMA FÍSICO-FINANCEIRO

9.1 Gestão/Unidade: 26428 / 158143 20RL Funcionamento das Instituições da Rede Federal de Educação Profissional, Científica e Tecnológica - Fonte: 81000000.

10. DA VIGÊNCIA DO CONTRATO

10.1 O CONTRATO decorrente da ATA REGISTRO DE PREÇOS (ARP) terá vigência de 36 (trinta e seis) meses, a contar de sua assinatura.

10.2 O início da execução contratual fica condicionado à apresentação da garantia contratual fiduciária constante deste Termo de Referência. O encerramento da vigência contratual não interrompe a obrigação de prestação da GARANTIA TÉCNICA, devendo a CONTRATADA honrá-la durante todo o período estipulado.

11. DO REAJUSTE DE PREÇO

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

11.2 Dentro do prazo de vigência do contrato e mediante solicitação da contratada, os preços contratados poderão sofrer reajuste após o interregno de um ano, aplicando-se o Índice de Custos de Tecnologia da Informação – ICTI exclusivamente para as obrigações iniciadas e concluídas após a ocorrência da anualidade.

11.3 Nos reajustes subsequentes ao primeiro, o interregno mínimo de um ano será contado a partir dos efeitos financeiros do último reajuste.

11.4 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.

11.5 Nas aferições finais, o índice utilizado para reajuste será, obrigatoriamente, o definitivo.

11.6 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.

11.7 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.

11.8 O reajuste será realizado por apostilamento.

12. DOS CRITÉRIOS DE SELEÇÃO DO FORNECEDOR

12.1 Regime, Tipo E Modalidade Da Licitação

12.1.1. Quanto ao tipo, em conformidade com o art. 1° da Lei n° 10.520/2002 e com o Decreto n° 10.024/2019, o OBJETO pretendido enquadra-se como “BEM COMUM” por apresentar, independentemente de sua complexidade, “padrões de desempenho e qualidade que possam ser objetivamente definidos pelo edital, por meio de especificações usuais no mercado”.

12.1.2. A presente contratação adotará como regime de execução a Empreitada por Preço Global.

12.1.3. De acordo com o §1º do Art. 1º do Decreto nº 10.024, de 20 de setembro de 2019, esta licitação deve ser realizada na modalidade de PREGÃO NA FORMA ELETRÔNICA, com julgamento pelo critério de MENOR PREÇO.

12.1.4. O Modo de Disputa será ABERTO E FECHADO conforme justificado no Estudo Técnico Preliminar e definindo no Decreto n° 10.024/2019.

12.1.5. A Lei n° 8.666/1993, em seu inc. II do art. 15, estabelece que *“as compras,sempre que possível, deverão ser processadas através de sistema de registro de preços*" - assim definido como o "*conjunto de procedimentos para registro forma de preços relativos à prestação de serviços e aquisição de bens para contratações futuras*" (Decreto n" 7.892/2013, art. 1", I). À luz do princípio da eficiência, o SRP tem por escopo instrumentalizar meios para aquisição parcelada de bens e serviços pela Administração Pública, sendo, portanto, compatível com a modalidade Pregão Eletrônico (Lei nº 10.520/02, art. 11).

12.1.5.1. A adoção do sistema de registro de preço justifica-se pela forma de aquisição dos bens e serviços, que terá previsão de entregas parceladas, segundo a necessidade do IFB, uma vez que segundo Decreto nº 7.892/2013:

"Art. 3- O Sistema de Registro de Preços poderá ser adotado nas seguintes hipóteses:

I. *- quando, pelas características do bem ou serviço, houver necessidade de contratações frequentes;*

II. *– quando o for conveniente a aquisição de bens com previsão de entregas parceladas ou contratação de serviços remunerados por unidade de medida ou em regime de tarefa;*

[...]

IV - quando, pela natureza do objeto, não for possível definir previamente o quantitativo a ser demandado pela Administração."

12.1.5.2. Portanto, a presente contratação enquadra-se no Art. 3, Incisos II, III e IV do Decreto n° 7.892/2013.

12.1.5.3. Por outro lado, de acordo com o art. 16 do Decreto nº 7.892/2013, a existência de preços registrados não obriga a Administração Pública a contratar,

facultando-se a realização de licitação específica para a aquisição pretendida, assegurada preferência ao fornecedor registrado em igualdade de condições.

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

12.2.1. Nos termos da legislação vigente, quando aplicável, 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, e nos art. 44 e 45 da Lei Complementar n° 123, de 14 de dezembro de 2006. 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. Destacando-se que a aplicação desse critério e direito ocorre de forma automática no sistema compras governamentais.

12.3 Dos Critérios de Qualificação Técnica para a Habilitação

12.3.1 Todas as especificações técnicas contidas no item ESPECIFICAÇÃO TÉCNICA desse Termo de Referência devem ser comprovadas mediante documentação do próprio fabricante e deverá ser inclusa em anexo na proposta de preço indicando a página e parágrafo ou captura de tela de comprovação de cada um dos subitens dos requisitos técnicos para que a empresa licitante seja habilitada.

12.3.2. Requisitos de Capacidade e Experiência:

12.3.2.1. Atestado de Capacidade Técnica (ACT) em nome da licitante emitido(s) por pessoa(s) jurídica(s) de direito público ou privado, onde comprove ter prestado serviços de entrega, instalação, configuração, treinamento e suporte técnico;

12.3.2.2. A empresa licitante deverá apresentar atestado(s) que comprove, no mínimo, atendimento à 50% dos quantitativos previstos para o item pretendido.

12.3.3. A LICITANTE deve anexar à proposta de preço uma declaração que manterá em seu corpo funcional, durante todo o período de suporte contratado, equipe especializada contendo, no mínimo 02 (dois) profissionais treinados e com certificação máxima disponível pelo fabricante da solução ofertada, podendo comprovar através de certificados emitidos pelo fabricante.

12.3.4. Os preços deverão ser expressos em reais e conter todos os tributos e encargos decorrentes da prestação dos serviços relativos a esta contratação. Os preços poderão ser cotados com até 2 (duas) casas decimais.

12.3.5. A licitante classificada e habilitada provisoriamente em primeiro lugar deve preencher o preço do item em que for vencedora, conforme lances no modelo de proposta de preços ANEXO V - MODELO DE PROPOSTA deste Termo de Referência.

12.3.6. A licitante classificada e habilitada provisoriamente em primeiro lugar para fins de comprovação de atendimento das especificações técnicas, deverá entregar em sua proposta a descrição da marca e modelo dos bens ofertados, a documentação necessária bem como planilha ponto-a-ponto indicando nos documentos os requisitos que trata o ANEXO I - ESPECIFICAÇÃO TÉCNICA deste Termo de Referência. O simples "copia e cola" do termo de referência ensejará da desclassificação da licitante.

12.3.7. Durante a apresentação da proposta, a licitante deverá demonstrar que o produto ofertado atende às exigências solicitadas nesta especificação. Para esta comprovação, serão aceitos catálogos, datasheets, manuais, sites ou outra documentação oficial onde se possa identificar de maneira inequívoca a solução proposta.

12.3.8. Em caso de dúvidas na comprovação da especificação, poderão ser solicitados por meio de diligência, esclarecimentos sobre a especificação do produto cotado pela licitante.

12.3.9. A licitante deverá apresentar declaração de que o produto atende a todas especificações exigidas.

12.3.10. Caso o Relatório Final de Avaliação indique a não-conformidade da solução tecnológica ajustada às especificações exigidas, a licitante não será habilitada.

12.3.11. No caso de desclassificação da licitante, será convocada a próxima licitante classificada para envio da proposta de preço e assim, sucessivamente, até que uma licitante cumpra os requisitos e funcionalidades especificadas e seja declarada vencedora.

12.3.12. O adjudicatário prestará garantia de execução do contrato, nos moldes do art. 56 da Lei nº 8.666, de 1993, com validade durante a execução do contrato e por 90 (noventa) dias após o término da vigência contratual, em valor correspondente a 3% (três por cento) do valor total do contrato.

12.3.13. No prazo máximo de 10 (dez) dias úteis, prorrogáveis por igual período, a critério da CONTRATANTE, contados da assinatura do contrato, a contratada deverá apresentar comprovante de prestação de garantia, podendo optar por caução em dinheiro ou títulos da dívida pública, seguro- garantia ou fiança bancária.

12.3.14. A inobservância do prazo fixado para apresentação da garantia acarretará a aplicação de multa de 0,07% (sete centésimos por cento) do valor total do contrato por dia de atraso, até o máximo de 2% (dois por cento).

12.3.15. O atraso superior a 25 (vinte e cinco) dias autoriza a Administração a promover a rescisão do contrato por descumprimento ou cumprimento irregular de suas cláusulas, conforme dispõem os incisos I e II do art. 78 da Lei n. 8.666 de 1993.

12.3.16. A validade da garantia, qualquer que seja a modalidade escolhida, deverá abranger um período de 90 dias após o término da vigência contratual, conforme item 3.1 do Anexo VII-F da IN SEGES/MP nº 5/2017.

12.3.17. A garantia assegurará, qualquer que seja a modalidade escolhida, o pagamento de:

12.3.17.1. prejuízos advindos do não cumprimento do objeto do contrato e do não adimplemento das demais obrigações nele previstas;

12.3.17.2. prejuízos diretos causados à Administração decorrentes de culpa ou dolo durante a execução do contrato;

12.3.17.3. multas moratórias e punitivas aplicadas pela Administração à CONTRATADA; e obrigações trabalhistas e previdenciárias de qualquer natureza e para com o FGTS, não adimplidas pela contratada, quando couber.

12.3.18. A modalidade seguro-garantia somente será aceita se contemplar todos os eventos indicados no item anterior, observada a legislação que rege a matéria.

12.3.19. A garantia em dinheiro deverá ser efetuada em favor da CONTRATANTE, em conta específica na Caixa Econômica Federal, com correção monetária.

12.3.20. Caso a opção seja por utilizar títulos da dívida pública, estes devem ter sido emitidos sob a forma escritural, mediante registro em sistema centralizado de liquidação e de custódia autorizado pelo Banco Central do Brasil, e avaliados pelos seus valores econômicos, conforme definido pelo Ministério da Fazenda.

12.3.21. No caso de garantia na modalidade de fiança bancária, deverá constar expressa renúncia do fiador aos benefícios do artigo 827 do Código Civil.

12.3.22. No caso de alteração do valor do contrato, ou prorrogação de sua vigência, a garantia deverá ser ajustada à nova situação ou renovada, seguindo os mesmos parâmetros utilizados quando da contratação.

12.3.23. Se o valor da garantia for utilizado total ou parcialmente em pagamento de qualquer obrigação, a CONTRATADA obriga-se a fazer a respectiva reposição no prazo máximo de 15 (quinze) dias úteis, contados da data em que for notificada.

12.3.24. A CONTRATANTE executará a garantia na forma prevista na legislação que rege a matéria. Será considerada extinta a garantia:

12.3.24.1. com a devolução da apólice, carta fiança ou autorização para o levantamento de importâncias depositadas em dinheiro a título de garantia, acompanhada de declaração da CONTRATANTE, mediante termo circunstanciado, de que a Contratada cumpriu todas as cláusulas do contrato;

12.3.24.2. no prazo de 90 (noventa) dias após o término da vigência do contrato, caso a Administração não comunique a ocorrência de sinistros, quando o prazo será ampliado, nos termos da comunicação, conforme estabelecido na alínea "h2"do item 3.1 do Anexo VII-F da IN SEGES/MP n. 05/2017.

12.3.25. O garantidor não é parte para figurar em processo administrativo instaurado pela CONTRATANTE com o objetivo de apurar prejuízos e/ou aplicar sanções à contratada.

12.3.26. A contratada autoriza a CONTRATANTE a reter, a qualquer tempo, a garantia, na forma prevista no neste Edital e no Contrato.

12.3.27. Não será permitida a subcontratação em parte ou total do objeto licitatório.

13. DA EQUIPE DE PLANEJAMENTO DA CONTRATAÇÃO E DA APROVAÇÃO

13.1 A Equipe de Planejamento da Contratação foi instituída conforme Documento de Oficialização de Demanda da contratação, de 05 de outubro de 2021.

13.2 Conforme o §6º do art. 12 da IN SGD/ME nº 1, de 2019, o Termo de Referência será assinado pela Equipe de Planejamento da Contratação e pela autoridade máxima da Área de TIC, e aprovado pela autoridade competente.

INTEGRANTE REQUISITANTE	INTEGRANTE TÉCNICO	INTEGRANTE ADMINISTRATIVO
Assinado eletronicamente Daniel Pereira de Sousa **Matrícula/SIAPE: 2226521** Brasília-DF, 07 de abril de 2022	***Assinado eletronicamente*** Hugo Silva Faria **Matrícula/SIAPE: 2249275** Brasília-DF, 07 de abril de 2022	***Assinado eletronicamente*** Israel Lara Amaral **Matrícula/SIAPE:** 2404437 Brasília-DF, 07 de abril de 2022

Autoridade Máxima da Área de TIC
Assinado eletronicamente Bruno Nepomuceno de Oliveira **Matrícula/SIAPE: 1590823** Brasília-DF, 07 de abril de 2022

Aprovo,

Autoridade Competente
Assinado eletronicamente Julliana Almeida Cavalcanti ***Pró-Reitora Substituta De Administração*** **Matrícula/SIAPE: 1581125** Brasília-DF, 07 de abril de 2022

ANEXO I DO TERMO DE REFERÊNCIA

ESPECIFICAÇÕES TÉCNICAS DA SOLUÇÃO

1. **Servidor de Administração e Console Administrativa**
    1. **Compatibilidade:**
        1. Microsoft Windows Server 2012 Standard / Core / Foundation / Essentials / Datacenter x64;
        2. Microsoft Storage Server 2012 e 2012 R2 x64;
        3. Microsoft Windows Server 2012 R2 Standard / Core / Foundation / Essentials / Datacenter x64;
        4. Microsoft Windows Server 2016 Standard / Core / Datacenter x64;
        5. Microsoft Windows Server 2019 Standard / Core / Datacenter x64;
        6. Microsoft Windows 7 SP1 Professional / Enterprise / Ultimate x32/x64;
        7. Microsoft Windows 8 SP1 Professional / Enterprise x32/x64;
        8. Microsoft Windows 8 Professional / Enterprise x64;
        9. Microsoft Windows 8.1 Professional / Enterprise x32;
        10. Microsoft Windows 8.1 Professional / Enterprise x64;
        11. Microsoft Windows 10 x32;
        12. Microsoft Windows 10 x64

    2. **Suporta as seguintes plataformas virtuais:**

1.2.1. Vmware: Workstation 15.x Pro, vSphere 6.5, vSphere 6.7;
1.2.2. Microsoft Hyper-V 2019;
1.2.5. Parallels Desktop 14;
1.2.7. Citrix XenServer 7.1;

    3. **Características:**

        1. A console deve ser acessada via WEB (HTTPS) ou MMC;
        2. Console deve ser baseada no modelo cliente/servidor;
        3. Compatibilidade com Windows Failover Clustering ou outra solução de alta disponibilidade;

4. Deve permitir a atribuição de perfis para os administradores da Solução de Antivírus;
5. Deve permitir incluir usuários do AD para logarem na console de administração
6. Console deve ser totalmente integrada com suas funções e módulos caso haja a necessidade no futuro de adicionar novas tecnologias tais como, criptografia, Patch management e MDM;
7. As licenças deverão ser perpétuas, ou seja, expirado a validade da mesma o produto deverá permanecer funcional para a proteção contra códigos maliciosos utilizando as definições até o momento da expiração da licença;
8. Capacidade de remover remotamente e automaticamente qualquer solução de antivírus (própria ou de terceiros) que estiver presente nas estações e servidores;
9. Capacidade de instalar remotamente a solução de antivírus nas estações e servidores Windows, através de compartilhamento administrativo, login script e/ou GPO de Active Directory;
10. Deve registrar em arquivo de log todas as atividades efetuadas pelos administradores, permitindo execução de análises em nível de auditoria;
11. Deve armazenar histórico das alterações feitas em políticas;
12. Deve permitir voltar para uma configuração antiga da política de acordo com o histórico de alterações efetuadas pelo administrador apenas selecionando a data em que a política foi alterada;
13. Deve ter a capacidade de comparar a política atual com a anterior, informando quais configurações foram alteradas;
14. A solução de gerencia deve permitir, através da console de gerenciamento, visualizar o número total de licenças gerenciadas;
15. Através da solução de gerência, deve ser possível verificar qual licença está aplicada para determinado computador;
16. Capacidade de instalar remotamente a solução de segurança em smartphones e tablets de sistema iOS, Android e Windows;
17. Capacidade de instalar remotamente qualquer “app” em smartphones e tablets de sistema iOS;
18. A solução de gerência centralizada deve permitir gerar relatórios, visualizar eventos, gerenciar políticas e criar painéis de controle;
19. Deverá ter a capacidade de criar regras para limitar o tráfego de comunicação cliente/servidor por subrede com os seguintes parâmetros: KB/s e horário;
20. Capacidade de gerenciar estações de trabalho e servidores de arquivos (tanto Windows como Linux e Mac) protegidos pela solução antivírus;
21. Capacidade de gerenciar smartphones e tablets (Windows Phone, Android e iOS) protegidos pela solução de segurança;
22. Capacidade de instalar atualizações em computadores de teste antes de instalar nos demais computadores da rede;
23. Capacidade de gerar pacotes customizados (auto executáveis) contendo a licença e configurações do produto;
24. Capacidade de atualizar os pacotes de instalação com as últimas vacinas;
25. Capacidade de fazer distribuição remota de qualquer software, ou seja, deve ser capaz de remotamente enviar qualquer software pela estrutura de gerenciamento de antivírus para que seja instalado nas máquinas clientes;
26. A comunicação entre o cliente e o servidor de administração deve ser criptografada;
27. Capacidade de desinstalar remotamente qualquer software instalado nas máquinas clientes;
28. Deve permitir a realocação de máquinas novas na rede para um determinado grupo sem ter um agente ou endpoint instalado utilizando os seguintes parâmetros:

- Nome do computador;
- Nome do domínio;
- Range de IP;
- Sistema Operacional;
- Máquina virtual.

29. Capacidade de importar a estrutura do Active Directory para descobrimento de máquinas;
30. Deve permitir, por meio da console de gerenciamento, extrair um artefato em quarentena de um cliente sem a necessidade de um servidor ou console de quarentena adicional;
31. Capacidade de monitorar diferentes subnets de rede a fim de encontrar máquinas novas para serem adicionadas à proteção;

32. Capacidade de monitorar grupos de trabalhos já existentes e quaisquer grupos de trabalho que forem criados na rede, a fim de encontrar máquinas novas para serem adicionadas a proteção;
33. Capacidade de, assim que detectar máquinas novas no Active Directory, subnets ou grupos de trabalho, automaticamente importar a máquina para a estrutura de proteção da console e verificar se possui o antivírus instalado. Caso não possuir, deve instalar o antivírus automaticamente;
34. Capacidade de agrupamento de máquina por características comuns entre as mesmas, por exemplo: agrupar todas as máquinas que não tenham o antivírus instalado, agrupar todas as máquinas que não receberam atualização nos últimos 2 dias, etc;
35. Capacidade de definir políticas de configurações diferentes por grupos de estações, permitindo que sejam criados subgrupos e com função de herança de políticas entre grupos e subgrupos;
36. Deve fornecer as seguintes informações dos computadores:
    1. Se o antivírus está instalado;
    2. Se o antivírus está iniciado;
    3. Se o antivírus está atualizado;
    4. Minutos/horas desde a última conexão da máquina com o servidor administrativo;
    5. Minutos/horas desde a última atualização de vacinas;
    6. Data e horário da última verificação executada na máquina;
    7. Versão do antivírus instalado na máquina;
    8. Se é necessário reiniciar o computador para aplicar mudanças;
    9. Data e horário de quando a máquina foi ligada;
    10. Quantidade de vírus encontrados (contador) na máquina;
    11. Nome do computador;
    12. Domínio ou grupo de trabalho do computador;
    13. Data e horário da última atualização de vacinas;
    14. Sistema operacional com Service Pack;
    15. Quantidade de processadores;
    16. Quantidade de memória RAM;
    17. Usuário(s) logado(s) naquele momento, com informações de contato (caso disponíveis no Active Directory);
    18. Endereço IP;
    19. Aplicativos instalados, inclusive aplicativos de terceiros, com histórico de instalação, contendo data e hora que o software foi instalado ou removido;
    20. Atualizações do Windows Updates instaladas;
    21. Informação completa de hardware contendo: processadores, memória, adaptadores de vídeo, discos de armazenamento, adaptadores de áudio, adaptadores de rede, monitores, drives de CD/DVD;
    22. Vulnerabilidades de aplicativos instalados na máquina;
37. Deve permitir bloquear as configurações do antivírus instalado nas estações e servidores de maneira que o usuário não consiga alterá-las;
38. Capacidade de reconectar máquinas clientes ao servidor administrativo mais próximo, baseado em regras de conexão como:
    1. Alteração de Gateway Padrão;
    2. Alteração de subrede;
    3. Alteração de domínio;
    4. Alteração de servidor DHCP;
    5. Alteração de servidor DNS;
    6. Alteração de servidor WINS;
    7. Alteração de subrede;
    8. Resolução de Nome;
    9. Disponibilidade de endereço de conexão SSL;

39. Capacidade de configurar políticas móveis para que quando um computador cliente estiver fora da estrutura de proteção possa atualizar-se via internet;
40. Capacidade de instalar outros servidores administrativos para balancear a carga e otimizar tráfego de link entre sites diferentes;
41. Capacidade de relacionar servidores em estrutura de hierarquia para obter relatórios sobre toda a estrutura de antivírus;
42. Capacidade de herança de tarefas e políticas na estrutura hierárquica de servidores administrativos;
43. Capacidade de eleger qualquer computador cliente como repositório de vacinas e de pacotes de instalação, sem que seja necessária a instalação de um servidor administrativo completo, onde outras máquinas clientes irão atualizar-se e receber pacotes de instalação, a fim de otimizar tráfego da rede;
44. Capacidade de fazer deste repositório de vacinas um gateway para conexão com o servidor de administração, para que outras máquinas que não consigam conectar-se diretamente ao servidor possam usar este gateway para receber e enviar informações ao servidor administrativo;
45. Capacidade de exportar relatórios para os seguintes tipos de arquivos: PDF, HTML e XML;
46. Capacidade de gerar traps SNMP para monitoramento de eventos;
47. Capacidade de enviar e-mails para contas específicas em caso de algum evento;
48. Listar em um único local, todos os computadores não gerenciados na rede;
49. Deve encontrar computadores na rede através de no mínimo três formas: Domínio, Active Directory e subredes;
50. Deve possuir compatibilidade com Microsoft NAP, quando instalado em um Windows 2008 Server;
51. Deve possuir compatibilidade com Cisco Network Admission Control (NAC);
52. Capacidade de baixar novas versões do antivírus direto pela console de gerenciamento, sem a necessidade de importá-los manualmente
53. Capacidade de ligar máquinas via Wake on Lan para realização de tarefas (varredura, atualização, instalação, etc), inclusive de máquinas que estejam em subnets diferentes do servidor;
54. Capacidade de habilitar automaticamente uma política caso ocorra uma epidemia na rede (baseado em quantidade de vírus encontrados em determinado intervalo de tempo);
55. Deve através de opções de otimizações fazer com que o computador gerenciado conceda recursos à outras aplicações, mantendo o antivírus ativo porém sem comprometer o desempenho do computador;
56. Deve permitir a configuração de senha no endpoint e configurar quando que será necessário a utilizá-la, (ex: Solicitar senha quando alguma tarefa de scan for criada localmente no endpoint);
57. Permitir fazer uma verificação rápida ou detalhada de um dispositivo removível assim que conectado no computador, podendo configurar a capacidade máxima em GB da verificação;
58. Deve ser capaz de configurar quais eventos serão armazenados localmente, nos eventos do windows ou ainda se serão mostrados na tela para o colaborador, sejam estes eventos informativos, de alertas ou de erros;
59. Capacidade de realizar atualização incremental de vacinas nos computadores clientes;
60. Deve armazenar localmente e enviar ao servidor de gerência a ocorrência de vírus com os seguintes dados, no mínimo:

- Nome do vírus;
- Nome do arquivo infectado;
- Data e hora da detecção;
- Nome da máquina ou endereço IP;
- Ação realizada.

61. Capacidade de reportar vulnerabilidades de softwares presentes nos computadores;
62. Capacidade de listar updates nas máquinas com o respectivo link para download
63. Deve criar um backup de todos arquivos deletados em computadores para que possa ser restaurado através de comando na Console de administração;
64. Deve ter uma quarentena na própria console de gerenciamento, permitindo baixar um artefato ou enviar direto para análise do fabricante;
65. Capacidade de realizar inventário de hardware de todas as máquinas clientes;
66. Capacidade de realizar inventário de aplicativos de todas as máquinas clientes;

67. Capacidade de diferenciar máquinas virtuais de máquinas físicas.

2. **Estações Windows**

1. **Compatibilidade:**

1. Microsoft Windows 7 Professional/Enterprise/Home SP1 x86 / x64;
2. Microsoft Windows 8 Professional/Enterprise x86 / x64;
3. Microsoft Windows 8.1 Professional / Enterprise x86 / x64;
4. Microsoft Windows 10 Pro / Enterprise / Home / Education x86 / x64;
5. Microsoft Windows Server 2019 Essentials / Standard / Datacenter;
6. Microsoft Windows Server 2016 Essentials / Standard / Datacenter;
7. Microsoft Windows Server 2012 R2 Foundation / Essentials / Standard / Datacenter;
8. Microsoft Windows Server 2012 Foundation / Essentials / Standard / Datacenter;
9. Microsoft Windows Server 2008 R2 Foundation / Essentials / Standard / Datacenter SP1;
10. Microsoft Windows Small Business Server 2011 Standard / Standard x64;
11. Microsoft Windows MultiPoint Server 2011 x64

2. **Características:**

1. Deve prover as seguintes proteções:
    1. Antivírus de Arquivos residente (anti-spyware, anti-trojan, anti-malware, etc) que verifique qualquer arquivo criado, acessado ou modificado;
    2. Antivírus de Web (módulo para verificação de sites e downloads contra vírus);
    3. Antivírus de E-mail (módulo para verificação de e-mails recebidos e enviados, assim como seus anexos);
    4. O Endpoint deve possuir opção para rastreamento por linha de comando, parametrizável, com opção de limpeza;
    5. Firewall com IDS;
    6. Autoproteção (contra-ataques aos serviços/processos do antivírus);
    7. Controle de dispositivos externos;
    8. Controle de acesso a sites por categoria, ex: Bloquear conteúdo adulto, sites de jogos, etc;
    9. Controle de acesso a sites por horário;
    10. Controle de acesso a sites por usuários;
    11. Controle de acesso a websites por dados, ex: Bloquear websites com conteúdos de vídeo e áudio;
    12. Controle de execução de aplicativos;
    13. Controle de vulnerabilidades do Windows e dos aplicativos instalados;
2. Capacidade de escolher quais módulos serão instalados, tanto na instalação local quanto na instalação remota;

3. As vacinas devem ser atualizadas pelo fabricante e disponibilizada aos usuários de, no máximo, uma em uma hora independentemente do nível das ameaças encontradas no período (alta, média ou baixa);
4. Capacidade de detecção de presença de antivírus de outro fabricante que possa causar incompatibilidade, bloqueando a instalação;
5. Capacidade de adicionar pastas/arquivos para uma zona de exclusão, a fim de excluí-los da verificação. Capacidade, também, de adicionar objetos a lista de exclusão de acordo com o veredicto do antivírus, (ex: “Win32.Trojan.banker”) para que qualquer objeto detectado com o veredicto escolhido seja ignorado;
6. Capacidade de adicionar aplicativos a uma lista de “aplicativos confiáveis”, onde as atividades de rede, atividades de disco e acesso ao registro do Windows não serão monitoradas;
7. Possibilidade de desabilitar automaticamente varreduras agendadas quando o computador estiver funcionando a partir de baterias (notebooks);
8. Capacidade de pausar automaticamente varreduras agendadas caso outros aplicativos necessitem de mais recursos de memória ou processamento;
9. Capacidade de verificar arquivos por conteúdo, ou seja, somente verificará o arquivo se for passível de infecção. O antivírus deve analisar a informação de cabeçalho do arquivo para fazer essa decisão e não tomar a partir da extensão do arquivo;
10. Ter a capacidade de fazer detecções por comportamento, identificando ameaças avançadas sem a necessidade de assinaturas;
11. Capacidade de verificar somente arquivos novos e alterados;
12. Capacidade de verificar objetos usando heurística;
13. Capacidade de agendar uma pausa na verificação;
14. Deve permitir a filtragem de conteúdo de URL avançada efetuando a classificação dos sites em categorias;
15. Capacidade de pausar automaticamente a verificação quando um aplicativo for iniciado;
16. Anteriormente a qualquer tentativa de desinfecção ou exclusão permanente, o antivírus deve realizar um backup do objeto;
17. Capacidade de verificar e-mails recebidos e enviados nos protocolos POP3, POP3S, IMAP, NNTP, SMTP e MAPI;
18. Capacidade de verificar links inseridos em e-mails contra phishings;
19. Capacidade de verificar tráfego nos browsers: Internet Explorer, Firefox, Google Chrome e Opera;
20. Capacidade de verificação de corpo e anexos de e-mails usando heurística;
21.
22. O antivírus de e-mail, ao encontrar um objeto potencialmente perigoso, deve:
    1. Perguntar o que fazer, ou;
    2. Bloquear o e-mail;
        1. Apagar o objeto ou tentar desinfectá-lo (de acordo com a configuração pré-estabelecida pelo administrador);
        2. Caso positivo de desinfecção:
            1. Restaurar o e-mail para o usuário;
        3. Caso negativo de desinfecção:
            1. Mover para quarentena ou apagar o objeto (de acordo com a configuração pré-estabelecida pelo administrador);
23. Caso o e-mail conter código que parece ser, mas não é definitivamente malicioso, o mesmo deve ser mantido em quarentena;
24. Possibilidade de verificar somente e-mails recebidos ou recebidos e enviados;
25. Capacidade de filtrar anexos de e-mail, apagando-os ou renomeando-os de acordo com a configuração feita pelo administrador;
26. Capacidade de verificação de tráfego HTTP e qualquer script do Windows Script Host (JavaScript, Visual Basic Script, etc), usando heurísticas;
27. Deve ter suporte total ao protocolo Ipv6;
28. Capacidade de alterar as portas monitoradas pelos módulos de Web e E-mail;
29. O antivírus de web deve realizar a verificação de, no mínimo, duas maneiras diferentes, sob escolha do administrador:
    1. Verificação *on-the-fly*, onde os dados são verificados enquanto são recebidos em tempo-real, ou;
    2. Verificação de *buffer*, onde os dados são recebidos e armazenados para posterior verificação;
30. Possibilidade de adicionar sites da web em uma lista de exclusão, onde não serão verificados pelo antivírus de web;
31. Deve possuir módulo que analise as ações de cada aplicação em execução no computador, gravando as ações executadas e comparando-as com

sequências características de atividades perigosas. Tais registros de sequências devem ser atualizados juntamente com as vacinas;

32. Deve possuir módulo que analise cada macro de VBA executada, procurando por sinais de atividade maliciosa;
33. Deve possuir módulo que analise qualquer tentativa de edição, exclusão ou gravação do registro, de forma que seja possível escolher chaves específicas para serem monitoradas e/ou bloqueadas;
34. Deve possuir módulo de bloqueio de *Phishing*, com atualizações incluídas nas vacinas, obtidas pelo *Anti-Phishing Working Group* (http://www.antiphishing.org/);
35. Capacidade de distinguir diferentes subnets e conceder opção de ativar ou não o firewall para uma subnet específica;
36. Deve possuir módulo IDS (*Intrusion Detection System*) para proteção contra *port scans* e exploração de vulnerabilidades de softwares. A base de dados de análise deve ser atualizada juntamente com as vacinas;
37. O módulo de Firewall deve conter, no mínimo, dois conjuntos de regras:
    1. Filtragem de pacotes: onde o administrador poderá escolher portas, protocolos ou direções de conexão a serem bloqueadas/permitidas;
    2. Filtragem por aplicativo: onde o administrador poderá escolher qual aplicativo, grupo de aplicativo, fabricante de aplicativo, versão de aplicativo ou nome de aplicativo terá acesso a rede, com a possibilidade de escolher quais portas e protocolos poderão ser utilizados.
38. Deve possuir módulo que habilite ou não o funcionamento dos seguintes dispositivos externos, no mínimo:
    1. Discos de armazenamento locais;
    2. Armazenamento removível;
    3. Impressoras;
    4. CD/DVD;
    5. Drives de disquete;
    6. Modems;
    7. Dispositivos de fita;
    8. Dispositivos multifuncionais;
    9. Leitores de smart card;
    10. Dispositivos de sincronização via ActiveSync (Windows CE, Windows Mobile, etc);
    11. Wi-Fi;
    12. Adaptadores de rede externos;
    13. Dispositivos MP3 ou smartphones;
    14. Dispositivos Bluetooth;
    15. Câmeras e Scanners.
39. Capacidade de liberar acesso a um dispositivo e usuários por um período de tempo específico, sem a necessidade de desabilitar a proteção e o gerenciamento central ou de intervenção local do administrador na máquina do usuário;
40. Capacidade de limitar a escrita e leitura em dispositivos de armazenamento externo por usuário;
41. Capacidade de limitar a escrita e leitura em dispositivos de armazenamento externo por agendamento;
42. Capacidade de habilitar “logging” em dispositivos removíveis tais como Pendrive, Discos externos, etc.
43. Capacidade de configurar novos dispositivos por Class ID/Hardware ID;
44. Capacidade de limitar a execução de aplicativos por hash MD5, nome do arquivo, versão do arquivo, nome do aplicativo, versão do aplicativo, fabricante/desenvolvedor, categoria (ex: navegadores, gerenciador de download, jogos, aplicação de acesso remoto, etc);
45. O controle de aplicações deve ter a capacidade de criar regras seguindo os seguintes modos de operação:
    1. Black list: Permite a execução de qualquer aplicação, exceto pelas especificadas por regras.
    2. White list: Impede a execução de qualquer aplicação, exceto pelas especificadas por regras.
46. Capacidade de bloquear execução de aplicativo que está em armazenamento externo;
47. Capacidade de limitar o acesso dos aplicativos a recursos do sistema, como chaves do registro e pastas/arquivos do sistema, por categoria, fabricante ou nível de confiança do aplicativo;
48. Capacidade de, em caso de epidemia, ativar política alternativa onde qualquer configuração possa ser alterada, desde regras de firewall até controle

de aplicativos, dispositivos e acesso à web;

49. Capacidade de, caso o computador cliente saia da rede corporativa, ativar política alternativa onde qualquer configuração possa ser alterada, desde regras de firewall até controle de aplicativos, dispositivos e acesso à web.
50. Capacidade de voltar ao estado anterior do sistema operacional após um ataque de malware.
51. Bloquear atividade de malware explorando vulnerabilidades em softwares de terceiros.
52. Capacidade de detectar anomalias no comportamento de um software, usando análise heurística e aprendizado de máquina (machine learning).
53. Capacidade de integração com o Windows Defender Security Center.
54. Capacidade de integração com a Antimalware Scan Interface (AMSI).
55. Capacidade de detecção de arquivos maliciosos executados em Subsistema Windows para Linux (WSL).

3. **Estações Mac OS X**

1. **Compatibilidade:**
    1. macOS Catalina 10.15
    2. macOS Mojave 10.14
    3. masOS High Sierra 10.13
    4. macOS Sierra 10.12

2. **Características:**

1. Deve prover proteção residente para arquivos (anti-spyware, anti-trojan, anti-malware, etc) que verifique qualquer arquivo criado, acessado ou modificado;
2. Possuir módulo de web-antivírus para proteger contra ameaças durante navegação na internet com possíbilidade de analisar endereços https;
3. Possuir módulo de bloqueio á ataques na rede;
4. Possibilidade de bloquear a comunicação entre a máquina atacante e os demais computadores por tempo definido pelo administrador;
5. Capacidade de criar exclusões para computadores que não devem ser monitorados pelo módulo de bloqueio à ataques na rede;
6. Possibilidade de importar uma chave no pacote de instalação;
7. Capacidade de escolher de quais módulos serão instalados, tanto na instalação local quanto na instalação remota;
8. A instalação e primeira execução do produto deve ser feita sem necessidade de reinicialização do computador, de modo que o produto funcione com toda sua capacidade;
9. Deve possuir suportes a notificações utilizando o Growl;
10. As vacinas devem ser atualizadas pelo fabricante e disponibilizada aos usuários de, no máximo, uma em uma hora independentemente do nível das ameaças encontradas no período (alta, média ou baixa);
11. Capacidade de voltar para a base de dados de vacina anterior;
12. Capacidade de varrer a quarentena automaticamente após cada atualização de vacinas;
13. Capacidade de adicionar pastas/arquivos para uma zona de exclusão, a fim de excluí-los da verificação. Capacidade, também, de adicionar objetos a lista de exclusão de acordo com o veredicto do antivírus, (ex: “Win32.Trojan.banker”) para que qualquer objeto detectado com o veredicto escolhido seja ignorado;

14. Possibilidade de desabilitar automaticamente varreduras agendadas quando o computador estiver funcionando a partir de baterias (notebooks);
15. Capacidade de verificar arquivos por conteúdo, ou seja, somente verificará o arquivo se for passível de infecção. O antivírus deve analisar a informação de cabeçalho do arquivo para fazer essa decisão e não tomar a partir da extensão do arquivo;
16. Capacidade de verificar somente arquivos novos e alterados;
17. Capacidade de verificar objetos usando heurística;
18. Capacidade de agendar uma pausa na verificação;
19. O antivírus de arquivos, ao encontrar um objeto potencialmente perigoso, deve:
    1. O que aplicar, o que fazer, ou;
    2. Bloquear acesso ao objeto;
        1. Apagar o objeto ou tentar desinfectá-lo (de acordo com a configuração pré-estabelecida pelo administrador);
        2. Caso positivo de desinfecção:
            1. Restaurar o objeto para uso;
        3. Caso negativo de desinfecção:
            1. Mover para quarentena ou apagar (de acordo com a configuração pré-estabelecida pelo administrador);
20. Anteriormente a qualquer tentativa de desinfecção ou exclusão permanente, o antivírus deve realizar um backup do objeto;
21. Capacidade de verificar arquivos de formato de email;
22. Possibilidade de trabalhar com o produto pela linha de comando, com no mínimo opções para atualizar as vacinas, iniciar uma varredura, para o antivírus e iniciar o antivírus pela linha de comando;
23. Capacidade de ser instalado, removido e administrado pela mesma console central de gerenciamento.

4. **Estações de trabalho Linux**
    1. **Compatibilidade:**
        1. **Plataforma 32-bits:**
            1. Ubuntu 16.04 LTS;
            2. Red Hat® Enterprise Linux® 6.7 Server;
            3. CentOS 6.7;
            4. Debian GNU / Linux 9.4 ;
            5. Debian GNU / Linux 10;
            6. Linux Mint 18.2;
            7. Linux Mint 19;
            8. GosLinux 6.6;
            9. Mageia 4;
            10. OS Lotos

        2. **Plataforma 64-bits:**
            1. Ubuntu 16.04 LTS;
            2. Ubuntu 18.04 LTS;
            3. Red Hat Enterprise Linux 6.7;
            4. Red Hat Enterprise Linux 7.2;
            5. Red Hat Enterprise Linux 8.0;
            6. CentOS 6.7;

7. CentOS 7.2;
8. CentOS 8.0;
9. Debian GNU / Linux 9.4
10. Debian GNU / Linux 10.1;
11. OracleLinux 7.3;
12. OracleLinux 8;
13. SUSE® Linux Enterprise Server 15;
14. openSUSE® Leap 15;
15. Amazon Linux AMI
16. Linux Mint 18.2;
17. Linux Mint 19;
18. GosLinux 6.6
19. GosLinux 7.2

2. **Características:**

1. Deve prover as seguintes proteções:
2. Antivírus de arquivos residente (anti-spyware, anti-trojan, anti-malware, etc) que verifique qualquer arquivo criado, acessado ou modificado;
3. As vacinas devem ser atualizadas pelo fabricante de, no máximo, uma em uma hora;
4. Capacidade de configurar a permissão de acesso às funções do antivírus com, no mínimo, opções para as seguintes funções:
5. Capacidade de criar exclusões por local, máscara e nome da ameaça;
6. Gerenciamento de status de tarefa (iniciar, pausar, parar ou resumir tarefas);
7. Gerenciamento de Backup: Criação de cópias dos objetos infectados em um reservatório de backup antes da tentativa de desinfectar ou remover tal objeto, sendo assim possível a restauração de objetos que contenham informações importantes;
8. Dectectar aplicações que possam ser utilizadas como vetor de ataque por hackers;
9. Fazer detecções através de heurística utilizando no mínimo as seguintes opções de nível:
    1. Alta;
    2. Média;
    3. Baixa;
    4. Recomendado.
10. Gerenciamento de Quarentena: Quarentena de objetos suspeitos e corrompidos, salvando tais arquivos em uma pasta de quarentena;
11. Verificação por agendamento: procura de arquivos infectados e suspeitos (incluindo arquivos em escopos especificados); análise de arquivos; desinfecção ou remoção de objetos infectados.
12. Em caso erros, deve ter capacidade de criar *logs* automaticamente, sem necessidade de outros softwares;
13. Capacidade de pausar automaticamente varreduras agendadas caso outros aplicativos necessitem de mais recursos de memória ou processamento;
14. Capacidade de verificar arquivos por conteúdo, ou seja, somente verificará o arquivo se for passível de infecção. O antivírus deve analisar a informação de cabeçalho do arquivo para fazer essa decisão e não tomar a partir da extensão do arquivo;
15. Capacidade de verificar objetos usando heurística;
16. Possibilidade de escolha da pasta onde serão guardados os backups e arquivos em quarentena;
17. Possibilidade de
18. Deve possuir módulo escolha da pasta onde arquivos restaurados de backup e arquivos serão gravados;de administração remoto através de

ferramenta nativa ou Webmin (ferramenta nativa GNU-Linux).

5. **Servidores Windows**
    1. **Compatibilidade:**
    2. **Plataforma 32-bits:**
        1. Windows Server 2003 Standard/Enterprise/Datacenter SP2 e posterior;
        2. Windows Server 2003 R2 Standard/Enterprise/Datacenter SP2 e posterior;
        3. Windows Server 2008 Standard/Enterprise/Datacenter SP1 e posterior;
        4. Windows Server 2008 Core Standard/Enterprise/Datacenter SP1 e posterior.
    3. **Plataforma 64-bits**
        1. Windows Server 2003 Standard/Enterprise/Datacenter SP2 e posterior;
        2. Windows Server 2003 R2 Standard/Enterprise/Datacenter SP2 e posterior;
        3. Microsoft Windows Server 2008 Standard / Enterprise / DataCenter SP1 ou posterior;
        4. Microsoft Windows Server 2008 Core Standard / Enterprise / DataCenter SP1 ou posterior.
        5. Microsoft Windows Server 2008 R2 Foundation / Standard / Enterprise / DataCenter SP1 ou posterior;
        6. Microsoft Windows Server 2008 R2 Core Standard / Enterprise / DataCenter SP1 ou posterior;
        7. Microsoft Small Business Server 2008 Standard / Premium
        8. Microsoft Windows Hyper-V Server 2008 R2 SP1 e posterior;
        9. Microsoft Microsoft Small Business Server 2011 Essentials / Standard
        10. Microsoft Windows MultiPoint Server 2011
        11. Microsoft Windows Server 2012 Essentials / Standard / Foundation / Datacenter / MultiPoint;
        12. Microsoft Windows Server 2012 R2 Essentials / Standard / Foundation / Datacenter;
        13. Microsoft Windows Server 2012 Core Standard / Datacenter;
        14. Microsoft Windows Server 2012 R2 Core Standard / Datacenter;
        15. Microsoft Windows Storage Server 2012;
        16. Microsoft Windows Storage Server 2012 R2;
        17. Microsoft Windows Hyper-V Server 2012;
        18. Microsoft Windows Hyper-V Server 2012 R2;
        19. Windows Server 2016 Essentials /Standard / Datacenter / MultiPoint Premium Server;
        20. Windows Server 2016 Core Standard / Datacenter;
        21. Windows Storage Server 2016;
        22. Windows Hyper-V Server 2016;
        23. Microsoft Windows Server 2019 Core / Terminal / Hyper-V
        24. Windows Server IoT 2019 for Storage

4. **Características:**

1. Deve prover as seguintes proteções:
    1. Antivírus de Arquivos residente (anti-spyware, anti-trojan, anti-malware, etc) que verifique qualquer arquivo criado, acessado ou

modificado;
    2. Auto-proteção contra-ataques aos serviços/processos do antivírus;
    3. Firewall com IDS;
    4. Controle de vulnerabilidades do Windows e dos aplicativos instalados;
2. Capacidade de escolher de quais módulos serão instalados, tanto na instalação local quanto na instalação remota;
3. As vacinas devem ser atualizadas pelo fabricante de, no máximo, uma em uma hora;
4. Capacidade de configurar a permissão de acesso às funções do antivírus com, no mínimo, opções para as seguintes funções:
    1. Gerenciamento de status de tarefa (iniciar, pausar, parar ou resumir tarefas);
    2. Gerenciamento de tarefa (criar ou excluir tarefas de verificação);
    3. Leitura de configurações;
    4. Modificação de configurações;
    5. Gerenciamento de Backup e Quarentena;
    6. Visualização de relatórios;
    7. Gerenciamento de relatórios;
    8. Gerenciamento de chaves de licença;
    9. Gerenciamento de permissões (adicionar/excluir permissões acima);
5. O módulo de Firewall deve conter, no mínimo, dois conjuntos de regras:
    1. Filtragem de pacotes: onde o administrador poderá escolher portas, protocolos ou direções de conexão a serem bloqueadas/permitidas;
    2. Filtragem por aplicativo: onde o administrador poderá escolher qual aplicativo, grupo de aplicativo, fabricante de aplicativo, versão de aplicativo ou nome de aplicativo terá acesso a rede, com a possibilidade de escolher quais portas e protocolos poderão ser utilizados.
6. Capacidade de separadamente selecionar o número de processos que irão executar funções de varredura em tempo real, o número de processos que executarão a varredura sob demanda e o número máximo de processos que podem ser executados no total;
7. Bloquear malwares tais como Cryptlockers mesmo quando o ataque vier de um computador sem antivírus na rede
8. Capacidade de resumir automaticamente tarefas de verificação que tenham sido paradas por anormalidades (queda de energia, erros, etc);
9. Em caso de erros, deve ter capacidade de criar *logs* e *traces* automaticamente, sem necessidade de outros softwares;
10. Capacidade de configurar níveis de verificação diferentes para cada pasta, grupo de pastas ou arquivos do servidor;
11. Capacidade de bloquear acesso ao servidor de máquinas infectadas e quando uma máquina tenta gravar um arquivo infectado no servidor;
12. Capacidade de criar uma lista de máquina que nunca serão bloqueadas mesmo quando infectadas;
13. Capacidade de detecção de presença de antivírus de outro fabricante que possa causar incompatibilidade, bloqueando a instalação;
14. Capacidade de adicionar pastas/arquivos para uma zona de exclusão, a fim de excluí-los da verificação. Capacidade, também, de adicionar objetos a lista de exclusão de acordo com o veredicto do antivírus, (ex: “Win32.Trojan.banker”) para que qualquer objeto detectado com o veredicto escolhido seja ignorado;
15. Capacidade de pausar automaticamente varreduras agendadas caso outros aplicativos necessitem de mais recursos de memória ou processamento;
16. Capacidade de verificar arquivos por conteúdo, ou seja, somente verificará o arquivo se for passível de infecção. O antivírus deve analisar a informação de cabeçalho do arquivo para fazer essa decisão e não tomar a partir da extensão do arquivo;
17. Capacidade de verificar somente arquivos novos e alterados;
18. Capacidade de escolher qual tipo de objeto composto será verificado (ex: arquivos comprimidos, arquivos auto descompressores, .PST, arquivos compactados por compactadores binários, etc.);
19. Capacidade de verificar objetos usando heurística;
20. Capacidade de configurar diferentes ações para diferentes tipos de ameaças;
21. Capacidade de agendar uma pausa na verificação;
22. Capacidade de pausar automaticamente a verificação quando um aplicativo for iniciado;
23. Anteriormente a qualquer tentativa de desinfecção ou exclusão permanente, o antivírus deve realizar um backup do objeto;
24. Possibilidade de escolha da pasta onde serão guardados os backups e arquivos em quarentena;

25. Possibilidade de escolha da pasta onde arquivos restaurados de backup e arquivos serão gravados;
26. Deve possuir módulo que analise cada script executado, procurando por sinais de atividade maliciosa.
27. Bloquear atividade de malware explorando vulnerabilidades em softwares de terceiros
28. Capacidade de detectar anomalias no comportamento de um software, usando análise heurística e aprendizado de máquina (machine learning).
29. Capacidade de bloquear a criptografia de arquivos em pastas compartilhadas, após a execução de um malware em um dispositivo que possua o mapeamento da pasta.

6. **Servidores Linux**
    1. **Compatibilidade:**

Plataforma 32-bits:

1. Ubuntu 16.04 LTS;
2. Red Hat® Enterprise Linux® 6.7 Server;
3. CentOS 6.7;
4. Debian GNU / Linux 9.4 ;
5. Debian GNU / Linux 10;
6. Linux Mint 18.2;
7. Linux Mint 19;
8. GosLinux 6.6;
9. Mageia 4;
10. OS Lotos

Plataforma 64-bits:

1. Ubuntu 16.04 LTS;
2. Ubuntu 18.04 LTS;
3. Red Hat Enterprise Linux 6.7;
4. Red Hat Enterprise Linux 7.2;
5. Red Hat Enterprise Linux 8.0;
6. CentOS 6.7;
7. CentOS 7.2;
8. CentOS 8.0;
9. Debian GNU / Linux 9.4
10. Debian GNU / Linux 10.1;
11. OracleLinux 7.3;
12. OracleLinux 8;
13. SUSE® Linux Enterprise Server 15;
14. openSUSE® Leap 15;
15. Amazon Linux AMI
16. Linux Mint 18.2;

17. Linux Mint 19;
18. GosLinux 6.6
19. GosLinux 7.2

2. **Características:**

1. Deve prover as seguintes proteções:
    1. Antivírus de Arquivos residente (anti-spyware, anti-trojan, anti-malware, etc) que verifique qualquer arquivo criado, acessado ou modificado;
    2. As vacinas devem ser atualizadas pelo fabricante de, no máximo, uma em uma hora;
2. Capacidade de configurar a permissão de acesso às funções do antivírus com, no mínimo, opções para as seguintes funções:
    1. Gerenciamento de status de tarefa (iniciar, pausar, parar ou resumir tarefas);
    2. Gerenciamento de Backup: Criação de cópias dos objetos infectados em um reservatório de backup antes da tentativa de desinfectar ou remover tal objeto, sendo assim possível a restauração de objetos que contenham informações importantes;
    3. Gerenciamento de Quarentena: Quarentena de objetos suspeitos e corrompidos, salvando tais arquivos em uma pasta de quarentena;
    4. Verificação por agendamento: procura de arquivos infectados e suspeitos (incluindo arquivos em escopos especificados); análise de arquivos; desinfecção ou remoção de objetos infectados;
3. Em caso erros, deve ter capacidade de criar *logs* automaticamente, sem necessidade de outros softwares;
4. Capacidade de pausar automaticamente varreduras agendadas caso outros aplicativos necessitem de mais recursos de memória ou processamento;
5. Capacidade de verificar arquivos por conteúdo, ou seja, somente verificará o arquivo se for passível de infecção. O antivírus deve analisar a informação de cabeçalho do arquivo para fazer essa decisão e não tomar a partir da extensão do arquivo;
6. Capacidade de verificar objetos usando heurística;
7. Possibilidade de escolha da pasta onde serão guardados os backups e arquivos em quarentena;
8. Possibilidade de escolha da pasta onde arquivos restaurados de backup e arquivos serão gravados;
9. Deve possuir módulo de administração remoto através de ferramenta nativa ou Webmin (ferramenta nativa GNU-Linux).

7. **Smartphones e tablets**

1. **Compatibilidade:**

1. Dispositivos com os sistemas operacionais:
    1. Android 5.0 – 5.1.1
    2. Android 6.0 – 6.0.1
    3. Android 7.0 – 7.12
    4. Android 8.0 – 8.1

5. Android 9.0
6. Android 10.0
7. iOS 10.0 – 10.3.3
8. iOS 11.0 – 11.3
9. iOS 12.0
10. iOS 13.0

2. **Características:**
    1. Deve prover as seguintes proteções:
        1. Proteção em tempo real do sistema de arquivos do dispositivo – interceptação e verificação de:
        2. Proteção contra adware e autodialers;
        3. Todos os objetos transmitidos usando conexões wireless (porta de infravermelho, Bluetooth) e mensagens EMS, durante sincronismo com PC e ao realizar download usando o browser;
        4. Arquivos abertos no smartphone;
        5. Programas instalados usando a interface do smartphone
        6. Verificação dos objetos na memória interna do smartphone e nos cartões de expansão sob demanda do usuário e de acordo com um agendamento;
    2. Deverá isolar em área de quarentena os arquivos infectados;
    3. Deverá atualizar as bases de vacinas de modo agendado;
    4. Deverá bloquear spams de SMS através de Black lists;
    5. Deverá ter função de bloqueio do aparelho caso o SIM CARD for trocado para outro não autorizado com mensagem de aviso ao utilizador do dispositivo;
    6. Capacidade de desativar por política:

- Wi-fi;
- Câmera;
- Bluetooth.

    7. Deverá ter função de limpeza de dados pessoais a distância, em caso de roubo, por exemplo;
    8. Capacidade de requerer uma senha para desbloquear o dispositivo e personalizar a quantidade de caracteres para esta senha;
    9. Deverá ter firewall pessoal (Android);
    10. Capacidade de tirar fotos quando a senha for inserida incorretamente;
    11. Possibilidade de instalação remota utilizando o Microsoft System Center Mobile Device Manager 2008 SP1;
    12. Capacidade de enviar comandos remotamente de:

- Localizar;
- Bloquear.

    13. Capacidade de detectar Jailbreak em dispositivos iOS;
    14. Capacidade de bloquear o acesso a site por categoria em dispositivos;
    15. Capacidade de bloquear o acesso a sites phishing ou malicioso;
    16. Capacidade de criar containers de aplicativos, separando dados corporativos de dados pessoais;
    17. Capacidade de bloquear o dispositivo quando o cartão “SIM” for substituído;
    18. Capacidade de configurar White e blacklist de aplicativos;
    19. Capacidade de localizar o dispositivo quando necessário;
    20. Permitir atualização das definições quando estiver em “roaming”;

21. Capacidade de selecionar endereço do servidor para buscar a definição de vírus;
22. Deve permitir verificar somente arquivos executáveis;
23. Deve ter a capacidade de desinfectar o arquivo se possível;
24. Capacidade de agendar uma verificação;
25. Capacidade de enviar URL de instalação por e-mail;
26. Capacidade de fazer a instalação através de um link QRCode;
27. Capacidade de executar as seguintes ações caso a desinfecção falhe:

- Deletar;
- Ignorar;
- Quarentenar;
- Perguntar ao usuário.

8. **Gerenciamento de dispositivos móveis (MDM)**
    1. **Compatibilidade:**

Dispositivos com os sistemas operacionais:

1. Android 5.0 – 5.1.1
2. Android 6.0 – 6.0.1
3. Android 7.0 – 7.12
4. Android 8.0 – 8.1
5. Android 9.0
6. Android 10.0
7. iOS 10.0 – 10.3.3
8. iOS 11.0 – 11.3
9. iOS 12.0
10. iOS 13.0

2. Softwares de gerência de dispositivos:
    1. VMWare AirWatch 9.3;
    2. MobileIron 10.0;
    3. IBM Maas360 10.68;
    4. Microsoft Intune 1908;
    5. SOTI MobiControl 14.1.4 (1693);

2. **Características:**

1. Capacidade de aplicar políticas de ActiveSync através do servidor Microsoft Exchange;

2. Capacidade de ajustar as configurações de:
    1. Sincronização de e-mail;
    2. Uso de aplicativos;
    3. Senha do usuário;
    4. Criptografia de dados;
    5. Conexão de mídia removível.
3. Capacidade de instalar certificados digitais em dispositivos móveis;
4. Capacidade de, remotamente, resetar a senha de dispositivos iOS;
5. Capacidade de, remotamente, apagar todos os dados de dispositivos iOS;
6. Capacidade de, remotamente, bloquear um dispositivo iOS;
7. Deve permitir configurar horário para sincronização do dispositivo com a console de gerenciamento;
8. Possibilidade de exigir senha para abrir aplicações instaladas em container;
9. Deve permitir que o usuário utilize autenticação do Active Directory para abrir aplicações em container;
10. Deve permitir que uma senha seja digitada a cada x(minutos) para continuar utilizando uma aplicação em container;
11. Deve permitir a criptografia de dados salvos pelas aplicações em container;
12. Permitir sincronização com perfil do “Touch Down”;
13. Capacidade de desinstalar remotamente o antivírus do dispositivo;
14. Deve permitir fazer o upgrade do antivírus de forma remota sem a necessidade de desinstalar a versão atual;
15. Capacidade de sincronizar com Samsung Knox.

9. **Criptografia**
    1. **Compatibilidade**
        1. Microsoft Windows 7 Professional SP1 ou superior x86/x64;
        2. Microsoft Windows 8 Enterprise x86/x64;
        3. Microsoft Windows 8 Pro x86/x64;
        4. Microsoft Windows 8.1 Pro x86/x64;
        5. Microsoft Windows 8.1 Enterprise x86/x64;
        6. Microsoft Windows 10 Pro / Enterprise / Home / Education x86 / x64

    2. **Características**
        1. O acesso ao recurso criptografado (arquivo, pasta ou disco) deve ser garantido mesmo em caso o usuário tenha esquecido a senha, através de procedimentos de recuperação;
        2. Utilizar, no mínimo, algoritmo AES com chave de 256 bits;
        3. Capacidade de criptografar completamente o disco rígido da máquina, adicionando um ambiente de pré-boot para autenticação do usuário;
        4. Capacidade de utilizar *Single Sign-On* para a autenticação de pré-boot;
        5. Permitir criar vários usuários de autenticação pré-boot;
        6. Capacidade de criar um usuário de autenticação pré-boot comum com uma senha igual para todas as máquinas a partir da console de gerenciamento;
        7. Capacidade de criptografar drives removíveis de acordo com regra criada pelo administrador, com as opções:
            1. Criptografar somente os arquivos novos que forem copiados para o disco removível, sem modificar os arquivos já existentes;
            2. Criptografar todos os arquivos individualmente;

3. Criptografar o dispositivo inteiro, de maneira que não seja possível listar os arquivos e pastas armazenadas;
4. Criptografar o dispositivo em modo portátil, permitindo acessar os arquivos em máquinas de terceiros através de uma senha;

8. Capacidade de selecionar pastas e arquivos (por tipo, ou extensão) para serem criptografados automaticamente. Nesta modalidade, os arquivos devem estar acessíveis para todas as máquinas gerenciadas pela mesma console de maneira transparente para os usuários;
9. Capacidade de criar regras de exclusões para que certos arquivos ou pastas nunca sejam criptografados;
10. Capacidade de selecionar aplicações que podem ou não ter acesso aos arquivos criptografados;
11. Verifica compatibilidade de hardware antes de aplicar a criptografia;
12. Possibilita estabelecer parâmetros para a senha de criptografia;
13. Bloqueia o reuso de senhas;
14. Bloqueia a senha após um número de tentativas pré-estabelecidas;
15. Capacidade de permitir o usuário solicitar permissão a determinado arquivo criptografado para o administrador mediante templates customizados;
16. Permite criar exclusões para não criptografar determinados “discos rígidos” através de uma busca por nome do computador ou nome do dispositivo
17. Permite criptografar as seguintes pastas pré-definidas: “meus documentos”, “Favoritos”, “Desktop”, “Arquivos temporários” e “Arquivos do outlook”;
18. Permite utilizar variáveis de ambiente para criptografar pastas customizadas;
19. Capacidade de criptografar arquivos por grupos de extensão, tais como: Documentos do office, Document, arquivos de audio, etc;
20. Permite criar um grupo de extensões de arquivos a serem criptografados;
21. Capacidade de criar regra de criptografia para arquivos gerados por aplicações;
22. Permite criptografia de dispositivos móveis mesmo quando o endpoint não possuir comunicação com a console de gerenciamento.
23. Capacidade de deletar arquivos de forma segura após a criptografia;
24. Capacidade de criptografar somente o espaço em disco utilizado;
25. Deve ter a opção de criptografar arquivos criados a partir de aplicações selecionadas pelo administrador;
26. Capacidade de bloquear aplicações selecionadas pelo administrador de acessarem arquivos criptografados;
27. Deve permitir criptografar somente o espaço utilizado em dispositivos removíveis tais como pendrives, HD externo, etc;
28. Capacidade de criptografar discos utilizando a criptografia BitLocker da Microsoft;
29. Deve ter a opção de utilização de TPM para criptografia através do BitLocker;
30. Capacidade de fazer “Hardware encryption”.

10. **Gerenciamento de Sistemas**
    1. Capacidade de criar imagens de sistema operacional remotamente e distribuir essas imagens para computadores gerenciados pela solução e para computadores *bare-metal*;
    2. Deve possibilitar a utilização de servidores PXE na rede para deploy de imagens;
    3. Capacidade de detectar softwares de terceiros vulneráveis, criando assim um relatório de softwares vulneráveis;
    4. Capacidade de corrigir as vulnerabilidades de softwares, fazendo o download centralizado da correção ou atualização e aplicando essa correção ou atualização nas máquinas gerenciadas de maneira transparente para os usuários;
    5. Capacidade de gerenciar licenças de softwares de terceiros;
    6. Capacidade de registrar mudanças de hardware nas máquinas gerenciadas;
    7. Capacidade de gerenciar um inventário de hardware, com a possibilidade de cadastro de dispositivos (ex: router, switch, projetor, acessório, etc), informando data de compra, local onde se encontra, service tag, número de identificação e outros;
    8. Possibilita fazer distribuição de software de forma manual e agendada;
    9. Suporta modo de instalação silenciosa;

10. Suporte a pacotes MSI, exe, bat, cmd e outros padrões de arquivos executáveis;
11. Possibilita fazer a distribuição através de agentes de atualização;
12. Utiliza tecnologia multicast para evitar tráfego na rede;
13. Possibilita criar um inventário centralizado de imagens;
14. Capacidade de atualizar o sistema operacional direto da imagem mantendo os dados do usuário;
15. Suporte a WakeOnLan para deploy de imagens;
16. Capacidade de atuar como servidor de atualização do Windows podendo fazer deploy de patches;
17. Suporta modo de teste, podendo atribuir alguns computadores para receberem as atualizações de forma automática para avaliação de alterações no comportamento;
18. Capacidade de gerar relatórios de vulnerabilidades e patches;
19. Possibilita criar exclusões para aplicação de patch por tipo de sistema operacional, Estação de trabalho e Servidor ou por grupo de administração;
20. Permite iniciar instalação de patch e correções de vulnerabilidades ao reiniciar ou desligar o computador;
21. Permite baixar atualizações para o computador sem efetuar a instalação
22. Permite o administrador instalar somente atualizações aprovadas, instalar todas as atualizações (exceto as bloqueadas) ou instalar todas as atualizações incluindo as bloqueadas;
23. Capacidade de instalar correções de vulnerabilidades de acordo com a severidade;
24. Permite selecionar produtos a serem atualizados pela console de gerenciamento;
25. Permite selecionar categorias de atualizações para serem baixadas e instaladas, tais como: atualizações de segurança, ferramentas, drivers, etc;
26. Capacidade de adicionar caminhos específicos para procura de vulnerabilidades e updates em arquivos;
27. Capacidade de instalar atualizações ou correções somente em computadores definidos, em grupos definidos ou em uma porcentagem de computadores conforme selecionado pelo administrador;
28. Capacidade de configurar o reinicio do computador após a aplicação das atualizações e correções de vulnerabilidades;
29. Deve permitir selecionar o idioma das aplicações que serão atualizadas;
30. Permitir agendar o sincronismo entre a console de gerenciamento e os sites da Microsoft para baixar atualizações recentes.

ANEXO II DO TERMO DE REFERÊNCIA

ESTUDO TÉCNICO PRELIMINAR

MINISTÉRIO DA EDUCAÇÃO
Instituto Federal de Educação, Ciência e Tecnologia de Brasília
DIRETORIA DE TECNOLOGIA DA INF E COMUNIC

ESTUDO TÉCNICO PRELIMINAR DA CONTRATAÇÃO

INTRODUÇÃO

O Estudo Técnico Preliminar tem por objetivo identificar e analisar os cenários para o atendimento da demanda que consta no Documento de Oficialização da Demanda, bem como demonstrar a viabilidade técnica e econômica das soluções identificadas, fornecendo as informações necessárias para subsidiar o respectivo processo de contratação.

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

1 – DEFINIÇÃO E ESPECIFICAÇÃO DAS NECESSIDADES E REQUISITOS

Informações Básicas

Número do processo: 23098.001656.2021-46

Identificação das necessidades de negócio

Dispor de licenças em formato digital de solução em programa informático de combate a vírus cibernéticos, antivírus, que tenha a competência de detectar, monitorar e combater quaisquer atividades relacionadas à softwares maliciosos que venham ou possam vir a causar danos ao parque computacional do Instituto Federal de Brasília.

Atualmente, há tanto um aumento exponencial de equipamentos e soluções digitais, quanto, equitativamente, o de riscos em sua utilização. Por meio de equipamentos comprometidos ou aplicações vulneráveis, dados sensíveis podem ser expostos, usuários podem ser ludibriados e graves consequências podem emergir.

Dentre as diversas formas de ameaças digitais, existem tipos específicos de aplicações maliciosas, dentre elas podem-se citar *worms*, *trojans*, *spywares*, *ransomwares*, *rootkits*, *keyloggers*, *adwares*, *browser hijackers*, *phishing*, entre outros.

Com a massificação do uso de soluções digitais advindo ao ambiente institucional, necessita-se de solução capaz de monitorar, identificar e proteger equipamentos informáticos, a fim de assegurar integridade dos dados e oferecer o mínimo de segurança cibernética necessária aos usuários do IFB que fazem uso de equipamentos da instituição. Visto que o licenciamento atual finda em 03 de janeiro de 2022, surge a necessidade de se adquirir nova solução para auxiliar no combate a possíveis riscos.

A necessidade em questão está diretamente alinhada com o Plano de Desenvolvimento Institucional 2021-2023, com o Plano Diretor de Tecnologia da Informação e Comunicação vigente para o período 2021 - 2023, com a Estratégia de Governo Digital e com o Plano Anual de Contratações 2021, conforme a apresentando a seguir:

ALINHAMENTO AOS PLANOS ESTRATÉGICOS	
ID	**Objetivos Estratégicos Institucionais**
OE 1.1	Assegurar a oferta de cursos de Educação Profissional e Tecnológica alinhados às necessidades de qualificação do mundo do trabalho
OE 3.3	Fomentar e aprimorar o uso da tecnologia da informação e comunicação
ID	**Objetivos Estratégicos da EGD**
OE 2	Avaliação de satisfação nos serviços digitais
OE 11	Garantia da segurança das plataformas de governo digital e de missão crítica

ALINHAMENTO AO PDTIC 2021 - 2023			
Objetivo Estratégico 3:*Prover a infraestrutura de TIC, a conectividade, a segurança da informação e comunicação*			
ID	**Ação do PDTIC**	**ID**	**Meta do PDTIC associada**
A.3.2.E1.1.1	Apoiar o processo de contratação da solução de Software de Antivírus	M 3.2.E1	Instruir 100% dos processos de aquisição/ contratação de TIC aprovadas no PDTIC 2021-2023

ALINHAMENTO AO PAC 2021	
Item	**Descrição**
100	LICENCIAMENTO DE DIREITOS PERMANENTES DE USO DE SOFTWARE PARA ESTAÇÃO DE TRABALHO

Portanto, resumidamente, as necessidades de negócio que conduzirão as análises de soluções e definição daquela mais adequada aos objetivos organizacionais são:

organizacionais sao:

- Atender as demandas registradas no PAC relacionadas à aquisição/renovação de licença de antivírus;
- Manter integridade dos dados institucionais e prover segurança da informação conforme legislação vigente;
- Prover recursos computacionais necessários ao perfeito desenvolvimento das atividades laborais. Trata-se de recursos de hardware e software que provenham apoio a execução de tarefas de suporte, administração e gestão de atividades meio e fim relacionados ao alcance mediato ou indireto do interesse público;
- Prover a continuidade dos serviços desenvolvidos no âmbito do IFB. Essa funcionalidade está ligada ao princípio da continuidade do serviço público, segundo o qual o Estado, na qualidade de detentor dos bens e interesses públicos não pode parar, caso contrário estaria deixando de defender ou representar a coletividade.

Identificação das necessidades tecnológicas

As necessidades tecnológicas, também chamadas de requisitos da solução de tecnologia, segundo o corpo de conhecimento de análise de negócios (guia BABOK v. 2.0) com adaptações, descrevem as características de uma solução que atende aos requisitos do negócio são desenvolvidas e definidas neste documento após a realização de uma análise de requisitos.

A segurança da informação – requisito essencial para a utilização de todos os serviços disponíveis - deve ser integrada à solução, com estratégia de proteção e conformidade de dispositivos, usuários, dados e aplicações, considerando o contexto de acesso, como uma ferramenta para Segurança dos Endpoint capaz de fornecer serviços de:

- Antivírus de Arquivos residente (anti-spyware, anti-ransomware anti-trojan, anti malware, etc.) que verifique qualquer arquivo criado, acessado ou modificado;
- Antivírus de Web (módulo para verificação de sites e downloads contra vírus);
- Antivírus de E-mail (módulo para verificação de e-mails recebidos e enviados, assim como seus anexos);
- O Endpoint deve possuir opção para rastreamento por linha de comando, parametrizável, com opção de limpeza;
- Firewall com IDS;
- Autoproteção (contra-ataques aos serviços / processos do antivírus);
- Controle de dispositivos externos;
- Controle de acesso a sites por categoria, ex: Bloquear conteúdo adulto, sites de jogos, etc;
- Controle de acesso a sites por horário;
- Controle de acesso a sites por usuários;
- Controle de acesso a websites por dados, ex: Bloquear websites com conteúdo de vídeo e áudio;
- Controle de execução de aplicativos;
- Controle de vulnerabilidades do Windows e dos aplicativos instalados.

Demais requisitos necessários e suficientes à escolha da solução de TIC

- Deve conter funcionalidades essenciais à segurança, como firewall, políticas de acesso à websites, bloqueio de transmissão de informações sensíveis e acesso às informações avançadas sobre as ações executadas, para que assim possam-se realizar auditorias referentes a possíveis danos ao ambiente institucional.
- Deve possuir plataforma para gerência de configurações e ajustes relacionados ao Endpoint.
- A plataforma deverá possuir características essenciais como envio de relatórios, por e-mail, referentes ao uso das funcionalidades da solução, como websites e aplicações bloqueadas e atividades referentes ao firewall, deverá possuir também dashboard personalizável com as informações que exigem maior atenção, como níveis de ameaça e quantidade de riscos.
- Deverá fornecer atualizações de políticas via rede e capacidade de agregar múltiplos dispositivos em diferentes unidades organizacionais, garantindo assim maior eficácia ao adotar as medidas personalizáveis de segurança.
- O endpoint deverá ser capaz de analisar as ações tomadas pelo usuário e identificar possíveis incidentes que afetem a rede de computadores. A solução deverá ser capaz de remover outras soluções que ajam de maneira concomitante com esta.
- O endpoint também deverá possuir controles relacionados a permissibilidade, para que apenas usuários administradores possam realizar configurações e ajustes manuais, como reiniciar módulos.
- Deverá realizar varreduras em unidades externas (exemplo: USB) que venham a se conectar com o dispositivo, e, caso possuam arquivos ou possam vir a causar malefícios, tomar medidas para o bloqueio da atividade suspeita, dentre outras funcionalidades.
- A instalação do software de gerência da solução será realizada na infraestrutura de TI do IFB de forma centralizada.
- A empresa contratada deverá comprovar que é reconhecida pelo fabricante do software como qualificada para a execução do serviço.

2 – ESTIMATIVA DA DEMANDA – QUANTIDADE DE LICENÇAS A SEREM CONTRATADAS[1]

Diante das análises qualitativa e quantitativa realizadas ao longo do presente estudo técnico preliminar, constata-se que, para fins de um processo de aquisição de renovação/upgrade de licenças, se faz necessário o seguinte quantitativo de licenças, distribuídos por campi e reitoria, para que a solução atenda a demanda da instituição:

Solução	**Quantitativo de Licenças por Campi / Reitoria CATMAT - 350949**		
	Unidade		**Quantidade de Licenças**
Kaspersky Endpoint	REIT	Reitoria	150
	CCEI	Campus Ceilândia	270
	CEST	Campus Estrutural	250
	CGAM	Campus Gama	520
	CPLA	Campus Planaltina	200

Security for Business Advanced	CSAM	Campus Samambaia	370
	CSSB	Campus São Sebastião	520
	CTAG	Campus Taguatinga	520
	CBRA	Campus Brasília	727
	CREM	Campus Recanto das Emas	320
	CRFD	Campus Riacho Fundo	195
	Total de Licenças		4.042

TABELA RESUMO

Item	Descrição	Qtde Licenças
01	Software de Antivírus	4.042

3 – ANÁLISE DE SOLUÇÕES

3.1 – IDENTIFICAÇÃO DAS SOLUÇÕES

Atualmente, a necessidade se solução de antivírus está sendo atendida por meio das 3.000 licenças adquiridas pelo contrato nº 19 de 2018, com vigência de licenciamento de 36 meses.

A solução utilizada na instituição é o software Kaspersky Endpoint Security for Business Select para estações de trabalho e servidores, que detecta e corrige vulnerabilidades para reduzir os pontos de entrada dos ataques economizando tempo e automatizando as tarefas de implementação de software e dos sistemas operacionais.

Tal solução apresentou alto índice de proteção no que tange a websites maliciosos, aplicações maliciosas e dispositivos bloqueados. As verificações realizadas pela solução não eram dispendiosas aos recursos computacionais, portanto não afetaram a normalidade de uso dos equipamentos e permitiram que a instituição mantivesse um ambiente seguro e confiável.

A solução apresentou funcionalidades compatíveis ao Sistema Operacional Windows, majoritariamente utilizado pela instituição, realizou proteção antimalware, análise de riscos dos endpoints (a terminologia derivada de “software de antivírus endpoint” se refere a solução que atua em conjunto com múltiplas aplicações relacionadas à segurança, visto que, para se atingir um ínfimo de segurança, múltiplos fatores devem ser

considerados), controle avançado de ameaças, controle avançado contra exploração de vulnerabilidades, controle de conteúdo, controle de dispositivos, defesa em ataques relacionados a rede, firewall, dentre outras. Assim, foi avaliada pela equipe técnica como uma ferramenta eficaz, de fácil usabilidade e com excelente ambiente de gerência.

Todavia, há no mercado outras soluções de antivírus endpoint que possam vir a atender as necessidades aqui elencadas, total ou parcialmente, e algumas delas já utilizadas por outras instituições públicas, a exemplo do Bitdefender, adquirida pelo IFSULDEMINAS (Instituto Federal do Sul de Minas) e o F-Secure, utilizado pela USP (Universidade de São Paulo). Além disso, pode-se verificar que a própria Karpersky apresenta a versão Business Advanced, que dispõe de recursos extras que culminam com o avanço crescente do aumento da necessidade e amplitude das proteções tecnológicas em seus diversos níveis.

No mercado também existem soluções alternativas, como TrendMicro e soluções Open Source. Apesar de que, no momento da realização deste estudo técnico, não foram encontradas soluções open source de antivírus endpoint que atendessem às necessidades da instituição.

Abaixo uma tabela exemplificativa desse comparativo de mercado:

	Armadito-av	**BitDefender**	**ClamAV**	**F-Secure**	**Kaspersky**	**TrendMicro**
Antimalware	Não	Sim	Não	Sim	Sim	Sim
Análise de risco dos Endpoints	Não	Sim	Não	Sim	Sim	Sim
Controle avançado de ameaças	Não	Sim	Não	Sim	Sim	Não
Controle avançado contra exploração de vulnerabilidades	Não	Sim	Não	Sim	Sim	Não
Controle de conteúdo	Não	Sim	Não	Sim	Sim	Sim
Controle de Dispositivos	Não	Sim	Não	Sim	Sim	Sim
Defesa em ataques relacionados à rede	Não	Sim	Não	Sim	Sim	Sim
Firewall	Não	Sim	Não	Sim	Sim	Sim

Dada a tabela acima, pode-se observar que existem diversas soluções presentes no mercado que possam cumprir, ao menos em partes, os requisitos aqui elencados. Destacam-se a solução Kaspersky, que já possui implementação no parque informático do IFB e demonstra atender todos os requisitos elencados, a solução Bitdefender e a solução F-Secure, que, em sucinta análise, também se demonstraram capazes de gerir as necessidades da instituição, porém, exigindo maior recurso de tempo e financeiro, para capacitar toda a equipe técnica numa ferramenta totalmente nova e para preparar todo o ambiente para uma nova infraestrutura de serviço.

Dessa forma, os cenários considerados para este estudo foram:

Id	Descrição da solução (ou cenário)
1	Renovação do Kaspersky Endpoint Security for Business Select
2	Upgrade para a Solução Kaspersky Endpoint Security for Business Advanced
3	Licitação para aquisição de novo antivírus
4	Antivírus gratuito

3.2 – ANÁLISE COMPARATIVA DE SOLUÇÕES

ID	Solução	Análise da Solução
1	**Renovação do Kaspersky Endpoint Security for Business Select**	Atualmente utilizada pela instituição. Apresentou alto índice de proteção no que tange a websites maliciosos, aplicações maliciosas e dispositivos bloqueados. As verificações realizadas pela solução não eram dispendiosas aos recursos computacionais, portanto não afetaram a normalidade de uso dos equipamentos e permitiram que a instituição mantivesse um ambiente seguro e confiável. Avaliada pela equipe técnica como uma ferramenta eficaz, de fácil usabilidade e com excelente ambiente de gerência.
	Upgrade para a Solução Kaspersky	É uma atualização do sistema anterior, com melhoramento de diversas funcionalidades do antivírus; além disso, simplifica o gerenciamento da segurança centralizada com uma console local, na Web ou na nuvem, criptografando dados para evitar danos causados por vazamento de dados, inclui todas as funcionalidades disponíveis no Kaspersky Endpoint Security for Business Select, além de tecnologias avançadas adicionais para facilitar o

2	**Kaspersky Endpoint Security for Business Advanced**	gerenciamento e fortalecer a segurança dos servidores da rede do IFB, possui segurança adaptativa ao identificar vulnerabilidades e aplicar as correções mais recentes para fechar os pontos de entrada de ataque. Fornece proteção extra para servidores de dados como servidores Linux e Windows e contém funções de criptografia, além de função de firewall e de gerenciamento de criptografia integrados ao sistema operacional e com tecnologia de proteção alinhada com a LGPD.
3	**Licitação para aquisição de novo antivírus**	Aquisição de novas licenças de Antivírus – acarretaria em um novo processo de implantação, treinamento e adaptação que ocorreria em um longo período de tempo, devido ao tamanho da rede e a quantidade de equipamentos, além de nova capacitação da equipe técnica para gerir a nova ferramenta (software). Ou seja, maior tempo de implantação, implementação e maior gasto financeiro.
4	**Antivírus gratuito**	Soluções de antivírus gratuitos não atendem às demandas do IFB. Licenças Free são limitadas no que tange às especificações técnicas. O principal diferencial, está em painéis de controle centralizados – para facilitar a administração do antivírus em milhares de máquinas – e também no suporte técnico, que as fabricantes de antivírus não oferecem para quem usa o programa gratuito.

Verificar a disponibilidade de solução similar em outro órgão ou entidade da Administração Pública. Deve-se considerar apenas a pesquisa de preços de mercado na plataforma Painel de Preços do Governo Federal; Por se tratar de contratação de prestação de serviço de subscrição de software antivírus do tipo endpoint, classificado como serviço comum, amplamente utilizado pelos órgãos públicos, registra-se que **NÃO SE APLICA**:

- Verificar a disponibilidade de a existência de software público brasileiro;
- As políticas, os modelos e padrões de Governo eMAG, ePWG, ICP - Brasil, e eARQ.

Assim, esta demanda deverá ser atendida por meio de contratação de serviço**DEVENDO CONSIDERAR:**

- Contratação de serviço na modalidade de subscrição de software, observando as restrições do Anexo da Instrução Normativa SGD/ME 01 de 2019;
- As políticas, o modelo e o padrão de governo ePing.

4 – REGISTRO DE SOLUÇÕES CONSIDERADAS INVIÁVEIS

1. A implantação de uma nova solução de segurança num ambiente tecnológico complexo e distribuído, como o do Instituto Federal de Brasília – IFB não é trivial. Além da perda do investimento em licenças iniciais, a implantação de uma nova solução envolveria esforços de dimensionamento, projeto, instalação, configuração, customização, treinamento dos técnicos, distribuição de componentes para equipamentos servidores e estações de trabalho. Assim, a manutenibilidade da solução atual, inclusive com a possibilidade de upgrade de versão, enseja a continuidade operacional, visto que, a solução já está implantada e disseminada por toda a estrutura de TIC do IFB homologada, compatibilizada e com servidores treinados para administrá-la e dar-lhe manutenção. Além disso, esta solução já é utilizada por vários institutos federais (Conforme pesquisa realizada no site do Painel de Preços do Ministério do Planejamento, Desenvolvimento e Gestão (http://www.comprasnet.gov.br) identificou-se que há contratações de serviços semelhantes à do objeto em questão, atualizada e expandida com resultados satisfatórios. Atende ainda esta justificativa ao princípio da economicidade nas compras públicas, uma vez que neste momento de contingenciamento do Estado, manter a solução atual evitará custos adicionais de treinamento e implantação na operacionalização de uma nova solução.
2. Até o momento da realização deste estudo técnico, não foram encontradas soluções de antivírus Open Source que atendessem às demandas da instituição, uma vez que são mais limitadas no que tange às especificações técnicas: não apresentam painéis de controle centralizados – para facilitar a administração do antivírus em centenas de máquinas; não há um suporte técnico satisfatório para o tempo de resposta e às exigências institucionais, dentre outras características.
3. Portanto, as Soluções 3 e 4 são consideradas inviáveis para este momento.

5 – DESCRIÇÃO DA SOLUÇÃO DE TIC A SER CONTRATADA

5.1 – COMPARATIVO DAS SOLUÇÕES

COMPARATIVO DAS VERSÕES KASPERSKY SECURITY FOR BUSINESS SELECT X ADVANCED			
CARACTERÍSTICAS / FUNCIONALIDADES		**Kaspersky Endpoint Security for Business Select**	**Kaspersky Endpoint Security for Business Advanced**
	Oferece segurança multicamadas: Mecanismo antimalware que combina segurança com base em assinatura, heurística e análise		

	comportamental e tecnologias assistidas em nuvem para proteger a instituição contra ameaças conhecidas, desconhecidas e avançadas. Pode defender qualquer combinação de desktops e laptops Mac, Linux e Windows.	**X**	**X**
	Atualização da segurança: Oferece atualizações de banco de dados com muito mais frequência do que qualquer outro fornecedor de segurança. Além disso, utiliza várias tecnologias de segurança avançadas para garantir o fornecimento de taxas de detecção bastante aprimoradas com redução do tamanho das atualizações, para que uma porção maior da largura de banda para comunicação esteja disponível para outras tarefas.	**X**	**X**
	Proteção contra ameaças avançadas e desconhecidas: Quando um novo item de malware é revelado ao mundo, há um período de alto risco. Para oferecer proteção de hora zero contra essas ameaças, as tecnologias e a inteligência contra ameaças da Kaspersky Lab estão em constante evolução para garantir que a instituição fique protegida contra as novas ameaças, até mesmo as mais sofisticadas.	**X**	**X**
	Detecção de comportamento suspeito: Sempre que um aplicativo é inicializado na rede corporativa, o módulo Inspetor do Sistema monitora seu comportamento. Se um comportamento suspeito for detectado, o Inspetor do Sistema bloqueará automaticamente o aplicativo. Além disso, como o Inspetor do Sistema mantém um	**X**	**X**

Proteção de desktops e laptops Windows, Linux e Mac	Inspetor do Sistema mantem um registro dinâmico do sistema operacional, do registro etc., ele reverte automaticamente as ações mal-intencionadas que o malware implementou antes de ser bloqueado.		
	Proteção contra explorações: A tecnologia Automatic Exploit Prevention (AEP) inovadora ajuda a garantir que um malware não possa explorar as vulnerabilidades dos sistemas operacionais ou aplicativos em execução na rede. A AEP monitora especificamente os aplicativos mais usados como alvo, como Adobe Reader, Internet Explorer, Microsoft Office, Java e muitos outros, para oferecer uma camada extra de proteção e monitoramento de segurança contra ameaças desconhecidas.	**X**	**X**
	Controle de aplicativos e conectividade: Para alguns aplicativos, mesmo que os aplicativos possam não ser classificados como mal-intencionados, suas atividades podem ser consideradas de alto risco. Em muitos casos, é aconselhável que essas atividades sejam restritas. O Host-Based Intrusion Prevention System (HIPS) restringe as atividades no endpoint, de acordo com o "nível de confiança" atribuído ao aplicativo. O HIPS funciona em conjunto com o firewall pessoal em nível de aplicativo, que restringe a atividade de rede.	**X**	**X**
	Bloqueio de ataques à rede: A tecnologia Network Attack Blocker detecta e monitora atividades suspeitas na rede corporativa e		

	suspeitas na rede corporativa e permite que se pré-configure a forma como os sistemas responderão se for encontrado um comportamento suspeito.	**X**	**X**
	Utilização do poder da nuvem para uma segurança ainda melhor: Com milhões de usuários deixando o Kaspersky Security Network (KSN) com base na nuvem recebendo dados sobre comportamento suspeito em seus computadores, a instituição poderá se beneficiar de proteção aprimorada contra os malwares mais recentes. Esse fluxo de dados em tempo real garante que seus clientes possam se beneficiar de uma resposta rápida a novos ataques e ajuda a reduzir a incidência de "falsos positivos".	**X**	**X**
Proteção de servidores de arquivos	*Proteção de ambientes heterogêneos:* Protege servidores de arquivos que executam Windows, Linux ou FreeBSD. Os processos de verificação otimizados ajudam a garantir um impacto mínimo no desempenho de seus servidores. Além de proteger servidores de cluster, também protege servidores de terminal Microsoft e Citrix.	**X**	**X**
	Garantia de proteção confiável: No caso de um dos servidores de arquivos apresentar uma falha, as tecnologias de segurança serão automaticamente reinicializadas assim que o servidor de arquivos for reiniciado.	**X**	**X**
	Aumento da capacidade de gerenciamento: Cada minuto gasto com a administração e a geração de relatórios poderia ser dedicado a atividades estrategicamente		

	importantes. É por isso que a solução fornece um console centralizado que permite gerenciar a segurança em todos os endpoints (servidores de arquivos, estações de trabalho e dispositivos móveis) e facilita a geração de relatórios detalhados.	**X**	**X**
Controle de aplicativos, dispositivos e acesso à Internet	*Listas brancas dinâmicas para complementar a segurança:* O fornecedor investiu na criação de seu próprio Laboratório de listas brancas, que verifica os riscos de segurança de aplicativos. O banco de dados de aplicativos incluídos na lista branca contém mais de 1,3 bilhão de arquivos exclusivos e está crescendo em mais de 1 milhão de arquivos por dia. O Controle de aplicativos e Whitelist dinâmico torna mais fácil executar uma política de Default Deny que bloqueia todos os aplicativos, a menos que eles estejam em sua whitelist. Numa implementação ou atualização de uma política de Negação Padrão, o novo modo de teste permitirá configurar a política em um ambiente de teste, para que se possa verificar se a política está configurada corretamente, antes da "entrada em operação".	**X**	**X**
	Prevenção da conexão de dispositivos não autorizados: As ferramentas de Controle de dispositivos facilitam o gerenciamento dos dispositivos que têm permissão para acessar sua rede corporativa de TI. Pode-se configurar controles com base na hora do dia, na localização geográfica ou no tipo de dispositivo. Pode-se também alinhar os controles com o Active	**X**	**X**

	Directory – para administração granular e atribuição de política. Os administradores também podem usar máscaras na criação de regras de controle de dispositivos, para que vários dispositivos possam ser facilmente incluídos em listas brancas para uso.		
	Monitoramento e controle do acesso à Internet: As ferramentas de Controle da Web permitem configurar políticas de acesso à Internet e monitorar o uso da Internet. É fácil proibir, limitar, permitir ou auditar as atividades dos usuários em sites individuais ou em categorias de sites, como sites de jogos, de apostas ou de redes sociais. Os controles de localização geográfica e de hora do dia podem ser alinhados com o Active Directory – para ajudar na administração e na definição de políticas.	**X**	**X**
Centralização das tarefas de gerenciamento	*Possibilidade de controlar todas as funções em um único console:* O Kaspersky Endpoint Security for Business | Advanced inclui o Kaspersky Security Center, um único console de gerenciamento unificado que garante a visibilidade e o controle de todas as tecnologias de segurança de endpoints da Kaspersky Lab que estiver executando. O Kaspersky Security Center permite gerenciar a segurança dos dispositivos móveis, laptops, desktops, servidores de arquivos, máquinas virtuais e muito mais, com a conveniência de um console de "painel único".		**X**
	Oferece um nível mais alto de integração: Como o código		

	altamente integrado resulta em produtos que proporcionam segurança, desempenho e capacidade de gerenciamento maiores, toda a funcionalidade de proteção de endpoint está contida na mesma base de códigos, para que não ocorra nenhum problema de incompatibilidade com o qual a equipe de TI da instituição tenha que lidar. Em vez disso, ela se beneficia com as tecnologias de segurança integradas com perfeição que fazem mais para proteger seu ambiente de TI, enquanto o gerenciamento centralizado economiza tempo.	**X**	**X**
	Segurança de dispositivos móveis robusta: O antiphishing oferece proteção contra sites que tentam roubar informações ou detalhes de identidade, e o antispam ajuda a filtrar chamadas e textos indesejados. As ferramentas de controle flexíveis permitem bloquear a execução de aplicativos não autorizados e o acesso a sites perigosos. O rastreamento e o bloqueio de incidentes são detectados automaticamente, e os dispositivos são bloqueados.		**X**
	Separação de dados corporativos e pessoais: A tecnologia de "empacotamento de aplicativos" permite configurar contêineres especiais em cada dispositivo. Os aplicativos corporativos são armazenados nos contêineres – totalmente separados dos dados pessoais do usuário. É possível aplicar a criptografia a todos os dados conteinerizados e impedir que os dados sejam copiados e colados fora do contêiner. Além		**X**

Proteção de dispositivos móveis*	disso, pode-se solicitar autorização de usuário adicional antes de os aplicativos conteinerizados terem permissão para serem executados. Se um servidor sair da instituição, o recurso Limpeza seletiva operado remotamente permitirá a exclusão do contêiner corporativo, sem a exclusão das configurações e dos dados pessoais do proprietário do dispositivo.		
	Suporte a plataformas comuns de MDM: Com os recursos de gerenciamento de dispositivos móveis (MDM) aprimorados, fica fácil aplicar as políticas de MDM de grupo ou individuais aos dispositivos Microsoft Exchange ActiveSync e iOS MDM, através de uma única interface. O suporte para Samsung KNOX permite gerenciar várias configurações de dispositivos Samsung.X		**X**
*Alguns recursos não estão disponíveis para algumas das plataformas móveis suportadas.	*Bloqueio, limpeza e localização de dispositivos ausentes:* Os recursos de segurança operados remotamente ajudam a proteger dados corporativos nos dispositivos ausentes. Os administradores e os usuários podem bloquear o dispositivo, excluir dados corporativos e identificar sua localização. Se um ladrão alterar o cartão SIM, o recurso Verificação do Chip enviará o novo número de telefone, para que você possa ainda executar os recursos antirroubo. O suporte a Google Cloud Messaging (GCM) ajuda a garantir que os telefones Android recebam comandos antirroubo rapidamente.		**X**

	Portal de autoatendimento: O Portal de autoatendimento facilita a ativação de dispositivos móveis pessoais na rede corporativa. Além disso, o portal oferece aos usuários acesso remoto aos principais recursos antirroubo, para que os usuários possam dar uma resposta rápida à perda de um dispositivo e reduzir o risco de perda de dados, sem sobrecarregar os administradores.		**X**
	Redução da sobrecarga sobre os administradores de TI: Um console centralizado único permite gerenciar dispositivos móveis (e sua segurança) e facilita a aplicação de políticas consistentes em diferentes plataformas móveis. Além disso, o Console da Web permite gerenciar os dispositivos móveis e sua segurança, além da segurança de outros endpoints, de qualquer lugar onde você possa estar on-line.		**X**
Gerenciamento de sistemas	Gerenciamento de vulnerabilidades e correções: Detecção e priorização automatizadas de vulnerabilidades do SO e de aplicativos, combinadas com a rápida distribuição automatizada de correções e atualizações.		**X**
Inventários de hardware e software e gerenciamento de licenças	Identificação, visibilidade e controle (incluindo bloqueio), juntamente com o gerenciamento de uso da licença, fornecem informações sobre todos os softwares e hardwares implementados por todo o ambiente, incluindo dispositivos removíveis. Estão disponíveis também: gerenciamento de licenças de software e hardware, detecção de dispositivos		**X**

	detecção de dispositivos convidados, controles de privilégios e provisionamento de acesso.		
Criptografia Poderosa Proteção de dados	Criptografia dos arquivos / pastas (FLE) e do disco completo (FDE) pode ser aplicada aos endpoints. O suporte para o "modo portátil" garante a administração de criptografia em todos os dispositivos que saem dos domínios administrativos.		**X**
Conexão flexível do usuário	Autenticação pré-inicialização (Pre-boot authentication - PBA) para aumentar a segurança que inclui login único opcional para transparência do usuário. Também está disponível a autenticação com base em dois fatores ou em token.		**X**
Criação de políticas Integradas	Integração única de criptografia com controles de aplicativos e dispositivos fornece uma camada adicional de segurança aprimorada e facilidade administrativa.		**X**
Controle de acesso com base em função (Role Based Access Control — RBAC)	Responsabilidades administrativas podem ser atribuídas através de redes complexas, com exibição do console personalizada de acordo com as funções e direitos atribuídos.		**X**
Implementação do sistema operacional	Armazenamento e implementação de imagens "golden" do SO a partir de um local centralizado, incluindo suporte a UEFI.		**X**
Integração SIEM	Suporte para sistemas IBM® QRadar e HP ArcSight SIEM.		**X**
Distribuição e solução de problemas de	Implementação e aplicação remotas do software e atualização do SO disponível por demanda ou programada. A solução de problemas remota com economia		**X**

software	de tempo e a distribuição eficiente de software são suportadas através da tecnologia Multicast.		

5.2 - DA SOLUÇÃO ESCOLHIDA

A natureza sensível das informações elaboradas ou tramitadas pelo Instituto Federal de Brasília – IFB impõe severos requisitos de confidencialidade, integridade, autenticidade e disponibilidade dessas informações. A perda e/ou roubo de informações por malwares, códigos maliciosos, não enseja apenas em impacto nos recursos financeiros, mas também na desativação de serviços e perdas intangíveis que incluem a confiança na Instituição e sua reputação.

Dessa forma, é de fundamental importância que todos os ativos (servidores, estações de trabalho) do Instituto Federal de Brasília – IFB possuam a proteção de um antivírus compatível com os requisitos de segurança da informação e que possa ser gerenciada pelos responsáveisde TIC deste Instituto.

Atualmente o Instituto Federal de Brasília – IFB possui aproximadamente 3.000 licenças do Kaspersky Endpoint Security for Business Select, entretanto, com o aumento de ataques mais elaborados e com a preocupação com a Lei Geral de Proteção de Dados (LGPD) a qual, naturalmente, exige um nível maior de proteção, foi identificada a necessidade de upgrade da solução para o Kaspersky Endpoint Security for Business Advanced, que é uma atualização do sistema anterior, com melhoramento de diversas funcionalidades do antivírus. Além disso:

- Simplifica o gerenciamento da segurança centralizada com uma console local, na Web ou na nuvem, criptografando dados para evitar danos causados por vazamento de dados;
- Inclui todas as funcionalidades disponíveis no Kaspersky Endpoint Security for Business Select, versão utilizada atualmente pela instituição;
- Oferece tecnologias avançadas adicionais para facilitar o gerenciamento e fortalecer a segurança dos servidores da rede do IFB;
- Possui segurança adaptativa ao identificar vulnerabilidades e aplicar as correções mais recentes para fechar os pontos de entrada de ataque;
- Permite controlar quais aplicativos podem ser executados ou não;
- Possui recursos de detecção e resposta para endpoints que identificam comportamentos anormais;
- Detecta e neutraliza automaticamente ransomware direcionado e, em particular, ameaças sem arquivo, que tentam imitar o comportamento comum, como a execução de scripts do PowerShell;
- Fornece proteção extra para servidores de dados como servidores Linux e Windows e contém funções de criptografia, além de função de firewall e de gerenciamento de criptografia integrados ao sistema operacional e com tecnologia de proteção alinhada com a LGPD;
- Fornece gerenciamento simplificado de sistemas e automatiza tarefas de software, incluindo a criação, o armazenamento e a clonagem de imagens do sistema operacional para economizar tempo sempre que existir; dentre outras funcionalidades;
- Oferece proteção contra as ameaças móveis mais recentes. O antiphishing oferece proteção contra sites que tentam roubar informações ou detalhes de identidade, e o antispam ajuda a filtrar chamadas e textos indesejados. As ferramentas de controle flexíveis permitem bloquear a execução de aplicativos não autorizados e o acesso a sites perigosos. O rastreamento e o bloqueio de incidentes são detectados automaticamente, e os dispositivos são bloqueadas;
- Oferece um console centralizado único que permite gerenciar dispositivos móveis (e sua segurança) e facilita a aplicação de políticas consistentes em diferentes plataformas móveis. Os recursos de segurança operados remotamente podem ajudar a proteger dados

corporativos nos dispositivos ausentes. Os administradores e os usuários podem bloquear o dispositivo, excluir dados corporativos e identificar sua localização, dentre outras ações possíveis.

Dentre as características que deverão compor a solução, destacam-se:

- Uma solução de Antivírus padronizada com gerência centralizada;
- Visão situacional com relação ao nível de infecção da rede computacional do IFB;
- Rastreamento em tempo real de arquivos e processos maliciosos;
- Efetivo controle do número de licenças de antivírus de propriedade do Instituto Federal de Brasília – IFB em uso;
- Privacidade das informações, ou seja, nem mesmo o fabricante da solução terá acesso a essas informações, a não ser que o Instituto Federal de Brasília – IFB deseje e permita;
- Antimalware: a solução deverá realizar análises heurísticas acerca dos tipos de vírus que podem vir a causar malefícios ao dispositivo, tais quais vírus, worms, trojans, spywares, adwares, keyloggers, rootkits, entre outros. Deverá também conter formas personalizáveis de escaneamento envolvendo processamento em nuvem;
- Análise de riscos dos Endpoints: identifica, realiza o acesso e remedia vulnerabilidades através de análises de vulnerabilidade, que por sua vez podem ser agendadas ou requisitadas. Após realizar a análise, a solução deverá fornecer um resumo dos riscos encontrados em uma dashboard, ou um relatório, e instruir dicas de como mitigar as vulnerabilidades;
- Controle avançado de ameaças: Destinado a aplicações maliciosas que por ventura venham a evadir a análises heurísticas. Neste módulo, a solução deverá monitorar, de maneira contínua, o comportamento dos processos e bloquear possíveis formas de manipulação;
- Controle avançado contra exploração de vulnerabilidades: A solução deverá atuar contra-ataques zero-day. Neste módulo, a solução se atualizará sobre os exploits mais recentes para que possa mitigar vulnerabilidades que possam ter se evadido de outras varreduras. Deverá acompanhar processos e proteger o dispositivo contra brechas de segurança;
- Controle de conteúdo: A solução deverá executar ações como controle de tráfego, controle de acesso à web, proteção de dados e controle de aplicações;
- Controle de dispositivos: Prevenir que dados sensíveis ou vírus sejam atrelados ao computador via dispositivos removíveis, como CD/DVDs, pendrives, dispositivos de armazenamento, entre outros;
- Defesa em ataques relacionados a rede: A solução deverá realizar uma análise do tráfego de rede a fim de identificar vulnerabilidades;
- Firewall: Este módulo deverá controlar a atividade de rede nas aplicações do computador;
- Contemple dispositivos remotos; e
- Implemente recursos de segurança que atendam às recomendações da Lei Geral de Proteção de Dados (LGPD).

Portanto, quando se trata de tecnologia e de segurança da informação, sempre existe a necessidade de adquirir produtos com sistemas mais avançados de detecção de ataques virtuais ou quaisquer outros programas maliciosos pulverizados pela internet.

Nesse sentido, faz imperioso a atualização dos sistemas antivírus do IFB pela versão Kaspersky Endpoint Security for Business Advanced, ainda mais quando observados o crescente número de ataques de ransomwares em órgãos da Administração Pública Federal nos últimos dois anos e a realidade que se impôs com a Pandemia da Covid-19 de trabalho remoto, onde aumentou o uso dos dispositivos institucionais e pessoais de forma remota, o que exige da Instituição uma atenção maior com a Segurança da Informação e com o que a Lei Geral de Proteção de Dados (LGPD) recomenda.

Além disso, o levantamento orçamentário realizado neste estudo técnico preliminar para a versão mais avançada da solução do antivírus não afronta o previsto no Plano Diretor de Tecnologia da Informação e Comunicação do IFB para o triênio 2021-2023, uma vez que neste consta a previsão de valor unitário de licenciamento de aproximadamente de R$ 140,63 (cento e quarenta reais e sessenta e três centavos), e o valor médio encontrado neste estudo é de R$ 108,40 (Cento e oito reais e quarenta centavos). Essa análise se encontra no item 7 deste documento.

Assim, a equipe de planejamento da contratação optou pela solução:***Kaspersky Endpoint Security for Business Advanced.***

5.3 - REQUISITOS DE GARANTIA, MANUTENÇÃO E SUPORTE

A CONTRATADA deverá observar os seguintes requisitos de garantia, manutenção e suporte:

- O período de licenciamento do software será de 36 (trinta e seis) meses;
- Prestar o serviço suporte técnico em horário comercial no regime de 08 (oito) horas por dia, 5 (cinco) dias por semana, durante todo o período de vigência do contrato, salvaguardados os casos de interrupções emergenciais.
- Deverá ser garantida neste prazo a atualização de versões, releases, componentes (bibliotecas, filtros, etc.) e módulos dos produtos. Todos os produtos deverão ter o mesmo período de licenciamento.
- Oferecer equipe técnica Composta de técnicos certificados pelo fabricante do software fornecido, e preparada para dar todo o suporte técnico e ajuda necessária para maximizar os benefícios oferecidos pelo software, aumentando a sua performance;
- Fornecer número telefônico para contato e e-mail, para abertura e registro de chamados de suporte técnico;
- Comunicar à CONTRATANTE, por escrito, qualquer anormalidade nos serviços e prestar os esclarecimentos julgados necessários;
- Disponibilizar ao IFB mecanismos para que os técnicos do Órgão possam solicitar diretamente ao fabricante as mídias ou as autorizações para download das versões/atualizações, 36 meses de suporte prestado diretamente pelo fabricante.
- Disponibilizar, sem custo adicional, as atualizações da solução de software antivírus;
- Não será admitida cobrança retroativa de valores referentes a serviços de suporte técnico e de atualização de versões relativa a eventual período em que a contratante possa ficar sem cobertura contratual;
- Não será admitida cobrança de valores para eventual reativação do serviço durante a vigência da subscrição;
- Não será admitida cobrança de valores relativos a serviço de correção de erros durante a vigência da subscrição, inclusive retroativos, que devem ser corrigidos sem ônus à contratante. Caso os erros venham a ser corrigidos em versão posterior do software, essa versão deverá ser fornecida sem ônus para a contratante.

6 – ANÁLISE DE CUSTOS

6.1 – PESQUISA DE PREÇOS – CUSTO POR LICENÇA

	Estimativa de Custo por Licença

Kaspersky Endpoint Security for Business Advanced	Pregão 04/2021 - IFAM (R$)	Pregão 04/2021 UNIFESSPA (R$)	Pregão 20/2021 ALMT (R$)	Pregão 07/2021 UFRS (R$)	Proposta VTECH/IFB 12/2021 (R$)
Valor Licença	106,00	81,70	123,44	111,86	119,00
Qtde Licenças	5.230	1.000	1.400	1.000	3.000[2]
Valor total R$	**554.380,00**	**81.700,00**	**172.816,00**	**111.860,00**	**357.000,00**

6.2 – ESTIMATIVA DE CUSTOS CONFORME PESQUISA DE PREÇOS

Descrição da solução	Estimativa de Custo					
	Qtde Licença	Pregão 04/2021 - IFAM (R$)	Pregão 04/2021 UNIFESSPA (R$)	Pregão 20/2021 ALMT (R$)	Pregão 07/2021 UFRS (R$)	Proposta VTECH/IFB 12/2021 (R$)
Upgrade para a Solução Kaspersky Endpoint Security for Business Advanced	1	106,00	81,70	123,44	134,53	119,00
	4.042	428.452,00	330.231,40	498.944,48	452.138,12	480.998,00

7 – ESTIMATIVA DE CUSTO TOTAL DA CONTRATAÇÃO

A estimativa de custo para atendimento foi obtida a partir da média dos preços elencados no item 6 deste documento. Portanto, totaliza cerca de R$ 438.152,80 (Quatrocentos e trinta e oito mil, cento e cinquenta e dois reais, oitenta centavos), onde o custo médio por licença é de R$ 108,40 (Cento e oito reais e quarenta centavos).

Solução	Estimativa de Custo Total da Contratação		
	Qtde Licença	Preço Médio (R$)	Cálculo de Referência
Kaspersky Endpoint Security for Business Advanced	1	108,40	(106,00 + 81,70 + 123,44 + 111,86 + 119,00) / 5
	4.042	438.152,80	(428.452,00 + 330.231,40 + 498.944,48 + 452.138,12 + 480.998,00) / 5

A Tabela seguinte apresenta a estimativa do Valor Total da Contratação por Unidade do Instituto Federal de Brasília.

Solução	Quantitativo de Licenças por Campi / Reitoria CATMAT - 350949				
	Unidade		Quantidade de Licenças	Valor Unitário R$	Valor Total R$
Kaspersky Endpoint Security for Business Advanced	REIT	Reitoria	150	108,40	16.260,00
	CCEI	Campus Ceilândia	270	108,40	29.268,00
	CEST	Campus Estrutural	250	108,40	27.100,00
	CGAM	Campus Gama	520	108,40	56.368,00
	CPLA	Campus Planaltina	200	108,40	21.680,00
	CSAM	Campus Samambaia	370	108,40	40.108,00
	CSSB	Campus São Sebastião	520	108,40	56.368,00
	CTAG	Campus Taguatinga	520	108,40	56.368,00
	CBRA	Campus Brasília	727	108,40	78.806,80

CREM	Campus Recanto das Emas	320	108,40	34.688,00
CRFD	Campus Riacho Fundo	195	108,40	21.138,00
Total de Licenças		**4.042**		**438.152,80**

8 – JUSTIFICATIVA PARA O PARCELAMENTO OU NÃO DA SOLUÇÃO

A aquisição das licenças, deverá ser realizada em única parcela no que tange a compra. Uma vez que o mercado oferece diversas empresas na área de TI, com capacidade de atender a esta demanda.

9 – RESULTADOS PRETENDIDOS

- Manter o sistema de segurança do parque computacional do IFB;
- Evitar novos gastos com o processo de configuração inicial caso fosse adquirido um novo software;
- Manter as atividades administrativas e educacionais desenvolvidas nos Campi /Reitoria do IFB;
- Deixar o IFB mais próximo daquilo que é preconizado pela LGPD.

10 – DECLARAÇÃO DE VIABILIDADE DA CONTRATAÇÃO

Declara-se a viabilidade da contratação visto que:

- O objeto desta demanda enquadra-se como serviço comum, nos termos do parágrafo único do artigo 1º da Lei 10.520/02 e o parágrafo segundo ao artigo 2º do Decreto 5.450/05, por possuir padrões de desempenho e características gerais e especificações usualmente encontradas no mercado;
- Esta contratação está prevista no Plano Diretor de TIC 2021 - 2023, assim como no Plano Anual de Compras 2021;
- Os requisitos desta demanda estão de acordo com o Anexo - I DIRETRIZES ESPECÍFICAS DE PLANEJAMENTO DA CONTRATAÇÃO - CONTRATAÇÃO DE LICENCIAMENTO DE SOFTWARE E SERVIÇOS AGREGADOS da Instrução Normativa SGD/ME 01/2019.

Portanto, com o objetivo de especificar requisitos, foi realizado um levantamento de soluções disponíveis no mercado. A solução escolhida foi a de realizar pregão eletrônico (SRP) para aquisição da renovação das licenças do antivírus Kaspersky com upgrade para a versão Business Advanced. Assim, diante do exposto acima, entendemos ser VIÁVEL a contratação da solução demandada.

11 – ITENS DO PLANEJAMENTO QUE NÃO SE APLICAM

- Contratações Correlatas e/ou Interdependentes;
- Providências futuras a serem adotadas;
- Possíveis impactos ambientais.

12 – ASSINATURAS

A Equipe de Planejamento da Contratação foi instituída conforme Documento de Oficialização da Demanda (CONTRATACAO_TI 32/2021 - DTIC/RIFB/IFBRASILIA).

Conforme o § 2º do Art. 11 da IN SGD/ME nº 01, de 2019, o Estudo Técnico Preliminar deverá ser aprovado e assinado pelos Integrantes Técnicos e Requisitantes e pela autoridade máxima da área de TIC:

INTEGRANTE TÉCNICO	INTEGRANTE REQUISITANTE
Assinado eletronicamente Edimária Cerqueira Rodrigues Lamounier **Matrícula/SIAPE: 2249275** Brasília-DF, 23 de dezembro de 2021.	***Assinado eletronicamente*** Daniel Pereira de Sousa **Matrícula/SIAPE: 2226521** Brasília-DF, 23 de dezembro de 2021.

13 – APROVAÇÃO E DECLARAÇÃO DE CONFORMIDADE

Conforme parecer da equipe de planejamento da contratação, o levantamento orçamentário realizado neste estudo para renovação da solução de antivírus com upgrade de versão não afronta financeiramente o previsto no Plano Diretor de Tecnologia da Informação e Comunicação do IFB para o triênio 2021-2023 ao mesmo tempo que permitirá uma camada a mais de proteção à instituição. Portanto, aprovo este Estudo Técnico Preliminar e atesto sua conformidade às disposições da Instrução Normativa SGD/ME nº 1, de 4 de abril de 2019.

AUTORIDADE MÁXIMA DA ÁREA DE TIC

Assinado eletronicamente

Bruno Nepomuceno de Oliveira

Matrícula/SIAPE: 1590823

Brasília-DF, 23 de dezembro de 2021.

---

[1] O quantitativo foi baseado no que foi informado no Plano Diretor de Tecnologia da Informação e Comunicação do Instituto Federal de Brasília 2021-2023 e ratificado junto aos gestores dos campi e da reitoria via e-mail anexado a este documento.

[2] A cotação junto ao fornecedor no quantitativo de 3.000 licenças foi baseada no licenciamento vigente no momento da construção do Estudo Técnico Preliminar, dado que, até o momento da solicitação da cotação, nem todos os campi haviam informado a quantidade necessária de licenças para se fechar o quantitativo de licenciamento da contratação atual. Portanto, a cotação foi baseada no quantitativo de licenças vigente até dezembro de 2021. Todavia, a contratação será baseada no quantitativo descrito na tabela que se encontra no item 4 deste documento e conforme previsto no Estudo Técnico Preliminar.

ANEXO III DO TERMO DE REFERÊNCIA

Modelo de Termo de Compromisso

TERMO DE COMPROMISSO DE MANUTENÇÃO DE SIGILO

Pelo presente instrumento o <NOME DO ÓRGÃO>, sediado em <ENDEREÇO>, CNPJ n° <CNPJ>, doravante denominado CONTRATANTE, e, de outro lado, a <NOME DA EMPRESA>, sediada em <ENDEREÇO>, CNPJ n° <Nº do CNPJ>, 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.

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.

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.

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 ideias, 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.

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.

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. 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.

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

- 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.
- 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.

- A CONTRATANTE elege o foro da <CIDADE DA CONTRATANTE> , 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.
- 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 IV DO TERMO DE REFERÊNCIA

Modelo de Termo de Ciência

TERMO DE CIÊNCIA

CONTRATO Nº	xxxx/aaaa		
OBJETO	<objeto do contrato>		
CONTRATADA	<nome da contratada>	CNPJ	xxxxxxxxxxxx
PREPOSTO	<Nome do Preposto da Contratada>		
GESTOR DO CONTRATO	<Nome do Gestor do Contrato>	MATR.	xxxxxxxxxxxx

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)>	**<xxxxxxxxxx>**	
<Nome do(a) Funcionário(a)>	**<xxxxxxxxxx>**	
...	**...**	**...**

_ <Local>, <dia> de <mês> de <ano>.

ANEXO V DO TERMO DE REFERÊNCIA

Modelo de Proposta

PREGÃO ELETRÔNICO N. xx/21

OBJETO: Esta licitação tem por objeto o registro de preços para contratação de empresa para fornecimento e instalação de solução de controle de acesso, equipamentos comutadores de dados (swtich) e pontos de acesso (access point), abrangendo todos os acessórios, softwares, licenças, instalação e treinamento para equipe, com garantia técnica on-site de 60 (sessenta) meses para o Instituto Federal de Brasília, conforme quantidades e exigências estabelecidas neste instrumento.

EMPRESA:_____CNPJ:_____ENDEREÇO:_____TELEFONE:_____E-MAIL: _____

Ao IFB

Em atendimento ao Edital do Pregão à epígrafe, apresentamos a seguinte proposta de preços:

				Indicar a origem do produto (nacional ou importado)			**PREÇO UNITÁRIO**	**PREÇO TOTAL**

ITEM	DESCRIÇÃO	MARCA	MODELO		UN.	QUANT.	R$	R$
1					U			
2					U			
3					U			
4					U			
5	...				U			

PREÇO TOTAL POR EXTENSO:

PRAZO DE VALIDADE DA PROPOSTA:_____(por extenso) dias (observar o disposto no Edital).

PRAZO DE GARANTIA DO OBJETO:_(por extenso) meses (observar o disposto no Edital).

PRAZO DE ENTREGA DO OBJETO, CONFORME DEFINIDO NO ANEXO XXX DO EDITAL

Declaramos que:

a. **os equipamentos ofertados, caso necessário, receberão atendimento de garantia na rede de assistência autorizada pelo fabricante;**
b. **informaremos os preços unitários dos equipamentos, das peças e dos demais componentes que integram o objeto da licitação sempre que solicitado pela CONTRATANTE, para fins de registro patrimonial;**
c. **serão fornecidas peças de reposição originais durante todo o período de garantia, podendo também ser utilizadas peças de tecnologia mais recente, também originais, de desempenho igual ou superior.**

DADOS PARA ASSINATURA DA ATA DE RP E DO CONTRATO	

Nome do signatário	
Cargo	
Qualificação **(CPF, naturalidade e domicílio)**	
OBS.: O signatário deve possuir poderes de administração estabelecidos em contrato social e/ou possuir procuração com poderes para assinar atas de registro de preços e contratos em nome da empresa. **A documentação comprobatória deverá ser encaminhada quando da assinatura da ata de registro de preços.**	

Brasília, xx de xxxx 2021.

Assinatura do representante legal da empresa

Nome do representante legal da empresa

ANEXO VI DO TERMO DE REFERÊNCIA

ORDEM DE SERVIÇO OU DE FORNECIMENTO DE BENS

1 – IDENTIFICAÇÃO			
Nº da OS/OFB	**xxxx/aaaa**	**Data de emissão**	**<dd/mm/aaaa>**
Contrato nº	**xx/aaaa**		
Objeto do Contrato	**<Descrição do objeto do contrato>**		

Contratada	**<Nome da contratada>**	**CNPJ**	**99.999.999/9999-99**
Preposto	**<Nome do preposto>**		
Início vigência	**<dd/mm/aaaa>**	**Fim vigência**	**<dd/mm/aaaa>**
ÁREA REQUISITANTE			
Unidade	**< Sigla – Nome da unidade>**		
Solicitante	**<Nome do solicitante>**	**E-mail**	**xxxxxxxxxxxx**

2 – ESPECIFICAÇÃO DOS BENS/SERVIÇOS E VOLUMES ESTIMADOS

Item	Descrição do bem ou serviço	Métrica	Valor unitário (R$)	Qtde/Vol.	Valor Total (R$)
1					
...					
Valor total estimado da OS/OFB					

3 – DATAS E PRAZOS PREVISTOS

Data de Início:	**<dd/mm/aaaa>**	**Data do Fim:**	**<dd/mm/aaaa>**

CRONOGRAMA DE EXECUÇÃO/ENTREGA

Item	Tarefa/entrega	Início	Fim
1		**<dd/mm/aaaa>**	**<dd/mm/aaaa>**
...		**<dd/mm/aaaa>**	**<dd/mm/aaaa>**

4 – ARTEFATOS / PRODUTOS

Fornecidos	A serem gerados e/ou atualizados

Autoriza-se a <execução dos serviços / entrega dos bens> correspondentes à presente <OS/OFB>, no período e nos quantitativos acima identificados.

<Nome >

<Responsável pela demanda/ Fiscal Requisitante>

Matr.: <Nº da matrícula>

<Nome >

Gestor do Contrato

Matr.: <Nº da matrícula>

<Local>, xx de xxxxxxxxx de xxxx

Documento assinado eletronicamente por:

- **Hugo Silva Faria**, **TEC DE TECNOLOGIA DA INFORMACAO**, em 20/04/2022 14:12:31.
- **Daniel Pereira de Sousa**, **COORDENADOR - FG1 - CITIC**, em 20/04/2022 13:48:48.
- **Julliana Almeida Cavalcanti Fialho**, **PRO-REITOR - SUBST - PRAD**, em 20/04/2022 11:12:02.
- **Bruno Nepomuceno de Oliveira**, **DIRETOR - CD3 - DTIC**, em 20/04/2022 10:28:19.

Este documento foi emitido pelo SUAP em 19/04/2022. Para comprovar sua autenticidade, faça a leitura do QRCode ao lado ou acesse https://suap.ifb.edu.br/autenticar-documento/ e forneça os dados abaixo:

Código Verificador: 372540
Código de Autenticação: fe85944a57

INSTITUTO FEDERAL
Brasília

Reitoria
Setor de Autarquias Sul, Quadra 02, Lote n° 03, Edifício Siderbrás., Asa Sul, BRASILIA / DF, CEP 70.070-906
(61) 2103-2154

MODELO DE TERMO DE CONTRATO – SOLUÇÃO DE TECNOLOGIA DA INFORMAÇÃO E COMUNICAÇÃO

ANEXO .....

PROCESSO Nº 23098.001656.2021-46

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 xxxxx/2022, QUE FAZEM ENTRE SI O INSTITUTO FEDERAL DE EDUCAÇÃO, CIÊNCIA E TECNOLOGIA DE BRASÍLIA – IFB **E A EMPRESA .....**

O INSTITUTO FEDERAL DE EDUCAÇÃO, CIÊNCIA E TECNOLOGIA DE BRASÍLIA – IFB, Autarquia Federal vinculada ao Ministério da Educação – MEC, com sede no SAUS, Quadra 2, Bloco E, Subsolo 2° e Andares: 4º; 5º; 6º;7º;8º; 9º e 10º, Asa Sul – Brasília-DF, CEP. 70.070-020, inscrito no CNPJ sob o nº 10.791.831/0001-82, neste ato representado(a) pelo(a) ..... (*cargo e nome*), nomeado(a) pela Portaria nº ....., de ..... de ..... de 20..., publicada no *DOU* de ..... de ..... de ....., portador(a) da carteira de identidade n° ....., expedida pela ....., CPF: ..... e Matrícula Funcional nº ....., doravante denominado 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 23098.001656.2021-46 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 empresa especializada para prestação de serviços de renovação da SOLUÇÃO ANTIVIRUS KASPERSKY ENDPOINT SECURITY FOR BUSINESS - ADVANCED pelo período de 36 (trinta e seis) meses, com serviços de instalação, suporte técnico, treinamento da equipe se necessário e garantia, 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	QTDE	VALOR UNITÁRIO (R$)	VALOR TOTAL (R$)
1 350949	Licença Kaspersky Endpoint Security for Business Advanced com serviços de instalação, suporte técnico, treinamento da equipe se necessário e garantia, pelo período de 36 (trinta e seis) meses.	UN	4.402		
VALOR TOTAL DA CONTRATAÇÃO R$					

2. CLÁUSULA SEGUNDA – VIGÊNCIA

2.1. O prazo de vigência deste Contrato é aquele fixado no Termo de Referência anexo do Edital, 36(trinta e seis) meses com início na data da sua assinatura.

2.1.1. A vigência poderá ultrapassar o exercício financeiro, desde que as despesas referentes à contratação sejam integralmente empenhadas até 31 de dezembro, para fins de inscrição em restos a pagar, conforme Orientação Normativa AGU n° 39, de 13/12/2011.

2.2. O fornecimento da solução será iniciado na data de início constante na Ordem de Serviço-OS, cujas etapas observarão o cronograma fixado no Termo de Referência.

2.3. A prorrogação dos prazos de execução e vigência do contrato será precedida da correspondente adequação do cronograma físico-financeiro, bem como de justificativa e autorização da autoridade competente para a celebração do ajuste, devendo ser formalizada nos autos do processo administrativo.

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:

Nota de Empenho: Emitida em:

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

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 Subseção Judiciária de Brasília, integrante da Seção Judiciária do Distrito Federal - Justiça Federal, para dirimir os litígios que decorrerem da execução deste Termo de Contrato que não possam ser compostos pela conciliação, conforme art. 55, §2º da Lei nº 8.666/93.

Para firmeza e validade do pactuado, o presente Termo de Contrato foi lavrado em duas (duas) vias de igual teor, que, depois de lido e achado em ordem, vai assinado pelos contraentes e por duas testemunhas.

Brasília, ... de..... de 2022.

_____ _____

Representante legal do CONTRATANTE Representante legal da CONTRATADA

TESTEMUNHAS:

NOME: NOME:
CPF: CPF:

MINISTÉRIO DA EDUCAÇÃO

Instituto Federal de Educação, Ciência e Tecnologia de Brasília

ATA DE REGISTRO DE PREÇOS

Ministério da Educação
Instituto Federal de Educação, Ciência e Tecnologia de Brasília

ATA DE REGISTRO DE PREÇOS
N.º .....

O INSTITUTO FEDERAL DE EDUCAÇÃO, CIÊNCIA E TECNOLOGIA DE BRASÍLIA - IFB com sede à à SAUS QUADRA 2 LOTE 03 bloco E, Edifício Siderbrás Asa Sul – Brasília/DF, CEP 70.070-906, inscrito(a) no CNPJ/MF sob o nº ....., neste ato representado(a) pelo(a) ..... (*cargo e nome*), nomeado(a) pela Portaria nº ..... de ..... de ..... de 200..., publicada no ..... de ..... de ..... de ....., portador da matrícula funcional nº .....,, considerando o julgamento da licitação na modalidade de pregão, na forma eletrônica, para REGISTRO DE PREÇOS nº ...../200..., publicada no ..... de ...../...../200....., processo administrativo n.º ....., RESOLVE registrar os preços da(s) empresa(s) indicada(s) e qualificada(s) nesta ATA, de acordo com a classificação por ela(s) alcançada(s) e na(s) quantidade(s) cotada(s), atendendo as condições previstas no edital, sujeitando-se as partes às normas constantes na Lei nº 8.666, de 21 de junho de 1993 e suas alterações, no Decreto n.º 7.892, de 23 de janeiro de 2013, e em conformidade com as disposições a seguir:

1. DO OBJETO

1.1. **A presente Ata tem por objeto o registro de preços para a eventual renovação da SOLUÇÃO ANTIVIRUS KASPERSKY ENDPOINT SECURITY FOR BUSINESS - ADVANCED pelo período de 36 (trinta e seis) meses, com serviços de instalação, suporte técnico, treinamento da equipe se necessário e garantia, especificado no item 2.1 do Termo de Referência, anexo I do edital de *Pregão* nº 18/2022, 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, a quantidade, fornecedor(es) e as demais condições ofertadas na(s) proposta(s) são as que seguem:

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

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

3. ÓRGÃO(S) GERENCIADOR

3.1. O órgão gerenciador será o **Instituto Federal de Educação, Ciência e Tecnologia de Brasília.**

3.2. (SUPRESSÃO)

4. DA ADESÃO À ATA DE REGISTRO DE PREÇOS

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

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 tornar-se 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 7892/13.

8.3. (SUPRESSÃO)

8.3.1. (SUPRESSÃO)

8.3.2. (SUPRESSÃO)

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, compõe anexo a esta Ata de Registro de Preços, nos termos do art. 11, §4º do Decreto n. 7.892, de 2014.

Para firmeza e validade do pactuado, a presente Ata foi lavrada em .... (....) vias de igual teor, que, depois de lida e achada em ordem, vai assinada pelas partes.

Local e data
Assinaturas

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