MINISTÉRIO DA AGRICULTURA E PECUÁRIA

EDITAL

MINISTÉRIO DA AGRICULTURA E PECUÁRIA
PREGÃO ELETRÔNICO Nº 16/2023

PROCESSO Nº 21000.020025/2023-02

CONTRATANTE (UASG): Ministério da Agricultura e Pecuária - Sede (130005).

OBJETO: Contratação de solução de proteção de rede com características de *Next Generation Firewall* (NGFW).

VALOR TOTAL DA CONTRATAÇÃO: R$ 11.536.760,44 (onze milhões, quinhentos e trinta e seis mil, setecentos e sessenta reais e quarenta e quatro centavos).

DATA DA SESSÃO PÚBLICA: 18/10/2023 às 9h (horário de Brasília).

CRITÉRIO DE JULGAMENTO: Menor preço do grupo.

MODO DE DISPUTA: Aberto.

PREFERÊNCIA ME/EPP/EQUIPARADAS: Sim.

Torna-se público que a **UNIÃO**, por meio do **MINISTÉRIO DA AGRICULTURA E PECUÁRIA (Coordenação-Geral de Aquisições)**, sediado na Esplanada dos Ministérios, Bloco D, Edifício Anexo - 2º andar - Ala B, Sala 207-B, Brasília - DF, CEP 70.043-900, realizará licitação, na modalidade PREGÃO, na forma ELETRÔNICA, nos termos da Lei nº 14.133, de 2021, e demais legislação aplicável e, ainda, de acordo com as condições estabelecidas neste Edital.

1. DO OBJETO

1.1. O objeto da presente licitação é a contratação de empresa para o fornecimento de solução de proteção de rede com características de *Next Generation Firewall* (NGFW), contemplando os hardwares com licenciamento, suporte e garantia, instalação e configuração, treinamento, plataforma de gestão, treinamento e Plataforma de ZTNA pelo período de dois anos, para atender a demanda do Ministério da Agricultura e Pecuária e órgãos demandantes (Ministério da Pesca e Aquicultura/Ministério do Desenvolvimento Agrário e Agricultura Familiar), conforme condições, quantidades e exigências estabelecidas neste Edital e seus anexos.

1.2. A licitação será realizada em grupo único, formados por 9 (nove) itens, conforme tabela constante no Termo de Referência, devendo o licitante oferecer proposta para todos os itens que o compõem.

2. DA PARTICIPAÇÃO NA LICITAÇÃO

2.1. Poderão participar deste Pregão os interessados que estiverem previamente credenciados no Sistema de Cadastramento Unificado de Fornecedores - SICAF e no Sistema de Compras do Governo Federal (www.gov.br/compras).

2.1.1. Os interessados deverão atender às condições exigidas no cadastramento no Sicaf até o terceiro dia útil anterior à data prevista para recebimento das propostas.

2.2. 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.

2.3. É de responsabilidade do cadastrado conferir a exatidão dos seus dados cadastrais nos Sistemas relacionados no item anterior 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.

2.4. A não observância do disposto no item anterior poderá ensejar desclassificação no momento da habilitação.

2.5. Será concedido tratamento favorecido para as microempresas e empresas de pequeno porte, para o microempreendedor individual - MEI, nos limites previstos da Lei Complementar nº 123, de 2006 e do Decreto nº 8.538, de

2015, bem como para bens e serviços produzidos com tecnologia produzida no país e bens produzidos de acordo com processo produtivo básico, na forma do art. 3° da Lei nº 8.248, de 1991 e art. 8° do Decreto n° 7.174, de 2010.

2.6. Não poderão disputar esta licitação:

2.6.1. aquele que não atenda às condições deste Edital e seu(s) anexo(s);

2.6.2. autor do anteprojeto, do projeto básico ou do projeto executivo, pessoa física ou jurídica, quando a licitação versar sobre serviços ou fornecimento de bens a ele relacionados;

2.6.3. empresa, isoladamente ou em consórcio, responsável pela elaboração do projeto básico ou do projeto executivo, ou empresa da qual o autor do projeto seja dirigente, gerente, controlador, acionista ou detentor de mais de 5% (cinco por cento) do capital com direito a voto, responsável técnico ou subcontratado, quando a licitação versar sobre serviços ou fornecimento de bens a ela necessários;

2.6.4. pessoa física ou jurídica que se encontre, ao tempo da licitação, impossibilitada de participar da licitação em decorrência de sanção que lhe foi imposta;

2.6.5. aquele que mantenha vínculo de natureza técnica, comercial, econômica, financeira, trabalhista ou civil com dirigente do órgão ou entidade contratante ou com agente público que desempenhe função na licitação ou atue na fiscalização ou na gestão do contrato, ou que deles seja cônjuge, companheiro ou parente em linha reta, colateral ou por afinidade, até o terceiro grau;

2.6.6. empresas controladoras, controladas ou coligadas, nos termos da Lei nº 6.404, de 15 de dezembro de 1976, concorrendo entre si;

2.6.7. pessoa física ou jurídica que, nos 5 (cinco) anos anteriores à divulgação do edital, tenha sido condenada judicialmente, com trânsito em julgado, por exploração de trabalho infantil, por submissão de trabalhadores a condições análogas às de escravo ou por contratação de adolescentes nos casos vedados pela legislação trabalhista;

2.6.8. agente público do órgão ou entidade licitante;

2.6.9. pessoas jurídicas reunidas em consórcio;

2.6.10. Organizações da Sociedade Civil de Interesse Público - OSCIP, atuando nessa condição;

2.6.11. Não poderá participar, direta ou indiretamente, da licitação ou da execução do contrato agente público do órgão ou entidade contratante, devendo ser observadas as situações que possam configurar conflito de interesses no exercício ou após o exercício do cargo ou emprego, nos termos da legislação que disciplina a matéria, conforme § 1º do art. 9º da Lei n.º 14.133, de 2021.

2.7. O impedimento de que trata o item 2.6.4 será também aplicado ao licitante que atue em substituição a outra pessoa, física ou jurídica, com o intuito de burlar a efetividade da sanção a ela aplicada, inclusive a sua controladora, controlada ou coligada, desde que devidamente comprovado o ilícito ou a utilização fraudulenta da personalidade jurídica do licitante.

2.8. A critério da Administração e exclusivamente a seu serviço, o autor dos projetos e a empresa a que se referem os itens 2.6.2 e 2.6.3 poderão participar no apoio das atividades de planejamento da contratação, de execução da licitação ou de gestão do contrato, desde que sob supervisão exclusiva de agentes públicos do órgão ou entidade.

2.9. Equiparam-se aos autores do projeto as empresas integrantes do mesmo grupo econômico.

2.10. O disposto nos itens 2.6.2 e 2.6.3 não impede a licitação ou a contratação de serviço que inclua como encargo do contratado a elaboração do projeto básico e do projeto executivo, nas contratações integradas, e do projeto executivo, nos demais regimes de execução.

2.11. Em licitações e contratações realizadas no âmbito de projetos e programas parcialmente financiados por agência oficial de cooperação estrangeira ou por organismo financeiro internacional com recursos do financiamento ou da contrapartida nacional, não poderá participar pessoa física ou jurídica que integre o rol de pessoas sancionadas por essas entidades ou que seja declarada inidônea nos termos da Lei nº 14.133/2021.

2.12. A vedação de que trata o item 2.6.8 estende-se a terceiro que auxilie a condução da contratação na qualidade de integrante de equipe de apoio, profissional especializado ou funcionário ou representante de empresa que preste assessoria técnica.

3. DA APRESENTAÇÃO DA PROPOSTA E DOS DOCUMENTOS DE HABILITAÇÃO

3.1. Na presente licitação, a fase de habilitação sucederá as fases de apresentação de propostas e lances e de julgamento.

3.2. Os licitantes encaminharão, exclusivamente por meio do sistema eletrônico, a proposta com o preço ou o percentual de desconto, conforme o critério de julgamento adotado neste Edital, até a data e o horário estabelecidos para abertura da sessão pública.

3.3. Caso a fase de habilitação anteceda as fases de apresentação de propostas e lances, os licitantes encaminharão, na forma e no prazo estabelecidos no item anterior, simultaneamente os documentos de habilitação e a proposta com o preço ou o percentual de desconto, observado o disposto nos itens 7.1.1 e 7.13.1 deste Edital.

3.4. No cadastramento da proposta inicial, o licitante declarará, em campo próprio do sistema, que:

3.4.1. está ciente e concorda com as condições contidas no edital e seus anexos, bem como de que a proposta apresentada compreende a integralidade dos custos para atendimento dos direitos trabalhistas assegurados na Constituição Federal, nas leis trabalhistas, nas normas infralegais, nas convenções coletivas de trabalho e nos termos de ajustamento de conduta vigentes na data de sua entrega em definitivo e que cumpre plenamente os requisitos de habilitação definidos no instrumento convocatório;

3.4.2. 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;

3.4.3. 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;

3.4.4. cumpre as exigências de reserva de cargos para pessoa com deficiência e para reabilitado da Previdência Social, previstas em lei e em outras normas específicas.

3.5. O fornecedor enquadrado como microempresa, empresa de pequeno porte deverá declarar, ainda, em campo próprio do sistema eletrônico, 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, observado o disposto nos §§ 1º ao 3º do art. 4º, da Lei n.º 14.133, de 2021.

3.5.1. no item exclusivo para participação de microempresas e empresas de pequeno porte, a assinalação do campo “não” impedirá o prosseguimento no certame, para aquele item;

3.5.2. 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.

3.6. A falsidade da declaração de que trata os itens 3.4 ou 3.6 sujeitará o licitante às sanções previstas na Lei nº 14.133, de 2021, e neste Edital.

3.7. Os licitantes poderão retirar ou substituir a proposta ou, na hipótese de a fase de habilitação anteceder as fases de apresentação de propostas e lances e de julgamento, os documentos de habilitação anteriormente inseridos no sistema, até a abertura da sessão pública.

3.8. Não haverá ordem de classificação na etapa de apresentação da proposta e dos documentos de habilitação pelo licitante, o que ocorrerá somente após os procedimentos de abertura da sessão pública e da fase de envio de lances.

3.9. Serão disponibilizados para acesso público os documentos que compõem a proposta dos licitantes convocados para apresentação de propostas, após a fase de envio de lances.

3.10. Desde que disponibilizada a funcionalidade no sistema, o licitante poderá parametrizar o seu valor final mínimo ou o seu percentual de desconto máximo quando do cadastramento da proposta e obedecerá às seguintes regras:

3.10.1. a aplicação do intervalo mínimo de diferença de valores ou de percentuais entre os lances, que incidirá tanto em relação aos lances intermediários quanto em relação ao lance que cobrir a melhor oferta; e

3.10.2. os lances serão de envio automático pelo sistema, respeitado o valor final mínimo estabelecido e o intervalo de que trata o subitem acima.

3.11. O valor final mínimo ou o percentual de desconto final máximo parametrizado no sistema poderá ser alterado pelo fornecedor durante a fase de disputa, sendo vedado:

3.11.1. valor superior a lance já registrado pelo fornecedor no sistema, quando adotado o critério de julgamento por menor preço; e

3.11.2. percentual de desconto inferior a lance já registrado pelo fornecedor no sistema, quando adotado o critério de julgamento por maior desconto.

3.12. O valor final mínimo ou o percentual de desconto final máximo parametrizado na forma do item 3.11 possuirá caráter sigiloso para os demais fornecedores e para o órgão ou entidade promotora da licitação, podendo ser disponibilizado estrita e permanentemente aos órgãos de controle externo e interno.

3.13. Caberá ao licitante interessado em participar da licitação acompanhar as operações no sistema eletrônico durante o processo licitatório e se responsabilizar pelo ônus decorrente da perda de negócios diante da inobservância de mensagens emitidas pela Administração ou de sua desconexão.

3.14. O licitante deverá comunicar imediatamente ao provedor do sistema qualquer acontecimento que possa comprometer o sigilo ou a segurança, para imediato bloqueio de acesso.

4. DO PREENCHIMENTO DA PROPOSTA

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

4.1.1. Valor total do grupo.

4.1.2. Marca;

4.1.3. Fabricante;

4.2. Todas as especificações do objeto contidas na proposta vinculam o licitante.

4.3. Nos valores propostos estarão inclusos todos os custos operacionais, encargos previdenciários, trabalhistas, tributários, comerciais e quaisquer outros que incidam direta ou indiretamente na execução do objeto.

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

4.5. Se o regime tributário da empresa implicar o recolhimento de tributos em percentuais variáveis, a cotação adequada será a que corresponde à média dos efetivos recolhimentos da empresa nos últimos doze meses.

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

4.7. Na presente licitação, a Microempresa e a Empresa de Pequeno Porte poderão se beneficiar do regime de tributação pelo Simples Nacional.

4.8. A apresentação das propostas implica obrigatoriedade do cumprimento das disposições nelas contidas, em conformidade com o que dispõe o Termo de Referência, assumindo o proponente o compromisso de executar o objeto licitado 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.

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

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

4.10.1. Caso o critério de julgamento seja o de maior desconto, o preço já decorrente da aplicação do desconto ofertado deverá respeitar os preços máximos previstos no item 3.8.

4.11. 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.

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

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

5.2. Os licitantes poderão retirar ou substituir a proposta ou os documentos de habilitação, quando for o caso, anteriormente inseridos no sistema, até a abertura da sessão pública.

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

5.4. 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.

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

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

5.7. O licitante somente poderá oferecer lance de valor inferior ao último por ele ofertado e registrado pelo sistema.

5.8. O intervalo mínimo de diferença de valores ou percentuais entre os lances, que incidirá tanto em relação aos lances intermediários quanto em relação à proposta que cobrir a melhor oferta deverá ser de R$ 1,00 (um real).

5.9. O licitante poderá, uma única vez, excluir seu último lance ofertado, no intervalo de quinze segundos após o registro no sistema, na hipótese de lance inconsistente ou inexequível.

5.10. O procedimento seguirá de acordo com o modo de disputa adotado.

5.11. Caso seja adotado para o envio de lances no pregão eletrônico o modo de disputa “aberto”, os licitantes apresentarão lances públicos e sucessivos, com prorrogações.

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

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

5.11.3. Não havendo novos lances na forma estabelecida nos itens anteriores, a sessão pública encerrar-se-á automaticamente, e o sistema ordenará e divulgará os lances conforme a ordem final de classificação.

5.11.4. Definida a melhor proposta, se a diferença em relação à proposta classificada em segundo lugar for de pelo menos 5% (cinco por cento), o pregoeiro, auxiliado pela equipe de apoio, poderá admitir o reinício da disputa aberta, para a definição das demais colocações.

5.11.5. Após o reinício previsto no item supra, os licitantes serão convocados para apresentar lances intermediários.

5.12. Caso seja adotado para o envio de lances no pregão eletrônico o modo de disputa “aberto e fechado”, os licitantes apresentarão lances públicos e sucessivos, com lance final e fechado.

5.12.1. 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.

5.12.2. Encerrado o prazo previsto no subitem anterior, o sistema abrirá oportunidade para que o autor da oferta de valor mais baixo e os das ofertas com preços até 10% (dez por cento) superiores àquela possam ofertar um lance final e fechado em até cinco minutos, o qual será sigiloso até o encerramento deste prazo.

5.12.3. No procedimento de que trata o subitem supra, o licitante poderá optar por manter o seu último lance da etapa aberta, ou por ofertar melhor lance.

5.12.4. 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 em até cinco minutos, o qual será sigiloso até o encerramento deste prazo.

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

5.13. Caso seja adotado para o envio de lances no pregão eletrônico o modo de disputa “fechado e aberto”, poderão participar da etapa aberta somente os licitantes que apresentarem a proposta de menor preço/ maior percentual de desconto e os das propostas até 10% (dez por cento) superiores/inferiores àquela, em que os licitantes apresentarão lances públicos e sucessivos, até o encerramento da sessão e eventuais prorrogações.

5.13.1. Não havendo pelo menos 3 (três) propostas nas condições definidas no item 5.13, poderão os licitantes que apresentaram as três melhores propostas, consideradas as empatadas, oferecer novos lances sucessivos.

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

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

5.13.4. Não havendo novos lances na forma estabelecida nos itens anteriores, a sessão pública encerrar-se-á automaticamente, e o sistema ordenará e divulgará os lances conforme a ordem final de classificação.

5.13.5. Definida a melhor proposta, se a diferença em relação à proposta classificada em segundo lugar for de pelo menos 5% (cinco por cento), o pregoeiro, auxiliado pela equipe de apoio, poderá admitir o reinício da disputa aberta, para a definição das demais colocações.

5.13.6. Após o reinício previsto no subitem supra, os licitantes serão convocados para apresentar lances intermediários.

5.14. Após o término dos prazos estabelecidos nos subitens anteriores, o sistema ordenará e divulgará os lances segundo a ordem crescente de valores.

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

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

5.17. 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.

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

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

5.20. 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 Lei Complementar nº 123, de 2006, regulamentada pelo Decreto nº 8.538, de 2015.

5.20.1. 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.

5.20.2. A melhor classificada nos termos do subitem 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.

5.20.3. 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.

5.20.4. 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.

5.21. 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:

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

5.21.1.1. 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;

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

5.21.1.3. 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.

5.21.2. Os licitantes classificados que estejam enquadrados no item 5.21.1.1, 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.

5.21.3. Caso a preferência não seja exercida na forma do item 5.21.1.1, por qualquer motivo, serão convocadas as empresas classificadas que estejam enquadradas no item 6.21.1.2, na ordem de classificação, para a comprovação e o exercício do direito de preferência, aplicando-se a mesma regra para o item 5.21.1.3 caso esse direito não seja exercido.

5.21.4. 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.

5.22. 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.

5.22.1. Havendo eventual empate entre propostas ou lances, o critério de desempate será aquele previsto no art. 60 da Lei nº 14.133, de 2021, nesta ordem:

5.22.1.1. disputa final, hipótese em que os licitantes empatados poderão apresentar nova proposta em ato contínuo à classificação;

5.22.1.2. avaliação do desempenho contratual prévio dos licitantes, para a qual deverão preferencialmente ser utilizados registros cadastrais para efeito de atesto de cumprimento de obrigações previstos nesta Lei;

5.22.1.3. desenvolvimento pelo licitante de ações de equidade entre homens e mulheres no ambiente de trabalho, conforme regulamento;

5.22.1.4. desenvolvimento pelo licitante de programa de integridade, conforme orientações dos órgãos de controle.

5.22.2. Persistindo o empate, será assegurada preferência, sucessivamente, aos bens e serviços produzidos ou prestados por:

5.22.2.1. empresas estabelecidas no território do Estado ou do Distrito Federal do órgão ou entidade da Administração Pública estadual ou distrital licitante ou, no caso de licitação realizada por órgão ou entidade de Município, no território do Estado em que este se localize;

5.22.2.2. empresas brasileiras;

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

5.22.2.4. empresas que comprovem a prática de mitigação, nos termos da Lei nº 12.187, de 29 de dezembro

de 2009.

5.23. Encerrada a etapa de envio de lances da sessão pública, na hipótese da proposta do primeiro colocado permanecer acima do preço máximo ou inferior ao desconto definido para a contratação, o pregoeiro poderá negociar condições mais vantajosas, após definido o resultado do julgamento.

5.23.1. A negociação poderá ser feita com os demais licitantes, segundo a ordem de classificação inicialmente estabelecida, quando o primeiro colocado, mesmo após a negociação, for desclassificado em razão de sua proposta permanecer acima do preço máximo definido pela Administração.

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

5.23.3. O resultado da negociação será divulgado a todos os licitantes e anexado aos autos do processo licitatório.

5.23.4. O pregoeiro solicitará ao licitante mais bem classificado que, no prazo de 2 (duas) horas, envie a proposta adequada ao último lance ofertado após a negociação realizada, acompanhada, se for o caso, dos documentos complementares, quando necessários à confirmação daqueles exigidos neste Edital e já apresentados.

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

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

6. DA FASE DE JULGAMENTO

6.1. Encerrada a etapa de negociação, o pregoeiro verificará se o licitante provisoriamente classificado em primeiro lugar atende às condições de participação no certame, conforme previsto no art. 14 da Lei nº 14.133/2021, legislação correlata e no item 2.6 do edital, especialmente quanto à existência de sanção que impeça a participação no certame ou a futura contratação, mediante a consulta aos seguintes cadastros:

6.1.1. SICAF;

6.1.2. Cadastro Nacional de Empresas Inidôneas e Suspensas - CEIS, mantido pela Controladoria-Geral da União (https://www.portaltransparencia.gov.br/sancoes/ceis); e

6.1.3. Cadastro Nacional de Empresas Punidas – CNEP, mantido pela Controladoria-Geral da União (https://www.portaltransparencia.gov.br/sancoes/cnep).

6.2. A consulta aos cadastros será realizada em nome da empresa licitante e também de seu sócio majoritário, por força da vedação de que trata o artigo 12 da Lei n° 8.429, de 1992.

6.3. Caso conste na Consulta de Situação do licitante a existência de Ocorrências Impeditivas Indiretas, o Pregoeiro diligenciará para verificar se houve fraude por parte das empresas apontadas no Relatório de Ocorrências Impeditivas Indiretas. (IN nº 3/2018, art. 29, caput)

6.3.1. A tentativa de burla será verificada por meio dos vínculos societários, linhas de fornecimento similares, dentre outros. (IN nº 3/2018, art. 29, §1º).

6.3.2. O licitante será convocado para manifestação previamente a uma eventual desclassificação. (IN nº 3/2018, art. 29, §2º).

6.3.3. Constatada a existência de sanção, o licitante será reputado inabilitado, por falta de condição de participação.

6.4. Caso atendidas as condições de participação, será iniciado o procedimento de habilitação.

6.5. Caso o licitante provisoriamente classificado em primeiro lugar tenha se utilizado de algum tratamento favorecido às ME/EPPs, o pregoeiro verificará se faz jus ao benefício, em conformidade com o item 3.5 deste edital.

6.6. Verificadas as condições de participação e de utilização do tratamento favorecido, o pregoeiro examinará a proposta classificada em primeiro lugar quanto à adequação ao objeto e à compatibilidade do preço em relação ao máximo estipulado para contratação neste Edital e em seus anexos, observado o disposto no artigo 29 a 35 da IN SEGES nº 73, de 30 de setembro de 2022.

6.7. Será desclassificada a proposta vencedora que:

6.7.1. contiver vícios insanáveis;

6.7.2. não obedecer às especificações técnicas contidas no Termo de Referência;

6.7.3. apresentar preços inexequíveis ou permanecerem acima do valor estimado (unitários e total) definido para a contratação;

6.7.4. não tiverem sua exequibilidade demonstrada, quando exigido pela Administração;

6.7.5. apresentar desconformidade com quaisquer outras exigências deste Edital ou seus anexos, desde que insanável.

6.8. No caso de bens e serviços em geral, é indício de inexequibilidade das propostas valores inferiores a 50% (cinquenta por cento) do valor orçado pela Administração.

6.8.1. A inexequibilidade, na hipótese de que trata o caput, só será considerada após diligência do pregoeiro, que comprove:

6.8.1.1. que o custo do licitante ultrapassa o valor da proposta; e

6.8.1.2. inexistirem custos de oportunidade capazes de justificar o vulto da oferta.

6.9. Em contratação de serviços de engenharia, além das disposições acima, a análise de exequibilidade e sobrepreço considerará o seguinte:

6.9.1. Nos regimes de execução por tarefa, empreitada por preço global ou empreitada integral, semi-integrada ou integrada, a caracterização do sobrepreço se dará pela superação do valor global estimado;

6.9.2. No regime de empreitada por preço unitário, a caracterização do sobrepreço se dará pela superação do valor global estimado e pela superação de custo unitário tido como relevante, conforme planilha anexa ao edital;

6.9.3. No caso de serviços de engenharia, serão consideradas inexequíveis as propostas cujos valores forem inferiores a 75% (setenta e cinco por cento) do valor orçado pela Administração, independentemente do regime de execução.

6.9.4. Será exigida garantia adicional do licitante vencedor cuja proposta for inferior a 85% (oitenta e cinco por cento) do valor orçado pela Administração, equivalente à diferença entre este último e o valor da proposta, sem prejuízo das demais garantias exigíveis de acordo com a Lei.

6.10. Se houver indícios de inexequibilidade da proposta de preço, ou em caso da necessidade de esclarecimentos complementares, poderão ser efetuadas diligências, para que a empresa comprove a exequibilidade da proposta.

6.11. Caso o custo global estimado do objeto licitado tenha sido decomposto em seus respectivos custos unitários por meio de Planilha de Custos e Formação de Preços elaborada pela Administração, o licitante classificado em primeiro lugar será convocado para apresentar Planilha por ele elaborada, com os respectivos valores adequados ao valor final da sua proposta, sob pena de não aceitação da proposta.

6.11.1. Em se tratando de serviços de engenharia, o licitante vencedor será convocado a apresentar à Administração, por meio eletrônico, as planilhas com indicação dos quantitativos e dos custos unitários, seguindo o modelo elaborado pela Administração, bem como com detalhamento das Bonificações e Despesas Indiretas (BDI) e dos Encargos Sociais (ES), com os respectivos valores adequados ao valor final da proposta vencedora, admitida a utilização dos preços unitários, no caso de empreitada por preço global, empreitada integral, contratação semi-integrada e contratação integrada, exclusivamente para eventuais adequações indispensáveis no cronograma físico-financeiro e para balizar excepcional aditamento posterior do contrato.

6.11.2. Em se tratando de serviços com fornecimento de mão de obra em regime de dedicação exclusiva cuja produtividade seja mensurável e indicada pela Administração, o licitante deverá indicar a produtividade adotada e a quantidade de pessoal que será alocado na execução contratual.

6.11.3. Caso a produtividade for diferente daquela utilizada pela Administração como referência, ou não estiver contida na faixa referencial de produtividade, mas admitida pelo ato convocatório, o licitante deverá apresentar a respectiva comprovação de exequibilidade;

6.11.4. Os licitantes poderão apresentar produtividades diferenciadas daquela estabelecida pela Administração como referência, desde que não alterem o objeto da contratação, não contrariem dispositivos legais vigentes e, caso não estejam contidas nas faixas referenciais de produtividade, comprovem a exequibilidade da proposta.

6.11.5. Para efeito do subitem anterior, admite-se a adequação técnica da metodologia empregada pela contratada, visando assegurar a execução do objeto, desde que mantidas as condições para a justa remuneração do serviço.

6.12. Erros no preenchimento da planilha não constituem motivo para a desclassificação da proposta. A planilha poderá ser ajustada pelo fornecedor, no prazo indicado pelo sistema, desde que não haja majoração do preço e que se comprove que este é o bastante para arcar com todos os custos da contratação.

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

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

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

6.16. Caso o Termo de Referência exija a apresentação de amostra, o licitante classificado em primeiro lugar deverá apresentá-la, conforme disciplinado no Termo de Referência, sob pena de não aceitação da proposta.

6.17. Por meio de mensagem no sistema, será divulgado o local e horário de realização do procedimento para a avaliação das amostras, cuja presença será facultada a todos os interessados, incluindo os demais licitantes.

6.18. Os resultados das avaliações serão divulgados por meio de mensagem no sistema.

6.19. No caso de não haver entrega da amostra ou ocorrer atraso na entrega, sem justificativa aceita pelo Pregoeiro, ou havendo entrega de amostra fora das especificações previstas neste Edital, a proposta do licitante será recusada.

6.20. Se a(s) amostra(s) apresentada(s) pelo primeiro classificado não for(em) aceita(s), o Pregoeiro analisará a aceitabilidade da proposta ou lance ofertado pelo segundo classificado. Seguir-se-á com a verificação da(s) amostra(s) e, assim, sucessivamente, até a verificação de uma que atenda às especificações constantes no Termo de Referência.

7. DA FASE DE HABILITAÇÃO

7.1. Os documentos previstos no Termo de Referência, necessários e suficientes para demonstrar a capacidade do licitante de realizar o objeto da licitação, serão exigidos para fins de habilitação, nos termos dos arts. 62 a 70 da Lei nº 14.133, de 2021.

7.1.1. A documentação exigida para fins de habilitação jurídica, fiscal, social e trabalhista e econômico-financeira, poderá ser substituída pelo registro cadastral no SICAF.

7.2. Quando permitida a participação de empresas estrangeiras que não funcionem no País, as exigências de habilitação serão atendidas mediante documentos equivalentes, inicialmente apresentados em tradução livre.

7.3. Na hipótese de o licitante vencedor ser empresa estrangeira que não funcione no País, para fins de assinatura do contrato ou da ata de registro de preços, os documentos exigidos para a habilitação serão traduzidos por tradutor juramentado no País e apostilados nos termos do disposto no Decreto nº 8.660, de 29 de janeiro de 2016, ou de outro que venha a substituí-lo, ou consularizados pelos respectivos consulados ou embaixadas.

7.4. Quando permitida a participação de consórcio de empresas, a habilitação técnica, quando exigida, será feita por meio do somatório dos quantitativos de cada consorciado e, para efeito de habilitação econômico-financeira, quando exigida, será observado o somatório dos valores de cada consorciado.

7.4.1. Se o consórcio não for formado integralmente por microempresas ou empresas de pequeno porte e o termo de referência exigir requisitos de habilitação econômico-financeira, haverá um acréscimo de 10% (dez por cento) para o consórcio em relação ao valor exigido para os licitantes individuais.

7.5. Os documentos exigidos para fins de habilitação poderão ser apresentados em original, por cópia ou por versão digitalizada.

7.6. Os documentos exigidos para fins de habilitação poderão ser substituídos por registro cadastral emitido por órgão ou entidade pública, desde que o registro tenha sido feito em obediência ao disposto na Lei nº 14.133/2021.

7.7. Será verificado se o licitante apresentou declaração de que atende aos requisitos de habilitação, e o declarante responderá pela veracidade das informações prestadas, na forma da lei (art. 63, I, da Lei nº 14.133/2021).

7.8. Será verificado se o licitante apresentou no sistema, sob pena de inabilitação, a declaração de que cumpre as exigências de reserva de cargos para pessoa com deficiência e para reabilitado da Previdência Social, previstas em lei e em outras normas específicas.

7.9. O licitante deverá apresentar, sob pena de desclassificação, declaração de que suas propostas econômicas compreendem a integralidade dos custos para atendimento dos direitos trabalhistas assegurados na Constituição Federal, nas leis trabalhistas, nas normas infralegais, nas convenções coletivas de trabalho e nos termos de ajustamento de conduta vigentes na data de entrega das propostas.

7.10. Considerando que na presente contratação a avaliação prévia do local de execução é imprescindível para o conhecimento pleno das condições e peculiaridades do objeto a ser contratado, o licitante deve atestar, sob pena de inabilitação, que conhece o local e as condições de realização do serviço, assegurado a ele o direito de realização de vistoria prévia.

7.10.1. O licitante que optar por realizar vistoria prévia terá disponibilizado pela Administração data e horário exclusivos, a ser agendado conforme subitem 4.12 do Termo de Referência, Anexo I deste Edital, de modo que seu agendamento não coincida com o agendamento de outros licitantes.

7.10.2. Caso o licitante opte por não realizar vistoria, poderá substituir a declaração exigida no presente item por declaração formal assinada pelo seu responsável técnico acerca do conhecimento pleno das condições e peculiaridades da contratação.

7.11. A habilitação será verificada por meio do Sicaf, nos documentos por ele abrangidos.

7.11.1. Somente haverá a necessidade de comprovação do preenchimento de requisitos mediante apresentação dos documentos originais não-digitais quando houver dúvida em relação à integridade do documento digital ou quando a lei expressamente o exigir. (IN nº 3/2018, art. 4º, §1º, e art. 6º, §4º).

7.12. É de responsabilidade do licitante 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. (IN nº 3/2018, art. 7º, *caput*).

7.12.1. A não observância do disposto no item anterior poderá ensejar desclassificação no momento da habilitação. (IN nº 3/2018, art. 7º, parágrafo único).

7.13. A verificação pelo pregoeiro, em sítios eletrônicos oficiais de órgãos e entidades emissores de certidões

constitui meio legal de prova, para fins de habilitação.

7.13.1. Os documentos exigidos para habilitação que não estejam contemplados no Sicaf serão enviados por meio do sistema, em formato digital, no prazo de 2 (duas) horas, prorrogável por igual período, contado da solicitação do pregoeiro.

7.13.2. Na hipótese de a fase de habilitação anteceder a fase de apresentação de propostas e lances, os licitantes encaminharão, por meio do sistema, simultaneamente os documentos de habilitação e a proposta com o preço ou o percentual de desconto, observado o disposto no § 1º do art. 36 e no § 1º do art. 39 da Instrução Normativa SEGES nº 73, de 30 de setembro de 2022.

7.14. A verificação no Sicaf ou a exigência dos documentos nele não contidos somente será feita em relação ao licitante vencedor.

7.14.1. Os documentos relativos à regularidade fiscal que constem do Termo de Referência somente serão exigidos, em qualquer caso, em momento posterior ao julgamento das propostas, e apenas do licitante mais bem classificado.

7.14.2. Respeitada a exceção do subitem anterior, relativa à regularidade fiscal, quando a fase de habilitação anteceder as fases de apresentação de propostas e lances e de julgamento, a verificação ou exigência do presente subitem ocorrerá em relação a todos os licitantes.

7.15. Após a entrega dos documentos para habilitação, não será permitida a substituição ou a apresentação de novos documentos, salvo em sede de diligência, para (Lei 14.133/21, art. 64, e IN 73/2022, art. 39, §4º):

7.15.1. complementação de informações acerca dos documentos já apresentados pelos licitantes e desde que necessária para apurar fatos existentes à época da abertura do certame; e

7.15.2. atualização de documentos cuja validade tenha expirado após a data de recebimento das propostas;

7.16. Na análise dos documentos de habilitação, a comissão de contratação poderá sanar erros ou falhas, que não alterem a substância dos documentos e sua validade jurídica, mediante decisão fundamentada, registrada em ata e acessível a todos, atribuindo-lhes eficácia para fins de habilitação e classificação.

7.17. Na hipótese de o licitante não atender às exigências para habilitação, o pregoeiro examinará a proposta subsequente e assim sucessivamente, na ordem de classificação, até a apuração de uma proposta que atenda ao presente edital, observado o prazo disposto no subitem 7.13.1.

7.18. Somente serão disponibilizados para acesso público os documentos de habilitação do licitante cuja proposta atenda ao edital de licitação, após concluídos os procedimentos de que trata o subitem anterior.

7.19. A comprovação de regularidade fiscal e trabalhista das microempresas e das empresas de pequeno porte somente será exigida para efeito de contratação, e não como condição para participação na licitação (art. 4º do Decreto nº 8.538/2015).

7.20. Quando a fase de habilitação anteceder a de julgamento e já tiver sido encerrada, não caberá exclusão de licitante por motivo relacionado à habilitação, salvo em razão de fatos supervenientes ou só conhecidos após o julgamento.

8. DOS RECURSOS

8.1. A interposição de recurso referente ao julgamento das propostas, à habilitação ou inabilitação de licitantes, à anulação ou revogação da licitação, observará o disposto no art. 165 da Lei nº 14.133, de 2021.

8.2. O prazo recursal é de 3 (três) dias úteis, contados da data de intimação ou de lavratura da ata.

8.3. Quando o recurso apresentado impugnar o julgamento das propostas ou o ato de habilitação ou inabilitação do licitante:

8.3.1. a intenção de recorrer deverá ser manifestada imediatamente, sob pena de preclusão;

8.3.1.1. o prazo para a manifestação da intenção de recorrer não será inferior a 10 (dez) minutos.

8.3.2. o prazo para apresentação das razões recursais será iniciado na data de intimação ou de lavratura da ata de habilitação ou inabilitação;

8.3.3. na hipótese de adoção da inversão de fases prevista no § 1º do art. 17 da Lei nº 14.133, de 2021, o prazo para apresentação das razões recursais será iniciado na data de intimação da ata de julgamento.

8.4. Os recursos deverão ser encaminhados em campo próprio do sistema.

8.5. O recurso será dirigido à autoridade que tiver editado o ato ou proferido a decisão recorrida, a qual poderá reconsiderar sua decisão no prazo de 3 (três) dias úteis, ou, nesse mesmo prazo, encaminhar recurso para a autoridade superior, a qual deverá proferir sua decisão no prazo de 10 (dez) dias úteis, contado do recebimento dos autos.

8.6. Os recursos interpostos fora do prazo não serão conhecidos.

8.7. O prazo para apresentação de contrarrazões ao recurso pelos demais licitantes será de 3 (três) dias úteis, contados da data da intimação pessoal ou da divulgação da interposição do recurso, assegurada a vista imediata dos elementos indispensáveis à defesa de seus interesses.

8.8. O recurso e o pedido de reconsideração terão efeito suspensivo do ato ou da decisão recorrida até que sobrevenha decisão final da autoridade competente.

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

8.10. Os autos do processo permanecerão com vista franqueada aos interessados, cujas instruções para acesso podem ser obtidas por e-mail endereçado à **licitacao@agro.gov.br**.

9. DAS INFRAÇÕES ADMINISTRATIVAS E SANÇÕES

9.1. Comete infração administrativa, nos termos da lei, o licitante que, com dolo ou culpa:

9.1.1. deixar de entregar a documentação exigida para o certame ou não entregar qualquer documento que tenha sido solicitado pelo/a pregoeiro/a durante o certame;

9.1.2. Salvo em decorrência de fato superveniente devidamente justificado, não mantiver a proposta em especial quando:

9.1.2.1. não enviar a proposta adequada ao último lance ofertado ou após a negociação;

9.1.2.2. recusar-se a enviar o detalhamento da proposta quando exigível;

9.1.2.3. pedir para ser desclassificado quando encerrada a etapa competitiva; ou

9.1.2.4. deixar de apresentar amostra;

9.1.2.5. apresentar proposta ou amostra em desacordo com as especificações do edital;

9.1.3. não celebrar o contrato ou não entregar a documentação exigida para a contratação, quando convocado dentro do prazo de validade de sua proposta;

9.1.3.1. recusar-se, sem justificativa, a assinar o contrato ou a ata de registro de preço, ou a aceitar ou retirar o instrumento equivalente no prazo estabelecido pela Administração;

9.1.4. apresentar declaração ou documentação falsa exigida para o certame ou prestar declaração falsa durante a licitação

9.1.5. fraudar a licitação

9.1.6. comportar-se de modo inidôneo ou cometer fraude de qualquer natureza, em especial quando:

9.1.6.1. agir em conluio ou em desconformidade com a lei;

9.1.6.2. induzir deliberadamente a erro no julgamento;

9.1.6.3. apresentar amostra falsificada ou deteriorada;

9.1.7. praticar atos ilícitos com vistas a frustrar os objetivos da licitação

9.1.8. praticar ato lesivo previsto no art. 5º da Lei n.º 12.846, de 2013.

9.2. Com fulcro na Lei nº 14.133, de 2021, a Administração poderá, garantida a prévia defesa, aplicar aos licitantes e/ou adjudicatários as seguintes sanções, sem prejuízo das responsabilidades civil e criminal:

9.2.1. advertência;

9.2.2. multa;

9.2.3. impedimento de licitar e contratar e

9.2.4. declaração de inidoneidade para licitar ou contratar, enquanto perdurarem os motivos determinantes da punição ou até que seja promovida sua reabilitação perante a própria autoridade que aplicou a penalidade.

9.3. Na aplicação das sanções serão considerados:

9.3.1. a natureza e a gravidade da infração cometida.

9.3.2. as peculiaridades do caso concreto

9.3.3. as circunstâncias agravantes ou atenuantes

9.3.4. os danos que dela provierem para a Administração Pública

9.3.5. a implantação ou o aperfeiçoamento de programa de integridade, conforme normas e orientações dos órgãos de controle.

9.4. A multa será recolhida em percentual de 0,5% a 30% incidente sobre o valor do contrato licitado, recolhida no prazo máximo de **10 (dez) dias** úteis, a contar da comunicação oficial.

9.4.1. Para as infrações previstas nos itens 9.1.1, 9.1.2 e 9.1.3, a multa será de 0,5% a 15% do valor do contrato licitado.

9.4.2. Para as infrações previstas nos itens 9.1.4, 9.1.5, 9.1.6, 9.1.7 e 9.1.8, a multa será de 15% a 30% do valor do contrato licitado.

9.5. As sanções de advertência, impedimento de licitar e contratar e declaração de inidoneidade para licitar ou contratar poderão ser aplicadas, cumulativamente ou não, à penalidade de multa.

9.6. Na aplicação da sanção de multa será facultada a defesa do interessado no prazo de 15 (quinze) dias úteis, contado da data de sua intimação.

9.7. A sanção de impedimento de licitar e contratar será aplicada ao responsável em decorrência das infrações administrativas relacionadas nos itens 9.1.1, 9.1.2 e 9.1.3, quando não se justificar a imposição de penalidade mais grave, e impedirá o responsável de licitar e contratar no âmbito da Administração Pública direta e indireta do ente federativo a qual pertencer o órgão ou entidade, pelo prazo máximo de 3 (três) anos.

9.8. Poderá ser aplicada ao responsável a sanção de declaração de inidoneidade para licitar ou contratar, em decorrência da prática das infrações dispostas nos itens 9.1.4, 9.1.5, 9.1.6, 9.1.7 e 9.1.8, bem como pelas infrações administrativas previstas nos itens 9.1.1, 9.1.2 e 9.1.3 que justifiquem a imposição de penalidade mais grave que a sanção de impedimento de licitar e contratar, cuja duração observará o prazo previsto no art. 156, §5º, da Lei n.º 14.133/2021.

9.9. A recusa injustificada do adjudicatário em assinar o contrato ou a ata de registro de preço, ou em aceitar ou retirar o instrumento equivalente no prazo estabelecido pela Administração, descrita no item 9.1.3, caracterizará o descumprimento total da obrigação assumida e o sujeitará às penalidades e à imediata perda da garantia de proposta em favor do órgão ou entidade promotora da licitação, nos termos do art. 45, §4º da IN SEGES/ME n.º 73, de 2022.

9.10. A apuração de responsabilidade relacionadas às sanções de impedimento de licitar e contratar e de declaração de inidoneidade para licitar ou contratar demandará a instauração de processo de responsabilização a ser conduzido por comissão composta por 2 (dois) ou mais servidores estáveis, que avaliará fatos e circunstâncias conhecidos e intimará o licitante ou o adjudicatário para, no prazo de 15 (quinze) dias úteis, contado da data de sua intimação, apresentar defesa escrita e especificar as provas que pretenda produzir.

9.11. Caberá recurso no prazo de 15 (quinze) dias úteis da aplicação das sanções de advertência, multa e impedimento de licitar e contratar, contado da data da intimação, o qual será dirigido à autoridade que tiver proferido a decisão recorrida, que, se não a reconsiderar no prazo de 5 (cinco) dias úteis, encaminhará o recurso com sua motivação à autoridade superior, que deverá proferir sua decisão no prazo máximo de 20 (vinte) dias úteis, contado do recebimento dos autos.

9.12. Caberá a apresentação de pedido de reconsideração da aplicação da sanção de declaração de inidoneidade para licitar ou contratar no prazo de 15 (quinze) dias úteis, contado da data da intimação, e decidido no prazo máximo de 20 (vinte) dias úteis, contado do seu recebimento.

9.13. O recurso e o pedido de reconsideração terão efeito suspensivo do ato ou da decisão recorrida até que sobrevenha decisão final da autoridade competente.

9.14. A aplicação das sanções previstas neste edital não exclui, em hipótese alguma, a obrigação de reparação integral dos danos causados.

10. DA IMPUGNAÇÃO AO EDITAL E DO PEDIDO DE ESCLARECIMENTO

10.1. Qualquer pessoa é parte legítima para impugnar este Edital por irregularidade na aplicação da Lei nº 14.133, de 2021, devendo protocolar o pedido até 3 (três) dias úteis antes da data da abertura do certame.

10.2. A resposta à impugnação ou ao pedido de esclarecimento será divulgado em sítio eletrônico oficial no prazo de até 3 (três) dias úteis, limitado ao último dia útil anterior à data da abertura do certame.

10.3. A impugnação e o pedido de esclarecimento poderão ser realizados por forma eletrônica mediante e-mail endereçado à **licitacao@agro.gov.br**.

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

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

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

11. DAS DISPOSIÇÕES GERAIS

11.1. Será divulgada ata da sessão pública no sistema eletrônico.

11.2. 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.

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

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

11.5. 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.

11.6. 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.

11.7. 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.

11.8. 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.

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

11.10. O Edital e seus anexos estão disponíveis, na íntegra, no Portal Nacional de Contratações Públicas (PNCP) e endereço eletrônico: **https://www.gov.br/agricultura/pt-br/acesso-a-informacao/licitacoes-e-contratos/edital/mapa-sede-uasg-130005**.

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

11.11.1. Anexo I do Edital - Termo de Referência

11.11.1.1. Anexo I do Termo de Referência - Ordem de Serviço ou de Fornecimento de Bens

11.11.1.2. Anexo II do Termo de Referência - Modelo de Termo de Ciência

11.11.1.3. Anexo III do Termo de Referência - Modelo de Termo de Recebimento Provisório - Compras de TIC

11.11.1.4. Anexo IV do Termo de Referência - Modelo de Termo de Recebimento Definitivo

11.11.1.5. Anexo V do Termo de Referência - Modelo de Declaração de Realização da Vistoria Técnica ou Opção por Não Realização

11.11.1.6. Anexo VI do Termo de Referência - Modelo de Termo de Compromisso de Manutenção de Sigilo

11.11.1.7. Anexo VII do Termo de Referência - Especificação Técnica da Solução de TI

11.11.1.8. Apêndice do Anexo I do Edital - Estudo Técnico Preliminar

11.11.2. Anexo II do Edital - Minuta de Termo de Contrato

11.11.3. Anexo III do Edital - Modelo de Proposta de Preços

Brasília, 29 de setembro de 2023.

LUCAS BEZERRA CAMPOS
Agente Administrativo
Coordenação-Geral de Aquisições

Documento assinado eletronicamente por **LUCAS BEZERRA CAMPOS**, **Agente Administrativo**, em 29/09/2023, às 15:50, conforme horário oficial de Brasília, com fundamento no art. 4º,§ 3º, do Decreto nº 10.543, de 13 de novembro de 2020.

A autenticidade deste documento pode ser conferida no site: https://sei.agro.gov.br/sei/controlador_externo.php?acao=documento_conferir&id_orgao_acesso_externo=0 , informando o código verificador **31297856** e o código CRC **D6119E72**.

Termo de Referência 14/2023

Informações Básicas

Número do TR	UASG	Editado por	Atualizado em
14/2023	130005-COORD.-GERAL DE EXECUCAO ORç.E FIN. /DA/MAPA	THIAGO PEREIRA DA COSTA	29/09/2023 14:53 (v 25.0)

Status

CONCLUIDO

Outras informações

Categoria	Número da Contratação	Processo Administrativo
VII - contratações de tecnologia da informação e de comunicação.	203/2022	21000.020025/2023-02

1. CONDIÇÕES GERAIS DA CONTRATAÇÃO

1.1 . OBJETO E CONDIÇÕES GERAIS DA CONTRATAÇÃO

ITEM	ESPECIFICAÇÃO	CATSER	UNIDADE DE MEDIDA	QTDE	VALOR UNITÁRIO	VALOR TOTAL
1	Appliances físicos - Firewall - Solução de plataforma de segurança, denominada Next Generation Firewall (NGFW), com licenciamento incluso.	481646	UNIDADE	01	R$ 1.462.696,00	R$ 1.462.696,00
2	Suporte, garantia e manutenção do item 01.	27740	SERVIÇO	01	R$ 1.502.986,12	R$ 1.502.986,12
3	Appliances físicos - Firewall - Solução de plataforma de segurança, denominada Next Generation Firewall (NGFW).	481646	UNIDADE	03	R$ 559.120,00	R$ 1.677.360,00
4	Suporte, garantia e manutenção do item 03.	27740	SERVIÇO	01	R$ 2.106.985,12	R$ 2.106.985,12
5	Serviço de instalação e configuração dos firewalls NGFW dos itens 01 e 03.	26972	SERVIÇO	01	R$ 223.237,16	R$ 223.237,26
6	Appliance - Plataforma de gestão e monitoramento centralizado, com licenciamento, instalação e configuração.	481646 /481647	UNIDADE	01	R$ 118.072,29	R$ 118.072,29
7	Suporte, garantia e Manutenção do item 06.	27740	SERVIÇO	01	R$ 52.986,32	R$ 52.986,32
8	Treinamento ministrado por profissional certificado pelo fabricante.	16837/20052	CAPACITAÇÃO	01	R$ 62.896,12	R$ 62.896,12
9	Plataforma de ZTNA - Zero Trust Network Access.	27742	SERVIÇO	01	R$ 216.896.21	R$ 216.896.21
O objeto desta contratação **não** faz parte dos catálogos de soluções de TIC aos quais possuem condições padrões definidas pelo Órgão Central do SISP conforme destacado no link " https://www.gov.br/governodigital/pt-br/contratacoes/catalogo-de-solucoes-de-tic". Por isso, não é necessário preenchimento da coluna "cód. PMC-TIC" do modelo de TR da AGU.						

1.1.1 - Contratação de empresa para o fornecimento de solução de proteção de rede com características de Next Generation Firewall (NGFW), contemplando os hardwares com licenciamento, suporte e garantia, instalação e configuração, treinamento, plataforma de gestão, treinamento e Plataforma de ZTNA pelo período de 02 anos, para atender a demanda do Ministério da Agricultura e Pecuária e órgãos demandantes (Ministério da Pesca e Aquicultura / Ministério do Desenvolvimento Agrário e Agricultura Familiar), de acordo com as condições, exigências, especificações e quantidades constantes deste termo de referência e seus Anexos.

1.1.2 - Todos os bens e serviços desta contratação são caracterizados como comuns, pois possuem padrões de desempenho e qualidade objetivamente definidos pelo edital, por meio de especificações usuais no mercado. Além disso, o objeto desta contratação não se enquadra como sendo de bem de luxo, conforme Decreto Nº 10.818, de 27 de Setembro de 2021.

1.1.3 - O objeto da presente contratação não incide na hipótese do inciso II do artigo 3º da IN SGD/ME nº 94, de 23 de dezembro de 2022. Adicionalmente, o objeto desta contratação também **não** faz parte dos catálogos de soluções de TIC aos quais possuem condições padrões definidas pelo Órgão Central do SISP conforme destacado no link " https://www.gov.br/governodigital/pt-br /contratacoes/catalogo-de-solucoes-de-tic".

1.1.4. - O prazo de vigência contratual será de 02 anos, contados a partir da data de assinatura do contrato, prorrogável para até 05 anos, na forma dos artigos 106 e 107 da Lei N° 14.133, de 2021. O fornecimento de bens e serviços desta contratação em questão é enquadrado como continuado tendo em vista que são serviços de infraestrutura de segurança da informação essenciais para o funcionamento do órgão sem causar prejuízo à Administração Pública e cidadãos, sendo a vigência mais vantajosa considerando as propostas recebidas dos fornecedores e detalhados no mapa comparativo de preços SEI Nº .

1.1.5 - O contrato oferecerá maior detalhamento das regras que serão aplicadas em relação à vigência da contratação.

2. DESCRIÇÃO DA SOLUÇÃO COMO UM TODO

2.1 . DESCRIÇÃO DA SOLUÇÃO DE TIC

2.1.1. - Tratase de aquisição de solução de proteção de rede Next Generation Firewall (NGFW), em alta disponibilidade, contemplando os hardwares com licenciamento, suporte e garantia, instalação e configuração, treinamento, plataforma de gestão, treinamento e Plataforma de ZTNA pelo período de 02 anos, prorrogáveis até 05 anos, conforme descrição detalhada ao longo do termo de referência e anexos.

2.1.2. - A solução proposta consiste em um conjunto de equipamentos e funcionalidades para proteger a rede e as aplicações do MAPA e órgãos demandantes contra ameaças cibernéticas. Essa solução oferece inspeção e filtro de tráfego interno e externo, controle de aplicação, proteção contra ameaças avançadas, IPS, proteção de DNS, ZTNA,VPN, proteção Anti-DDos na camada de aplicação, entre outras funcionalidades que visam mitigar riscos de ataques e exploração de vulnerabilidades do ambiente de TI dos órgãos.

2.1.3. - A solução deverá ser constituída pelos equipamentos relacionados nos itens, sendo todos do mesmo fabricante, garantindo a entrega e execução dos serviços por uma única empresa e a total compatibilidade entre eles.

2.1.4. - A escolha do agrupamento dos itens em um único grupo visa a plena qualificação da empresa fornecedora que prestará os serviços de instalação e configuração, bem como prestará os serviços de garantia dos equipamentos, a total compatibilidade entre os mesmos, a redução de custos operacionais, a capacidade técnica de manter a solução em operação, os recursos humanos disponíveis para prestarem o devido apoio, treinamento e curva de aprendizagem e o custo total de propriedade.

2.1.5. - A descrição da solução como um todo encontrasse pormenorizada neste termo de referência, não sendo necessário, até mesmo pelo objeto da contratação, fazer a inclusão do estudo técnico preliminar, como anexo, neste termo.

2.2 . BENS E SERVIÇOS QUE COMPOEM A SOLUÇÃO DE TIC

GRUPO	ITEM	ESPECIFICAÇÃO	CÓDIGO CATSER /CATMAT	UNIDADE DE MEDIDA	QTDE
ÚNICO	**1**	Appliances físicos - Firewall - Solução de plataforma de segurança, denominada Next Generation Firewall (NGFW), com licenciamento incluso.	481646	UNIDADE	01
	2	Suporte, garantia e manutenção do item 01.	27740	SERVIÇO	01
	3	Appliances físicos - Firewall - Solução de plataforma de segurança, denominada Next Generation Firewall (NGFW).	481646	UNIDADE	03
	4	Suporte, garantia e manutenção do item 03.	27740	SERVIÇO	01
	5	Serviço de instalação e configuração dos firewalls NGFW dos itens 01 e 03.	26972	SERVIÇO	01
		Appliance - Plataforma de gestão e monitoramento centralizado,			

	6	com licenciamento, instalação e configuração.	481646/481647	UNIDADE	01
	7	Suporte, garantia e Manutenção do item 06.	27740	SERVIÇO	01
	8	Treinamento ministrado por profissional certificado pelo fabricante.	16837/20052	CAPACITAÇÃO	01
	9	Plataforma de ZTNA - Zero Trust Network Access.	27742	SERVIÇO	01

2.3. - PARCELAMENTO DA SOLUÇÃO DE TIC

2.3.1. - O objeto do certame não será parcelado, uma vez que os bens e serviços que compõem o objeto formam um conjunto indissociável, composto pela interligação dos serviços que funcionam harmonicamente. As melhores práticas de gestão de TI se baseiam na integração dos serviços, que são indissociáveis e apresentam inter-relação entre si, de forma que assegurem o alinhamento e a coerência em termos de qualidade técnica, resultando assim, no perfeito atendimento dos princípios da celeridade, economicidade e eficiência.

2.3.2. - Somente a execução de forma integrada dos serviços garante a disponibilidade, segurança e a preservação dos dados de execução, evitando transferência de responsabilidades, nos casos de eventuais problemas causados por serviços prestados por mais de uma empresa contratada.

2.3.3. - O fornecimento de itens por meio de contratadas distintas traria enormes riscos ao projeto. Um grande risco viria da necessidade contínua de comunicação entre os diferentes fornecedores, o que, historicamente, não ocorre com fluidez nem de forma satisfatória, sendo a parte mais prejudicada, o MAPA. Além disso, há necessidade de ocorrer perfeita integração técnica entre os itens do objeto. Dessa forma, o fornecimento parcial dos itens por diferentes fornecedores traria não apenas maior complexidade, como maiores custos de integração e riscos de não execução adequada.

2.3.4. - A licitação por item poderia causar prejuízo para o conjunto da licitação (questões técnicas) ou para a economia de escala (questões econômicas), e tornaria inviável e prejudicial o bom desempenho da solução, por se tratar de serviços complementares. Ademais, por se tratar de uma solução de serviços integrados, é fundamental para a garantia da qualidade do serviço, que sejam executados por um mesmo fornecedor, dada a impossibilidade de segregação do objeto sem que haja prejuízo ao conjunto, objetivando alcançar produtividade, economicidade e eficiência na realização dos serviços.

2.3.5. - Desta forma, o agrupamento de elementos que compõem a mesma solução compõe a melhor estratégia da Administração, quando a adjudicação de itens isolados onera o "o trabalho da administração pública, sob o ponto de vista do emprego de recursos humanos e da dificuldade de controle, colocando em risco a economia de escala e a celeridade processual", vide o ACÓRDÃO Nº 5301/2013 – TCU – 2ª Câmara. É importante também, se observar o posicionamento do Egrégio Tribunal de Contas da União, nos autos do Acórdão nº 1916/2009 – Plenário, sob a matéria:

> *"15. Acerca da alegada possibilidade de fragmentação do objeto, vale notar que nos termos do art. 23, § 1º, da Lei n. 8.666/1993, exige-se o parcelamento do objeto licitado sempre que isso se mostre técnica e economicamente viável. A respeito da matéria, esta Corte de Contas já editou a Súmula n. 247 /2004, in verbis: "É obrigatória a admissão da adjudicação por item e não por preço global, nos editais das licitações para a contratação de obras, serviços, compras e alienações, cujo objeto seja divisível, desde que não haja prejuízo para o conjunto ou complexo ou perda de economia de escala, tendo em vista o objetivo de propiciar a ampla participação de licitantes..." (grifou-se).*

2.3.6. - Depreende-se, portanto, que a divisão do objeto deverá ser implementada sempre que houver viabilidade técnica e econômica para a sua adoção.

2.3.7. - Nesse ponto, calha trazer à baila o escólio de Marçal Justen Filho: "O fracionamento em lotes deve respeitar a integridade qualitativa do objeto a ser executado. Não é possível desnaturar um certo objeto, fragmentando-o em contratações diversas e que importam o risco de impossibilidade de execução satisfatória." (Comentários à Lei de Licitações e Contratos Administrativos. 10. ed. São Paulo: Dialética, 2004. p. 209)."

2.3.8. - Adicionalmente, em virtude da especificidade do objeto, pode-se afirmar ser tecnicamente inadequado o seu desmembramento, sob pena de não se atender o objetivo buscado, no sentido de fortalecer a disponibilidade, segurança, a preservação dos dados e ativos de TI do MAPA na manutenção da operabilidade do ambiente de TI.

2.3.9. - Ainda, sob o ponto de vista econômico, não há elementos nos autos que permitam concluir que a adoção do parcelamento do objeto, seria, no caso concreto, mais vantajosa para o MAPA.

2.3.10. - Por fim, o objeto não será parcelado, pois constitui-se em uma única solução de TIC e os serviços que compõem o objeto licitado são serviços de mesma natureza, dependentes entre si, e sua divisão impactaria na execução do projeto e tornaria a contratação menos econômica, eficaz e eficiente para a Administração. Assim, considerando-se a inviabilidade técnica e econômica para o parcelamento do objeto da presente contratação, bem como consideradas as suas respectivas peculiaridades, interdependência e natureza acessória entre os serviços que compõem o objeto, a contratação pretendida deverá ser realizada em um único grupo.

3. FUNDAMENTAÇÃO E DESCRIÇÃO DA NECESSIDADE

3.1 - CONTEXTUALIZAÇÃO, JUSTIFICATIVA E DESCRIÇÃO DA NECESSIDADE

3.1.1 - As organizações e instituições públicas reconhecem que a informação é um dos seus principais ativos, desempenhando um papel fundamental na tomada de decisões em todos os níveis e na efetiva gestão governamental. Nesse sentido, os gestores devem adotar medidas para garantir a segurança dessas informações.

3.1.2 - Os constantes ataques cibernéticos, a necessidade de continuidade do negócio e a evolução de ameaças das mais variadas espécies criam a necessidade de contratação de uma solução eficaz que proteja as informações dos órgãos públicos (MAPA e Ministérios demandantes) e diminua os riscos de acessos indevidos às mesmas. Essa crescente disseminação de ataques, em especial à Administração Pública, vem sendo alvo de ações maliciosas com destaque para invasões de sites oficiais, indisponibilidade de recursos e serviços, exposição de vulnerabilidades e consequentes vazamentos de informações, causando assim prejuízos não só ao erário, mas também reflexos negativos no atendimento aos cidadãos , empresas e demais entes envolvidos.

3.1.3 - Devido ao aumento significativo dessas ameaças, é imprescindível implementar inteligência e automatização no gerenciamento das soluções de segurança. As ferramentas adotadas para o cenário de outrora tornaram-se insuficientes, uma vez que as tecnologias de mercado evoluíram e o ambiente se expandiu consistentemente. Assim, é prudente acompanhar a evolução e adotar as atualizações tecnológicas necessárias para fornecer serviços adequados e mais seguros/eficientes. Além disso, em um contexto dinâmico de constante evolução tecnológica e em um curto intervalo de tempo, os equipamentos destinados à segurança da informação podem se tornar obsoletos a tal ponto de não suportarem o aumento do tráfego de internet e dados, o crescimento de novos usuários/novas ameaças e tentativas de invasões das redes corporativas. As tecnologias voltadas à segurança da informação estão em constante aperfeiçoamento, e os fabricantes buscam soluções eficazes para obter o melhor desempenho dos firewalls e ao mesmo tempo prover inteligência proativa, reunindo as mais diversas funcionalidades.

3.1.4 - À medida que a dependência do MAPA por sistemas e serviços de informação aumenta, crescem também as ameaças cibernéticas que, muitas vezes, resultam em falhas de segurança críticas que, por sua vez, podem gerar centenas de milhões de reais de prejuízo aos cidadãos, além de causar grandes danos à imagem dos Ministérios (MAPA e Ministérios demandantes).

3.1.5 - O Gabinete de Segurança Institucional da Presidência da República (GSI/PR) responsável por coordenar as atividades de segurança da informação e das comunicações no governo federal, em sua portaria PORTARIA GSI/PR Nº 120, DE 21 DE DEZEMBRO DE 2022 (https://www.in.gov.br/en/web/dou/-/portaria-gsi/pr-n-120-de-21-de-dezembro-de-2022-452767918) deixa claro as orientações para proteção das entidades publicas do executivo federal, ao qual destacamos:

2. PREVENÇÃO

A prevenção é um processo constante de ações proativas com o objetivo de reduzir a probabilidade de ataques cibernéticos bem-sucedidos. Entre essas ações, enfatizam-se as de definição e de implementação de controles de segurança, de gerenciamento de vulnerabilidades, de conscientização e de capacitação.

As ações preventivas de segurança cibernética deverão contemplar aquelas previstas na política de segurança da informação do integrante da Regic.

2.1. Definição e implementação de controles de segurança preventivos

Os controles de segurança preventivos constituem-se em tecnológicos, organizacionais e físicos.

Os controles tecnológicos são aqueles utilizados para reduzir vulnerabilidades no **hardware** e no **software**. Entre os principais de controles tecnológicos estão:

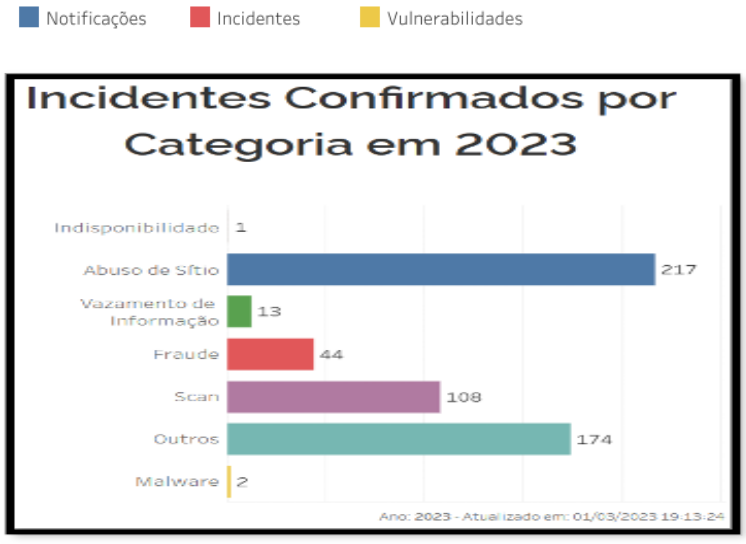
- dispositivos **endpoint** do usuário;
- restrição de acesso à informação;
- autenticação segura;
- proteção contra **malware**;
- **backup** das informações;
- atividades de monitoramento (log);
- segurança de redes;
- uso de criptografia; e
- gestão de mudanças.

3.1.6 - Ainda com relação à portaria citada, os controles físicos tem por finalidade prevenir ou evitar o acesso não autorizado à área ou material sensível, bem como os danos e interferências às áreas que contenham informações críticas ou sensíveis. Entre os principais controles físicos estão: Definição dos perímetros de segurança física; Monitoramento de segurança física; Proteção contra ameaças físicas e ambientais; Localização e proteção de equipamentos; Segurança de ativos fora das instalações da organização e Manutenção dos ativos.

3.1.7 - Ainda nesta linha o Centro de Prevenção , Tratamento e Resposta a Incidentes Cibernéticos de Governo, entidade que está enquadrada na categoria "CSIRT de responsabilidade nacional de coordenação" publica regularmente relatórios sobre a quantidade de incidentes descobertos (https://www.gov.br/ctir/pt-br/assuntos/ctir-gov-em-numeros/visao-geral) . Vejamos alguns dados importantes:

2019	2020	2021	2022	2023
23.674	24.300	22.298	18.489	3.254
10.716	5.257	4.910	3.786	559
1.201	2.270	3.917	3.189	680

Atualizado em: 01/03/2023 19:13:24



3.1.8 - Percebe-se que a quantidade de incidentes no âmbito do governo federal é extremamente relevante. Em relação à proteção de perímetro, temos que esta é uma das proteções mais importantes em uma instituição, e que se atualizam constantemente por meio de soluções que são conhecidas no mercado como NGFW.

A compra de um Next-Generation Firewall (NGFW) pode trazer vários benefícios para uma organização. Entre elas:

- **Proteção avançada contra ameaças:** Um NGFW oferece recursos de segurança avançados que podem proteger contra ameaças cibernéticas, como malware, phishing, ransomware e ataques de dia zero. Isso inclui recursos como detecção de intrusões, filtragem de URL, antivírus, inspeção de tráfego SSL/TLS e muito mais.

- **Controle de acesso a aplicativos:** Um NGFW permite que uma organização controle o acesso a aplicativos específicos, permitindo ou bloqueando o acesso com base em políticas de segurança definidas. Isso ajuda a proteger contra o uso indevido de aplicativos e reduz o risco de violações de dados.

- **Visibilidade e controle de tráfego:** Um NGFW fornece uma visão completa do tráfego de rede, permitindo que as organizações monitorem e controlem o tráfego de entrada e saída. Isso pode ajudar a identificar e mitigar atividades suspeitas e proteger contra vazamentos de dados.

- **Gerenciamento centralizado:** Um NGFW pode ser gerenciado de forma centralizada, permitindo que as organizações gerenciem políticas de segurança, implementem atualizações e monitorem o tráfego de rede em vários locais a partir de um único console.

3.1.9 - O padrão NGFW deve auxiliar na segurança da informação, figurando como a primeira camada de proteção da rede de computadores do MAPA, com objetivo de prover proteção de perímetro e borda da rede de computadores do MAPA. Os equipamentos visam fornecer condições seguras de acesso a sistemas sensíveis da instituição, que não podem ser disponibilizados diretamente na internet sob o risco de vazamento de informações sob sigilo, através de canais e acessos seguros (ZTNA), que tem as premissas de permitir, bloquear, filtrar, redirecionar, controlar o acesso a aplicações internas e externas, sites internos e Internet.

3.1.10 - A Lei Geral de Proteção de Dados nº 13.709, de 14 de agosto de 2018, entrou em vigência, ampliando as exigências do Marco Civil da Internet e reforçando a utilização de melhores práticas de mercado no que tange aspectos da Segurança da Informação. Tal Lei, a partir de 2021 passa a aplicar sanções administrativas pesadas para entidades privadas e públicas de até R$ 50.000.000,00 (cinquenta milhões de reais) por infração. A exemplificar, no caso de vazamento de informações de algum banco de dados de usuários deste Ministério, caracterizaria infração e aplicação de sanção.

3.1.11 - Com a Medida Provisória Nº 1.154, de 1º de janeiro de 2023, o compartilhamento de atividades de administração patrimonial, de material, de gestão de pessoas, de serviços gerais, de orçamento e finanças, de contabilidade, de logística, de contratos, **de tecnologia da informação**, de planejamento governamental e gestão estratégica e de outras atividades de suporte administrativo deve ser realizada por meio de arranjos colaborativos entre **Ministérios ou modelos centralizados**, por isso essa contratação também irá atender, por meio de arranjos colaborativos, os Ministérios da Pesca e Aquicultura e Ministério do Desenvolvimento Agrário e Agricultura Familiar. As despesas executadas para a prestação de serviços administrativos compartilhados serão assumidas pelo Ministério demandante, sem necessidade de celebração de termo de execução descentralizada, nos termos do inciso II do § 3º do art. 3º do Decreto nº 10.426, de 16 de julho de 2020.

3.1.12 - Dentro do contexto analisado, a substituição da solução de TIC relacionada ao firewall do MAPA e demais Ministérios demandantes (MPA e MDA) é essencial, uma vez que regula o tráfego de dados entre redes distintas e impede a transmissão e recepção de informações a partir de acessos nocivos ou não autorizados na rede, além de trazer outros inúmeros benefícios (Por exemplo, maior integração com outros fabricantes de soluções de segurança) que serão detalhados ao longo do no termo de referência.

3.2 . ALINHAMENTO DA SOLUÇÃO DE TIC COM OS INSTRUMENTOS DE PLANEJAMENTO

3.2.1. - ALINHAMENTO AO PAC 2022 (Disponível em https://www.gov.br/agricultura/pt-br/acesso-a-informacao/licitacoes-e-contratos/plano-anual-de-contratacoes/mapa-sede-uasg-130005 **)**

UASG	Nº ITEM	TIPO DE ITEM	SUBITEM	CÓDIGO DO ITEM	DESCRIÇÃO	VALOR TOTAL ESTIMADO R$
130005	274	Soluções de TIC.	Serviço de TIC	22993	Informática - Suporte Técnico (Software Equipamentos)	R$ 2.800.000,00

3.2.2. - ALINHAMENTO AO PDTIC 2021-2031/PLANEJAMENTO ESTRATÉGICO DO MAPA

META 7	NECESSIDADE 5	INDICADOR	OBJETIVO ESTRATÉGICO 23 Categoria - Segurança da Informação.

Tornar as informações, dados e conectividade protegidos e 100% compatível com Normativos de Segurança, incluindo a Lei Geral de Proteção de Dados.	Proteger dados, comunicações e ativos que sejam considerados estratégicos ou identifiquem pessoas físicas e jurídicas.	Aderência à LGPD.	Adequar a capacidade da tecnologia da informação aos novos desafios da transformação digital.

3.2.3. - Nos termos do Decreto Nº 8936, de 19 de dezembro de 2016, por não se tratar de oferta de serviços públicos digitais, consequentemente, o objeto da contratação também não será integrado à plataforma Gov.br.

3.3. - RELAÇÃO ENTRE A NECESSIDADE DA CONTRATAÇÃO DA SOLUÇÃO DE TIC E CARACTERÍSTICAS DO OBJETO / FORMA DE CÁLCULO PARA DEFINIÇÃO DO QUANTIDADE DE BENS E SERVIÇOS

GRUPO	ITEM	DESCRIÇÃO	QUANTIDADE	JUSTIFICATIVA/MEMÓRIA DE CÁLCULO
ÚNICO	**1**	Appliances físicos - Solução de plataforma de segurança em alta disponibilidade, denominada Next Generation Firewall, com licenciamento incluso.	01	Quantitativo referente a 01 conjunto(cluster) que funcionará no data center do bloco D da Esplanada dos Ministérios. Ele será o cluster principal de perímetro.
	2	Suporte, garantia e manutenção dos itens 01.	01	Serviço referente ao licenciamento, garantia e manutenção dos bens constantes do item 01.
	3	Appliances Físicos - Solução de plataforma de segurança em alta disponibilidade, denominada Next Generation Firewall, com licenciamento incluso.	03	Quantitativo referente a 03 conjuntos (clusters) que funcionarão no data center do bloco D da Esplanada dos Ministérios. Eles irão atuar na proteção de serviços WEB, banco de dados, DMZ, entre outros.
	4	Suporte, garantia e manutenção dos itens 03.	03	Serviço referente ao licenciamento, garantia e manutenção dos bens constantes do item 03.
	5	Serviço de instalação e configuração dos firewalls NGFW dos itens 01 e 03.	01	Quantitativo referente à instalação e configuração da solução baseada nas melhores práticas: Appliances de firewall de próxima geração e componentes de segurança. O serviço corresponde ao conjunto de instalação e configuração dos equipamentos fornecidos nos itens 01 ao 04.
	6	Appliance - Plataforma de gestão e monitoramento centralizado, com licenciamento, instalação e configuração.	01	Quantitativo levantado de acordo com a necessidade para gerência centralizada da solução.
	7	Suporte, garantia e manutenção do item 06.	01	Quantitativo levantado de acordo com o item 06.
	8	Treinamento Oficial ministrado por profissional certificado pelo fabricante.	01 Treinamento	Baseado no quantitativo de servidores que atuam na área de segurança da informação do MAPA. Detalhes da quantidade estão descritos no termo de referência.
	9	Plataforma de ZTNA.	01 Serviço	Serviço para ,no mínimo, 500 usuários simultâneos.

3.4. - RESULTADOS E BENEFÍCIOS A SEREM ALCANÇADOS COM A CONTRATAÇÃO

- Aumento da capacidade de resposta aos incidentes cibernéticos.
- Melhorar o acesso remoto de maneira estável aos colaboradores de forma segura.
- Aprimorar a segurança de TIC do Ministério da Agricultura e demais órgãos demandantes frente às recentes ameaças.
- Contribuir para a garantia de um nível adequado de Confidencialidade, Integridade e Disponibilidade.
- Maior visibilidade do trafego das informações e da rede, possibilitando a detecção e proteção em tempo real contra as ameaças. Com isso, será possível corrigir comportamentos inadequados; direcionar recursos para demandas mais relevantes; controlar serviços e aplicações suspeitas ou que interferem diretamente na produtividade.

- Permitir a criação de políticas de proteção da rede contra eventuais ataques de usuários mal-intencionados, através do bloqueio de portas não utilizadas e melhor controle de uso de banda de internet, com o objetivo de evitar abusos em sua utilização;
- Maior rapidez na detecção - Priorização de alertas de segurança e avisos constantes sobre normas de cibersegurança dentro de uma organização, evitando que erros humanos sejam cometidos na hora de acessar links duvidosos e outras páginas maliciosas.
- Aprimorar a detecção e bloqueio de ameaças avançadas, como malware, ataques de negação de serviço distribuídos (DDoS) e tentativas de invasão de rede.
- Melhoria na geração de relatórios diversos para rápida análise de informações sobre tráfego, aplicações, ameaças, usuários, etc.
- Conseguir atender à crescente dependência dos recursos de tecnologia da informação, que fazem com que a infraestrutura de rede deva apresentar cada vez maior confiabilidade, resiliência, disponibilidade, segurança, capacidade de resolução de problemas de maneira proativa e rápida e melhorar a experiência para todos os usuários da rede do MAPA, MDA e MPA.
- Melhoria na filtragem de conteúdo web, implementando uma filtragem mais abrangente, com criação de regras de uso de aplicações web, que permitam a limitação de acesso a certas categorias de serviços, por meio de análise de tráfego.
- Além das citadas, o NGFW permite a interação das seguintes funções em um mesmo equipamento:
    - Firewall Corporativo (Stateful Firewall).
    - Controle de aplicações (AVC-Application Visibility Control).
    - Prevenção de ameaças (IPS-Intrusion Prevention System).
    - Análises de malware "zero-day".
    - Filtro de URL e Identificação de usuários com controle granular de permissões.

4. REQUISITOS DA CONTRATAÇÃO DE TIC

4.1 . REQUISITOS DE NEGÓCIO

- Aquisição de solução de segurança da perímetro contemplando os hardwares, softwares, licenciamentos, implantações, configurações, treinamento, garantia, atualizações e suporte técnico, em atendimento ao documento de formalização da demanda SEI Nº 27476908 da Coordenação-Geral de Infraestrutura, Segurança e Serviços Digitais da Subsecretaria de Tecnologia da Informação do MAPA.
- Melhorar e garantir o perfeito funcionamento da infraestrutura da rede do MAPA e seus Ministérios demandantes.
- Prover e Garantir a segurança das informações como também a continuidade dos serviços de TIC do MAPA e seus Ministério demandantes.
- Assegurar a confidencialidade, disponibilidade e integridades das informações do MAPA e seus Ministérios demandantes em conformidade com a LGPD.
- Melhorar a identificação e o rastreamento das tentativas de invasão às redes do MAPA e seus Ministérios demandantes
- Melhoria na implementação de regras e políticas de seguranças relacionados ao uso da rede computacional do MAPA e seus Ministérios demandantes.
- Melhorar o nível de qualidade e segurança dos serviços e aplicações internas do MAPA e seus Ministérios demandantes
- Melhorar a proteção da infraestrutura de TIC de modo a impedir que a rede do MAPA e seus Ministérios demandantes seja utilizada para outros fins (por exemplo: Mineração de bitcoins, links de internet utilizados para download de conteúdo ilícito , ataques de negação de serviço- DDOS, entre outros).
- Melhoria no reconhecimento e controle da aplicação para detectar e bloquear aplicativos nocivos do MAPA e seus Ministérios demandantes.
- Melhorar o tempo de resposta aos ataques com automação de segurança.
- A solução deve estar sempre atualizada, em sua última versão disponível, durante a vigência do contrato.

4.2 . REQUISITOS LEGAIS

A presente contratação sujeita-se à legislação pertinente, mormente aos diplomas a seguir elencados, bem como às demais normas gerais que se apliquem, considerando-se a legislação consolidada com as respectivas alterações subsequentes:

4.2.1 . LEIS

- Lei Nº 14.133, de 1º de Abril de 2021.
- Lei Nº 13.709, de 14 de Agosto de 2018 e Lei Nº 13.853, de 08 de julho de 2019. (LGPD).

4.2.2 . DECRETOS

- Decreto Nº 10.024/2019: Regulamenta a licitação, na modalidade pregão, na forma eletrônica, para a aquisição de bens e a contratação de serviços comuns, incluídos os serviços comuns de engenharia, e dispõe sobre o uso da dispensa eletrônica, no âmbito da administração pública federal.
- Decreto Nº 9.507/2018: Dispõe sobre a execução indireta, mediante contratação, de serviços da administração pública federal direta, autárquica e fundacional e das empresas públicas e das sociedades de economia mista controladas pela União;
- Decreto Nº 7.174/2010: Regulamenta a contratação de bens e serviços de informática e automação pela administração pública federal, direta ou indireta, pelas fundações instituídas ou mantidas pelo Poder Público e pelas demais organizações sob o controle direto ou indireto da União;
- Decreto-Lei Nº 200, de 25 de fevereiro de 1967 - dispõe sobre a organização da Administração Federal, estabelece diretrizes para a Reforma Administrativa.
- Decreto Nº10.947, de 25 de Janeiro de 2022. (Regulamenta o inciso VII do caput do art. 12 da Lei nº 14.133, de 1º de abril de 2021, para dispor sobre o plano de contratações anual e instituir o Sistema de Planejamento e Gerenciamento de Contratações no âmbito da administração pública federal direta, autárquica e fundacional.)
- Decreto Nº 10.569, de 09 de dezembro de 2020 - Estratégia nacional de Segurança da Infraestrutura Críticas.

4.2.3 . INSTRUÇÕES NORMATIVAS

- Instrução Normativa SGD/ME Nº 94, de 23 de Dezembro de 2022 (Dispõe sobre o processo de contratação de soluções de Tecnologia da Informação e Comunicação - TIC pelos órgãos e entidades integrantes do Sistema de Administração dos Recursos de Tecnologia da Informação - SISP do Poder Executivo Federal).
- Instrução Normativa Nº 5 de 25 de maio de 2017 (Dispõe sobre as regras e diretrizes do procedimento de contratação de serviços sob o regime de execução indireta no âmbito da Administração Pública federal direta, autárquica e fundacional.)
- Instrução Normativa SEGES/ME Nº 65, de 7 de Julho de 2021-Dispõe sobre o procedimento administrativo para a realização de pesquisa de preços para aquisição de bens e contratação de serviços em geral, no âmbito da administração pública federal direta, autárquica e fundacional.
- Boas práticas, orientações e vedações para contratação de Ativos de TIC - Versão 4. Orientações específicas para a aquisição de Ativos de TIC. (Este guia está vinculado à Instrução Normativa SGD/ME nº 94, de 23 de dezembro de 2022, conforme § 2º do Art. 8º)
- Instruções normativas SEGES Nº 58, de 08 de agosto de 2022 - Dispõe sobre a elaboração de estudo técnicos preliminares-ETP para a aquisição de bens e contratação de serviços e obras, no âmbito da administração pública federal direta, autárquica e fundacional, e sobre o ETP Digital.
- Instrução normativa Nº 01 , de 19 de janeiro de 2010. - Dispõe sobre os critérios de sustentabilidade ambiental na aquisição de bens, contratação de serviços ou obras pela Administração Pública Federal, autárquica e fundacional e dá outras providências.)
- Instrução Normativas SEGES/ME Nº 81, de 25 de Novembro de 2022, a qual Dispõe sobre a elaboração do Termo de Referência – TR, para a aquisição de bens e a contratação de serviços, no âmbito da administração pública federal direta, autárquica e fundacional, e sobre o Sistema TR digital.

4.2.4 . PORTARIAS

- Portaria MGI Nº 43, de 31 de Janeiro de 2023. (Disciplina o compartilhamento de atividades de administração patrimonial, de material, de gestão de pessoas, de serviços gerais, de orçamento e finanças, de contabilidade, de logística, de contratos, de tecnologia da informação, de planejamento governamental e gestão estratégica e de outras atividades de suporte administrativo realizadas por meio de arranjos colaborativos entre Ministérios ou modelos centralizados, e dispõe sobre medidas transitórias decorrentes da edição da Medida Provisória nº 1.154, de 1º de janeiro de 2023.)
- Portaria GSI/PR Nº 120, de 21 de Dezembro de 2022. (Aprova o Plano de Gestão de Incidentes Cibernéticos para a administração pública federal).
- Portaria MAPA Nº 136, de 25 de Maio de 2021 (Aprova a Política de Segurança da Informação do Ministério da Agricultura, Pecuária e Abastecimento - POSIC/MAPA.)
- Portaria MAPA Nº 499, de 17 de Outubro de 2022 - Política de Gestão de Vulnerabilidades Cibernéticas.
- Portaria GSI/PR Nº 93, de 18 de outubro de 2021 - Aprova o glossário de segurança da informação.

4.3 . REQUISITOS TEMPORAIS

- O serviço de substituição de hardware será prestado na modalidade 24x7x365, ou seja, estará disponível para acionamento 24 horas por dia, 7 dias por semana, devendo substituir quaisquer peças ou componentes defeituosos em um prazo máximo conforme último tópico estipulado no item 4.5.2.2.2, contados a partir da data de abertura do chamado (ticket de atendimento).
- O prazo indicado no subitem anterior, durante seu transcurso, poderá ser prorrogado uma única vez, por igual período, mediante solicitação escrita e justificada da Contratada, devidamente aceita pelo fiscal técnico do contrato.

- A entrega total , configuração e implantação completa de todos os bens e da solução de TIC deve ocorrer em no máximo 60 dias úteis a partir da assinatura da ordem de serviço, devendo ser agendada com antecedência mínima de 48 horas. Para itens de software, poderá ser fornecido sem mídia de instalação, desde que seja indicado local seguro para download dos arquivos de instalação.
- O treinamento deverá ser iniciado em no máximo 10 dias úteis após a instalação e configuração da solução de TIC contratada.
- A contratada deverá cumprir todos os prazos descritos neste estudo técnico preliminar, respeitando os prazos máximos estabelecidos.

A seguir, segue um resumo de alguns requisitos temporais mais importantes:

ID	DESCRIÇÃO	PRAZO MÁXIMO (DIAS ÚTEIS)
1	Assinatura do contrato.(MAPA e Contratada)	Início dos prazos - D
2	Realização da reunião inicial. (MAPA e contratada). Apresentação formal da equipe de fiscalização do contrato e do preposto. (contratante e contratada) Repasse à contratada de conhecimentos necessários à execução dos serviços (contratante); Entrega do termo de compromisso e de ciência devidamente assinados (contratada).	D + 4
3	Entrega do projeto da implantação (Contratada).	D + 09
4	Análise e aprovação do projeto de implantação (contratante).	D + 14
5	Finalização da execução dos serviços e instalação dos bens. (Contratada)	D + 60
6	Início do treinamento	10 dias após o ID 5 ou a depender da disponibilidade dos recursos do MAPA.

4.4 . REQUISITOS SOCIAIS, AMBIENTAIS E CULTURAIS

- Durante a execução de tarefas no ambiente do MAPA, os funcionários da empresa contratada deverão observar, no trato c om os servidores públicos em geral, a urbanidade e os bons costumes de comportamento, tais como: asseio, pontualidade, cooperação, respeito mútuo, discrição e zelo com o patrimônio público.
- A documentação e os manuais de operação da solução deverão ser apresentados preferencialmente no idioma Português (Brasil – PT-BR) e, em sua ausência, deverão ser apresentados em idioma Inglês. Ademais, deverá entregar os documentos solicitados na forma digital, com vistas a evitar ou reduzir o uso de papel e impressão, em atendimento ao Art. 9º da Política de Nacional de Resíduos Sólidos (Lei nº 12.305, de 2 de agosto de 2010).
- A abertura de chamados técnicos e encaminhamento de demandas deverão ser realizados, obrigatoriamente, sob a forma eletrônica, evitando a impressão de papel. Além disso, as configurações de hardware e softwares deverão ser realizadas visando alto desempenho com a utilização racional de energia.
- Em conformidade com a IN SLTI Nº 01/2010 e citada no Guia nacional de Contratações Sustentáveis(disponível em: https://www.gov.br/agu/pt-br/composicao/cgu/cgu/guias/gncs_082022.pdf) , a contratada deverá cumprir com os seguintes requisitos de sustentabilidade ambiental, quando aplicável:
    - Que os bens sejam constituídos, no todo ou em parte, por material reciclado, atóxico, biodegradável, conforme ABNT NBR - 15448-1 e 15448-2.
    - Que sejam observados os requisitos ambientais para a obtenção de certificação do INMETRO, como produtos sustentáveis ou de menor impacto ambiental em relação aos seus similares.
    - Que os bens devam ser, preferencialmente, acondicionados em embalagem individual adequada, com o menor volume possível, que utilize materiais recicláveis, de forma a garantia máxima proteção durante o transporte e o armazenamento.
    - Que os bens não contenham substâncias perigosas em concentração acima da recomendada na diretiva RoHS (Restriction of certain Hazardous Substances), tais como mercúrio, chumbo, cromo hexavalente, cádmio, bifenilpolibromados (PBBs), éteres difenil-polibromados (PBDEs).
- Quanto aos critérios sociais, todos os profissionais da Contratada que desempenharão as atividades em contato direto com a Contratante deverão cumprir os seguintes requisitos:
    - Estar vestidos de forma adequada ao ambiente de trabalho físico ou virtual, evitando-se o vestuário que caracterize o comprometimento da boa imagem institucional da Contratante ou que ofenda o senso comum de moral e bons costumes;
    - Respeitar todos os servidores, funcionários e colaboradores, em qualquer posição hierárquica, preservando a comunicação e o relacionamento interpessoal construtivo;

- Atuar dentro das instalações do MAPA e órgãos demandantes com urbanidade e cortesia.

Abaixo, Seguem os requisitos tecnológicos:

4.5 . REQUISITOS TÉCNICOS GERAIS DA SOLUÇÃO DE TIC

- A comunicação entre os appliances de segurança e o módulo de gerência deve ser através de meio criptografado.
- Não serão aceitos modelos em listas de end-of-sale, cuja data do fim de vendas seja anterior data da proposta.
- Não serão aceitos modelos em lista de end-of-support, cuja data do fim do suporte seja anterior ao fim da vigência do contrato e/ou do fim do período de garantia e suporte exigido no edital.
- A solução de balanceamento deverá ser fornecida em Alta Disponibilidade do tipo Ativo/Ativo.
- Transferir todas as regras e configurações dos Firewalls em produção atualmente.
- Tanto os dispositivos físicos (“appliance”) quanto seus softwares deverão ser novos, de primeiro uso, e disponibilizados em suas versões mais atualizadas.
- As funcionalidades de proteção de rede que compõe a plataforma de segurança, podem funcionar em múltiplos equipamentos do mesmo fabricante, desde que obedeçam a todos os requisitos desta especificação (por item/por equipamento). A solução deve suportar o balanceamento entre os appliances de Next generation Firewall ofertados, de modo a permitir que seus throughputs, suas capacidades de análise, capacidades de inspeção bem como todas as funcionalidades pedidas nos itens 01 e 03 e seus subitens sejam somados.
- Os equipamentos dos itens 01, 03, 06 e 09 devem ser do **mesmo fabricante**, completamente interoperáveis, e devem ser capazes de fazer escalonamento de desempenho com movimentação de appliances dentro da topologia da rede. Autenticação de dois fatores, no que couber, principalmente na plataforma de gerenciamento (item 6 da contratação).
- A solução deve suportar a possibilidade de manutenção dinâmica de um equipamento de um grupo para outro, de acordo com a necessidade da arquitetura definida, sem que haja a perda do tráfego.
- A solução deverá possuir a quantidade de transceptores suficientes para conectar toda a solução à rede corporativa, o que inclui a gerência.

Nos itens 4.5.1 e 4.5.2 , estão as características básicas dos itens 01 ao 04 da contratação, os demais requisitos estão descritos no Anexo - Especificação técnica da solução de TIC. Já os itens 05 ao 09 estão totalmente especificados nos itens 4.5.3, 4.5.4, 4.5.5, 4.5.6 e 4.5.7.

4.5.1 . REQUISITOS GERAIS DO ITEM 01 e 03

- Solução integrada de proteção de rede do tipo “Next Generation Firewall” (NGFW), formada pelo conjunto de dispositivos ,obrigatoriamente físicos (appliances), interconectados e operando em modo de alta disponibilidade, com recursos de virtualização de sistemas, filtragem de pacotes, filtro de URL (web-filtering) com controle de transmissão de dados e de acesso à internet, controle de aplicação, controle por meio de identificação de usuários, controle de uso de largura debanda (QoS), VLAN, NAT, VPN, DHCP services (server, client e relay), sistema de prevenção de intrusão (IPS) e prevenção contra ameaças de vírus, spywares e malwares, incluindo os de tipo “Zero Day”.
- Conjunto de dispositivo físico (appliance) de proteção de rede com funcionalidades de Next Generation Firewall (NGFW), sistema operacional embarcado no dispositivo e software para sua gestão e monitoramento, permitindo o controle granular das políticas de segurança de rede, atuando além da camada 2 a 4 do modelo OSI, ou seja, além da filtragem por endereços MAC e endereços e portas TCP/IP, permitindo a configuração de políticas de segurança também por aplicações, incluindo seu conteúdo, usuários e tipos de tráfego de rede, recursos tipicamente executados em camada 7.
- O Firewall NGFW deve ser do tipo “rackmount”, permitindo sua instalação em racks de Datacenter , devendo consumir um espaço no rack de no máximo 4U por dispositivo.
- **Não** serão aceitos equipamentos servidores (“rack servers”) e sistemas operacionais de uso genérico, como Microsoft Windows ou distribuições Linux para usuários finais, adaptados para funcionar como “appliance” físico, ou seja, a solução como um todo de ser fabricada pelo mesmo fornecedor, tanto em seus componentes físicos de hardware quando seus softwares embarcados principais, sendo vedada solução de software livre.
- Todas as funcionalidades da solução Firewall NGFW deverão operar em caráter permanente, podendo ser utilizadas por tempo indeterminado, mesmo após o fim do contrato, e mesmo que o MAPA não tenha mais o direito de receber atualizações por descontinuidade da solução por parte da fabricante.
- A solução deve suportar a possibilidade de movimentação dinâmica de um equipamento de um grupo para outro, de acordo com a necessidade da arquitetura definida, sem que haja a perda do tráfego.
- A solução deverá ser provida de forma redundante, de modo que se houver a falha de um ou mais dispositivos, outro(s) possa(m) assumir totalmente o controle, sem que haja perda do tráfego.
- A solução deve ser compatível com SMPv2 e SMPv3. Os appliances devem permitir aceso ao equipamento via interface de comando(CLI), console, SSH, além de interface web HTTPS.
- Os appliances deverão vir acompanhados de todos os conectores, cabeamento e peças de fixação no Rack, necessários à sua instalação e funcionamento, conforme as especificações deste Termo de Referência.

- Todos os componentes devem ser próprios para montagem em rack “19” e deverão ser fornecidos pela Contratada, incluindo kit tipo trilho para adaptação, cabos de alimentação, suportes, gavetas e braços, se necessário.

4.5.2 . REQUISITOS GERAIS DOS ITENS 02 e 04

REQUISITOS DE SUPORTE/GARANTIA E MANUTENÇÃO

4.5.2.1 - GARANTIA

- A garantia será prestada com vistas a manter os equipamentos fornecidos e demais itens da solução de TIC em perfeitas condições de uso, sem qualquer ônus ou custo adicional para o MAPA e órgãos demandantes (MPA e MDA).
- Segundo o item 1.4.5.1, "Para aquisição de servidores de rede, aplicação, equipamentos de backup, armazenamento, segurança, entre outros, deve-se considerar o tempo de vida útil mínimo de 5 (cinco) anos para fins de posicionamento da tecnologia e de garantia de funcionamento", do documento "Orientações específicas para a aquisição de Ativos de TIC" vinculado à Instrução Normativa SGD/ME nº 94, de 23 de dezembro de 2022, a garantia recomendada é de 60 meses para os equipamentos de segurança. Entretanto, a garantia contratual exigida dos itens 01,03,06 e 09 será cobrada de maneira separada, pois caso fosse cobrada em seus próprios itens e com garantia direto de 60 meses, os valores ficariam muito altos, sendo inviável realizar os pagamentos à vista e, por isso, essa contratação está programada para ter uma vigência inicial de 02 anos, sendo prorrogável até 05 anos. Para os itens 02,04,07 e 09, eles terão prazo de garantia enquanto tiver contrato vigente, de acordo com os pagamento anuais. Ao término do contrato, em uma nova contratação, os únicos itens que devem ser contratados novamente são os suportes, garantia e manutenção dos itens 01,03,06 e 09.
- Durante o prazo de garantia, deve ser possível realizar a atualização de sistema operacional dos equipamentos e demais licenças/firmwares/softwares fornecidos com o objetivo de obter novas funcionalidades e correção de bugs. Durante o prazo de garantia, deve ser possível realizar a atualização das assinaturas de proteção da solução;
- Os chamados poderão ser abertos diretamente com a contratada, autorizada oficial do fabricante ou com o próprio fabricante no Brasil através de ligação telefônica gratuita (0800) no idioma português, website e e-mail durante a vigência da garantia. O suporte deverá ser na modalidade de 24x7x365 (24 horas por dia, 7 dias por semana);
- A contratada deve fornecer garantia de reposição de hardware, pelo prazo de vigência do contrato, para situações que sejam identificados problemas constantes na solução fornecida.
- A garantia abrange a realização da manutenção corretiva dos bens pela própria Contratada, ou, se necessário, por meio de assistência técnica autorizada, de acordo com as normas técnicas específicas.
- Todas as licenças, referentes aos softwares e drivers solicitados, devem estar registrados para utilização do Contratante, em modo definitivo (licenças perpétuas). Ao final do contrato, o MAPA deve ter as licenças mais recentes instaladas em modo definitivo (licenças perpétuas).
- O custo referente ao transporte dos equipamentos cobertos pela garantia será de responsabilidade da Contratada.
- Os serviços de “Garantia” também incluem:
    - Solução de problemas relativos à indisponibilidade da solução decorrentes de problemas de fabricação, desenvolvimento ou ocasionada pelo uso normal dos equipamentos.
    - Solução de falhas ou defeitos no funcionamento, incluindo a instalação de arquivos para correção dos erros.
    - Esclarecimento de dúvidas de alto nível.
    - Instalação de novas versões ou atualizações e patches.
- Os chamados abertos envolvendo garantia e manutenção deverão ser atendidos conforme os índices de criticidade abaixo:

CRITICIDADE	**DESCRIÇÃO DA ATIVIDADES/SERVIÇO**	**PRAZO MÁXIMO PARA SOLUÇÃO DO PROBLEMA**
Severidade Crítica	Equipamento ou software inoperante resultando em impacto nas operações críticas de negócio. Indisponibilidade dos itens da solução contratada.	08 horas após a abertura do chamado.
Severidade Alta	Alto impacto no ambiente de produção ou grande restrição de operabilidade.	16 horas úteis após a abertura do chamado.
Severidade Normal	Outros problemas de menor impacto no ambiente do MAPA e aplicado para instalação, configuração, update/upgrade da solução de TIC.	24 horas úteis após a abertura do chamado.
A definição de prazos máximos para início de atendimento não são necessárias. O foco é em resolver o problema e em quanto tempo, não sendo necessário estimar em quanto tempo terá início para atendimento do ticket.		

4.5.2.2 - MANUTENÇÃO

- Em caso de falha do(s) hardware(s), caso não seja feita a troca conforme prazo especificado, a contratada deve disponibilizar hardware(s) reserva(s) que irá(ão) permanecer em ambiente de produção do MAPA até o retorno do(s) hardware(s) original(is) reparado ou novo em substituição, a critério do MAPA e órgãos demandantes (MPA e MDA).
- Deverá assegurar que o hardware substituto, em qualquer caso, seja igual ao contratado inicialmente ou que possua características superiores a este, desde que estejam homologadas pelo fabricante como parte compatível da solução; As peças de substituição devem ser novas, não sendo aceitas peças usadas ou recondicionadas;
- A substituição do hardware será considerada consumada no momento em que a solução voltar ao seu funcionamento normal e for aceita formalmente pela equipe técnica do MAPA.

4.5.2.2.1 - MANUTENÇÃO PREVENTIVA

- A manutenção preventiva será destinada a atualizar os componentes do software e a realizar quaisquer operações que evitem uma parada parcial ou total da solução. Deve compreender a checagem da saúde e funcionamento da solução já implementada, permitindo diagnóstico preciso dos status da atual rede. Ao final de cada manutenção preventiva, deverá ser elaborado um relatório detalhado dos serviços executados.
- Durante a manutenção preventiva, a contratada deverá analisar toda a solução, sua condição atual de funcionamento, seus logs de sistemas e sugerir mudanças para uma melhor prática de utilização de ferramenta. A equipe técnica do MAPA junto ao fiscal técnico decidirá sobre a aplicação ou não das recomendações. A manutenção preventiva deverá ser executada pelo menos **02 vezes por mês** conforme cronograma a ser definido entre o fiscal técnico e equipe técnica da contratada.
- O cronograma anual poderá sofrer adequações durante o ano vigente , desde que a contratada e o MAPA estejam de acordo e que não seja descumprido o atendimento mensal.
- A futura contratada deverá realizar manutenção preventiva, realizando: Análise de logs e configurações da solução, identificando possíveis erros, conflitos e as correções necessárias; Análise de desempenho do funcionamento da solução no que diz respeito ao uso de CPU e memória e recomendar ajustes; Análise física dos equipamentos, incluindo verificações de temperatura, ventilação e eventuais alertas de falhas de hardwares; Análise de vulnerabilidades e de pendências de atualizações de versões de firmwares, engines, assinaturas ou qualquer componente da solução passível de atualização e recomendar as ações necessárias para regularização;

4.5.2.2.2 - MANUTENÇÃO CORRETIVA

- A manutenção corretiva será destinada a resolver os defeitos apresentados pelos componentes de software e hardware de toda solução de TIC do contrato, compreendendo também a atualização de versões e correções dos componentes de software e hardware que se fizerem necessários. Ademais, entende-se por manutenção corretiva aquela destinada a corrigir os defeitos apresentados pelos bens, compreendendo a substituição de peças, a realização de ajustes, reparos e correções necessárias.
- Corresponde ao tratamento dos problemas encontrados na operação da solução, incluindo esclarecimentos de dúvidas relacionadas à instalação, configuração, uso e atualização, além de reposição de peças defeituosas.
- A manutenção corretiva será realizada sempre que a solução apresentar falha que impeça o seu funcionamento regular e necessite de uma intervenção técnica especializada e, caso necessário, a substituição dos componentes. A manutenção corretiva pode ser solicitada a qualquer momento em que o sistema apresente pane, deficiência ou dificuldade de operação.
- As visitas para prestação dos serviços de manutenção preventiva e corretiva, independente da quantidade necessária, não deve implicar em custos adicionais para o MAPA.
- Entende-se por "manutenção corretiva", toda atividade do tipo corretiva não periódica que variavelmente poderá ocorrer durante o período de garantia. A atividade corretiva possui suas causas em falhas e erros no software/hardware e trata da correção dos problemas atuais e não iminentes de fabricação dos equipamentos. Essa "garantia" inclui os procedimentos destinados a recolocar em perfeito estado de operação os serviços e produtos ofertados, tais como:
    - **Do hardware:** Desinstalação, reconfiguração ou reinstalação decorrente de falhas de fabricação no hardware, fornecimento de peças de reposição, substituição de hardware defeituoso por defeito de fabricação ou ocasionada pelo uso normal dos equipamentos, atualização da versão de drivers e firmwares, ajustes e reparos necessários, de acordo com os manuais e as normas técnicas específicas para os recursos utilizados.
    - **Do Software:** Desinstalação, reconfiguração ou reinstalação decorrente de falhas de desenvolvimento do software, atualização da versão de software, outros problemas envolvidos, de acordo com os manuais e as normas técnicas específicas do fabricante para os recursos utilizados. Quanto às atualizações pertinentes aos softwares, entende-se como atualização o provimento de toda e qualquer evolução de software, incluindo correções, patches, fixes, updates, service packs, novas releases, versions, builds, upgrades, englobando inclusive versões não sucessivas, nos casos em que a solicitação de atualização de tais versões ocorra durante o período de garantia.
- A contratada deverá substituir as peças quebradas, com defeito ou gastas pelo uso normal dos equipamentos, por outras de configuração igual ou superior, originais e novas, sem que isso implique acréscimo aos preços contratados.
- Substituir, temporária ou definitivamente, o equipamento defeituoso por outro de mesma marca e modelo e com as mesmas características técnicas, novo e de primeiro uso, quando então, a partir de seu efetivo funcionamento, ficará

suspensa a contagem do prazo de reparo, nos casos em que não seja possível o reparo dentro dos prazos máximos estipulados.

- A CONTRATADA fornecerá e aplicará pacotes de correção, em data e horário a serem definidos pelo Contratante, sempre que forem encontradas falhas de laboratório (bugs) ou falhas comprovadas de segurança em software ou firmware dos aparelhos que integrem o objeto do contrato. O atendimento deste requisito está condicionado a liberação pelo fabricante dos pacotes de correção e/ou novas versões de software. Deverá fornecer, ainda, serviços de configuração, instalação, transferência de conhecimento, com licenciamento e garantia durante o período contratual, ao longo do qual deverão ser fornecidas sem custo adicional todas as correções (patches) e atualizações, inclusive de "firmware", da solução, sempre que houver adição de novas funcionalidades ou correções.
- A contratada deverá substituir os appliances (itens 01, 03, 06 e 09) componentes e/ou acessórios que apresentem defeitos, de forma definitiva, e qualquer outro appliance físico fornecido na contratação como um todo, após a intervenção corretiva nos seguintes prazos:
    - Máximo de 15 dias úteis para os itens 01, 03, 06 e 09.
    - Máximo de 20 dias úteis para os demais componentes e acessórios.

4.5.3 . REQUISITOS GERAIS DO ITEM 05

A contratada deverá prestar serviços de instalação e configuração da solução, que compreendem, entre outros, os seguintes procedimentos:

- Reunião de alinhamento para criação do escopo do projeto previamente a instalação.
- Instalação física de todos os equipamentos (hardware) e licenças (softwares) adquiridos no local determinado pela equipe responsável pelo projeto por parte do MAPA. Quando aplicável, considerar instalação em modo Alta Disponibilidade (ativo/passivo e ativo/ativo), a ser decidido no momento da instalação.
- Análise da topologia e arquitetura da rede, considerando todos equipamentos já existentes e instalados.
- Análise do acesso à Internet, sites remotos, serviços de rede oferecidos aos funcionários e aos usuários externos; Migração das regras de firewall existentes e aplicáveis à solução ofertada, considerando a adequação às políticas de aplicações em camada 7.
- Análise do posicionamento de qualquer outro equipamento ou sistema relevante na segurança de qualquer perímetro protegido pela solução.
- Configuração do sistema de firewall, IPS, Filtro URL, Antivírus e Anti-Malware de acordo com as exigências levantadas.
- Toda configuração do sistema deverá ser realizada de acordo com as melhores práticas recomendadas pelo fabricante da solução ofertada. O fabricante deverá disponibilizar ferramenta gratuita para acompanhamento da evolução da parametrização de proteção dos firewalls afim de garantir a melhor eficiência da solução durante o período de vigência das licenças.
- Configuração do sistema de gerenciamento centralizado considerando adição dos novos appliances.
- Todos os cabos de conexão, acessórios e itens relacionados ao completo funcionamento das soluções adquiridas devem ser fornecidos pela contratada.

4.5.4 . REQUISITOS GERAIS DO ITEM 06

A utilização de um appliance físico de gerenciamento centralizado facilita as tarefas de gerenciamentos de regras e políticas em um firewall. Por meio desse gerenciamento centralizado é possível gerenciar diversos appliances por meio de uma única interface. Além disso, é possível acessar registros (logs) de diversos equipamentos. Características técnicas mínimas:

- A solução de gerência deverá ser separada dos appliances de segurança, que irá gerenciar políticas de segurança de todos os firewalls e funcionalidades solicitadas nesse tópico.
- Caso a solução possua licenças relacionadas a capacidade de log indexados e armazenamento, deve ser ofertado a maior capacidade suportada ou ilimitada.
- Caso a solução possua módulo de relatórios estendida, deve ser também entregue junto com a solução.
- Deve possuir solução de gerenciamento e administração centralizado, funcionando ON PREMISES e em nuvem pública, e também possibilitando o gerenciamento dos diversos equipamentos licitados neste termo de referência.
- Suportar validação de regras antes da aplicação.
- Suportar validação das políticas, avisando quando houver regras que ofusquem ou conflitem com outras (shadowing);
- O gerenciamento da solução deve possibilitar a coleta de estatísticas de todo o tráfego que passar pelos equipamentos da plataforma de segurança.
- O Software de Gestão Centralizada deverá ser homologada e totalmente compatível com os itens 01 e 03.
- Deve permitir a exportação de logs via SCP ou FTP assim como permitir a exportação para soluções de gerenciamento de logs compatível com Syslog.).
- Centralizar a administração de regras e políticas dos Firewalls, usando uma única interface de gerenciamento.
- O gerenciamento deve permitir/possuir monitoração de logs, ferramentas de investigação de logs e acesso concorrente de administradores.
- Deve permitir controle global de políticas para todos os equipamentos que compõe a plataforma de segurança.

- Deve suportar organizar os dispositivos administrados em grupos: os sistemas virtuais devem ser administrados como dispositivos individuais, os grupos podem ser geográficos, por funcionalidade (por exemplo, IPS), e distribuição física /lógica ou topologia de rede.
- Deve implementar sistema de hierarquia entre os firewalls gerenciados, onde seja possível aplicar configurações de forma granular em grupos de firewalls.
- Deve implementar a criação de perfis de usuários com acesso a plataforma de gerenciamento com definição exata de quais informações e de quais firewalls e grupos de firewalls o usuário terá acesso referente a logs e relatórios.
- Deve permitir que a configuração dos firewalls seja importada de forma automática na plataforma de gerenciamento centralizado e que possa ser usada em outros firewalls e grupos de firewalls.
- Deve mostrar os status dos firewalls em alta disponibilidade a partir da plataforma de gerenciamento centralizado; Através da análise de tráfego de rede, web e DNS, deve suportar a verificação de máquinas potencialmente comprometidas ou usuários com uso de rede suspeito.
- Deve possuir um painel com as informações de máquinas comprometidas indicando informações de endereço IP dos usuários, veredito, número de incidentes, etc....
- O relatório deve apresentar eventos em um único portal (dashboard) e geração de relatório de todas as funcionalidades de segurança que estão ativadas nos firewalls, sendo que deve possuir relatório e telas de apresentação onde consta todo os principais eventos das funcionalidades de controle de aplicação web, filtro URL, prevenção de ameaças (IPS, Antivírus, Anti-Malware e Sandboxing).
- A solução deve permitir o login de múltiplos usuários administradores simultâneos com perfil de escrita, possibilitando agilidade e rapidez no gerenciamento pelo grupo de administradores da solução.
- Deve ser possível exportar os logs em CSV ou TXT.
- Deve possibilitar a geração de relatórios de eventos no formato PDF ou HTML.
- Simular o impacto de segurança das alterações de configuração antes da instalação de acordo com a aderência aos padrões regulatórios apresentados no item anterior.
- Permitir notificação instantânea sobre mudanças de política de segurança que impactam negativamente a segurança.
- Monitorar constantemente o status de conformidade da solução aos padrões regulatórios informados.
- Destacar potenciais violações de segurança e conformidade, reduzindo o tempo necessário e os erros associados a gestão de conformidade manual.
- Gerar alertas de conformidade notificando os usuários sobre o impacto de suas decisões de segurança trazendo as considerações regulatórias na gestão de segurança.
- Permitir o gerenciamento eficaz das ações e recomendações, facilitando a priorização e programação de itens de ação.
- Possuir alertas de políticas e os potenciais violações de conformidade.
- Possuir recomendações de segurança acionáveis e orientações sobre como melhorar a segurança.
- Gerar relatórios regulamentares com base nas configurações de segurança em tempo real.
- Permitir que os relatórios possam ser salvos, enviados e impressos.
- Deve permitir a criação de filtros com base em qualquer característica do evento, tais como a origem e o IP destino, serviço, tipo de evento, severidade do evento, nome do ataque, o país de origem e destino etc..
- A solução deve prover, no mínimo, as seguintes funcionalidades para análise avançada dos incidentes:
- Visualizar quantidade de tráfego utilizado de aplicações e navegação.
- Gráficos com principais eventos de segurança de acordo com a funcionalidade selecionada.
- A solução de correlação deve possuir mecanismo para detectar login de administradores em horários irregulares.
- A solução deve ser capaz de detectar ataques de tentativa de login e senha utilizando tipos diferentes de credencias.
- Deve suportar a geração de relatório gerencial para apresentar aos executivos os eventos de ataque de forma completamente visual, utilizando gráficos referentes a consumo de banda, ataques sofridos e quantidade de eventos gerados e protegidos.
- Deve permitir a integração com servidores de autenticação LDAP Microsoft Active Directory via Radius.
- Caso a solução possua licenciamento relacionado a capacidade de criação de certificados, deve ser contemplado a sua maior capacidade ou ilimitada.
- Permitir criações de políticas de acesso de usuários autenticada no Active Directory, de forma que reconheça os usuários de forma transparente.
- Geração de painel e relatórios contendo mapas geográficos gerados em tempo real para a visualização das principais ameaças através de origens e destinos do tráfego gerado na Instituição.
- A plataforma de gerência centralizada e monitoração deve possibilitar a visualização dos logs de Firewall, navegação web, conteúdo de arquivos, prevenção de ameaças e Sandbox, todos a partir de um único local centralizado possibilitando a procura correlacionada de logs em uma única tela, como por exemplo pesquisar logs de Antivirus e navegação web simultaneamente na mesma query de pesquisa.
- O relatório das emulações (sandboxing) deve conter, pelo menos, o print screen dos arquivos emulados, assim como todo detalhamento das atividades executadas em filesystem, registros, uso de rede e manipulação de processos e o relatório das emulações deverá ser individualizado para cada SO emulado.
- A plataforma de gerência centralizada e monitoração deve possibilitar a procura por endereços IP e redes, sendo que os resultados mostrem estas informações nos campos de origem e destino dos logs na mesma tela de pesquisa.
- Possuir mecanismo para que logs antigos sejam removidos automaticamente.

- Possuir a capacidade de personalização de gráficos como barra, linha e tabela.
- Deve permitir a criação de dashboards customizados para visibilidades do tráfego de aplicativos, categorias de URL, ameaças, serviços, países, origem e destino.
- Deve possuir a capacidade de visualizar na interface gráfica da solução, informações do sistema como licenças, memória, disco e uso de CPU.
- A solução deve ser capaz de correlacionar eventos de todas as fontes de log em tempo real.
- A solução deve fornecer conteúdo de correlação pré-definido organizado por categoria.
- A solução deve ser capaz de personalizar e criar regras de correlação.
- A solução deve fornecer uma interface gráfica para criação das regras citadas no item anterior.
- A solução deve possuir painéis de eventos em tempo real com possibilidade de configuração das atualizações e frequências.

4.5.5 . REQUISITOS GERAIS DO ITEM 07

- Suporte, garantia e manutenção, compreendendo a atualização do software com o objetivo de obter novas funcionalidades e correções de bugs. No que couber e sempre que necessário, os demais de suporte, garantia e manutenção deste item, serão os mesmos que estão especificados no tópico 4.5.2 e seus subitens (Requisitos de suporte /garantia/manutenção).

4.5.6 . REQUISITOS GERAIS DO ITEM 08

- Treinamento oficial sobre a solução de Firewall NGFW oferecida, a ser ministrada aos colaboradores do MAPA(no mínimo 04 pessoas) que atuarão diretamente na administração e operação da solução após sua implementação, com carga horária mínima de 30 horas ou carga horária oficial. Obrigatoriamente, é necessário emitir certificado de participante para 04 pessoas e outros colaboradores poderão participar como ouvintes.
- O treinamento deve iniciar em no máximo 10 dias úteis após a instalação e configuração da solução contratada ou a depender da disponibilidade do pessoal do MAPA.
- Os dias e horários para capacitação serão definidos pelo MAPA, conforme demanda do mesmo, podendo optar por utilizar apenas meio período do dia(ou até menos, se necessário) até completar a carga total prevista, e serão acordados com a contratada com uma antecedência mínima de 15 dias corridos antes do início do treinamento.
- O treinamento deverá abranger tanto teoria quanto exercícios práticos, voltados para conhecimento da arquitetura da solução, sua implantação, configuração/operação e gerenciamento, administração e monitoramento da solução, contemplando todos os aspectos essenciais de funcionamento, além de tratamento de problemas típicos envolvendo a operação da solução. Ademais, deve cobrir os seguintes tópicos: Arquitetura da solução; Configurações iniciais básicas; Alta disponibilidade; Controle de acesso dos administradores da solução; Configuração de Interfaces; Criação e gerenciamento de Zonas de Segurança, Políticas de Segurança e Endereçamento NAT; Controle por Identificação de Aplicações; Controle por Identificação de Usuários, com conexão a fontes externas de autenticação; Criação e gerenciamento de Filtro URL; Descriptografia de tráfego; Configurações de VPN (SSL e IPSec); Monitoramento e Relatórios; Log e Auditoria.
- Deverá ser fornecido certificado a cada um dos servidores públicos participantes do treinamento. A apresentação destes certificados é requisito obrigatório para a comprovação da execução do serviço, sendo o principal artefato a ser utilizado pela equipe de fiscalização contratual para validação do serviço e emissão do Termo de Recebimento Definitivo da solução.
- Todo material didático a ser utilizado deverá ser fornecido pela contratada ou pelo fabricante, devendo esse ser uma documentação oficial do próprio fabricante, impresso ou em PDF com todos os tópicos abordados no treinamento, inclusive com exemplos práticos e ilustrações.
- O instrutor deve ser profissional certificado pelo fabricante dos produtos e com experiência comprovada nos produtos fornecidos.

A critério do MAPA, o treinamento poderá ocorrer em:

- Nas instalações do MAPA. Neste caso, a contratada arcará com todas as despesas relativas e necessárias, tais como transporte, hospedagem e diárias do(s) instrutor(es); infraestrutura complementar da sala e instalações; material didático e coffee break, e demais gastos para a execução do treinamento;
- Em Brasília-DF. A contratada arcará com todas as despesas relativas e necessárias, tais como transporte, hospedagem e diárias do(s) instrutor(es); infraestrutura da sala, das instalações e equipamentos; material didático e coffee break, e demais gastos para a execução do treinamento.

4.5.7 . REQUISITOS GERAIS DO ITEM 09

- Deverá ter a característica de Zero Trust Network Access e funcionalidades para no mínimo 500 usuários **simultâneos** com os seguintes aspectos:

- Deve ser composta pelos agentes a serem instalados nas máquinas dos usuários finais, bem como por um proxy de acesso, o qual concentrará as requisições dos agentes para acesso às aplicações corporativas.
- Deve controlar o acesso por sessão, validando o usuário e dispositivo, bem como estabelecendo um túnel criptografado de modo automático para cada sessão.
- Deve prover um método para controlar o acesso, identificando o dispositivo do usuário, autenticação e postura com base em tags de Zero Trust.
- A solução de proxy de acesso deve prover suporte a um método de publicação de aplicações corporativas sem necessidade de agente, tal como mediante um portal web SSL a ser acessado por cada usuário.
- Deve permitir o gerenciamento dos agentes remotamente, a partir de uma console central do próprio fabricante a ser disponibilizada em nuvem.
- Deve ser escalável com usabilidade até até 3.000 agentes.
- O licenciamento deve se basear no número de agentes registrados na console de gerenciamento central do mesmo fabricante.
- Deve ser compatível com pelo menos os seguintes sistemas operacionais: Microsoft Windows: 7 (32 e 64 bits), 8.1 (32 e 64 bits), 10 (32 e 64 bits) e 11 (64 bits); Microsoft Windows Server: 2008 R2, 2012, 2012 R2, 2016, 2019 e 2022; Mac OS X: versões 13, 12, 11 e 10.15; Linux: Ubuntu 18.04 e posterior, Debian 11 e posterior, CentOS Stream 8, CentOS 7.4 e posterior, RedHat 7.4 e posterior, Fedora 36 e posterior.
- Deve dispor de mecanismos para analisar a requisição TLS Client hello e o cabeçalho HTTP User-Agent para determinar e controlar se a requisição está partindo de um dispositivo não passível de gerenciamento pela console central, tal como um dispositivo móvel.
- A comunicação de controle entre os agentes e a console central deve ser criptografada e acontecer através de TCP e TLS 1.2 e 1.3.
- Tanto mediante agente ou sem agente deve ser possível habilitar MFA (autenticação multifator) no processo de autenticação dos usuários.
- A console central deve emitir, assinar e instalar automaticamente um certificado para os agentes contendo ID único de cada agente, número de série do certificado e número de série da console central. O certificado emitido deverá ser único por agente e deverá ainda ser compartilhado com o proxy de acesso.
- Deve ser possível revogar o certificado de um agente por meio da console central.
- O certificado emitido deve ser utilizado no processo de autenticação via ZTNA para identificar o dispositivo do usuário final junto ao proxy de acesso.
- No passo de identificação do dispositivo mediante certificado deve ser possível averiguar se o identificador único do agente e número do certificado coincidem com o que o proxy de acesso conhece. Caso algum desses dados esteja diferente, o acesso deverá ser bloqueado por padrão.
- Deve ser possível configurar o idioma que o agente utiliza para, pelo menos, inglês, português, espanhol ou ainda usar o idioma do sistema operacional.
- A solução deve prover backup automático diariamente, permitindo que em um evento crítico seja possível restaurar os dados de até 05 dias anteriores ao ocorrido.
- Deve existir a possibilidade de restringir o usuário de realizar backup da configuração do agente.
- Deve ser possível enviar os logs para uma ferramenta de consolidação de logs do mesmo fabricante, visando consolidar os logs do proxy de acesso ZTNA em conjunto com os logs dos agentes.
- A solução deve suportar casos de uso utilizando IPv6 puro, bem como IPv6 em conjunto com IPv4.
- Deve ser possível agrupar agentes em grupos e atribuir grupos de agentes a perfis de políticas específicas.
- Deve ser possível exigir uma senha para desconectar o agente da console central.
- Deve ser possível evitar que o usuário realize shutdown do agente após estar registrado na console central.
- A console central deve apresentar um resumo das informações de cada endpoint, tais como nome do dispositivo, sistema operacional, IP privado, endereço mac, IP público, estado da conexão com a console central, zero trust tags associadas, detalhes da conexão de rede cabeada e WiFi, detalhes do hardware como modelo do dispositivo, fabricante, CPU, RAM, número de série e capacidade de armazenamento. Deve permitir ainda facilmente ver detalhes de qual política está associada com cada agente, qual versão de agente está em uso em um respectivo endpoint, número de série do agente, identificador único e número de série do certificado emitido para o processo de ZTNA.
- Deve permitir criação de regras de conformidade que avaliem à postura do dispositivo e auxiliem o administrador no controle de acesso à recursos da infraestrutura, impedindo que um cliente não conforme possa se conectar a redes críticas.
- A console central deve permitir mapear as regras de destinos de ZTNA a serem sincronizadas com os endpoints e permitir ainda definir para qual tráfego deve ser aplicada criptografia, tal como para tráfego HTTP sem criptografia nativa.
- Deve possibilitar definir funções administrativas relacionadas às permissões dos endpoints, de políticas e de configurações gerais.
- Deve permitir criação de regras de conformidade que avaliem à postura do dispositivo e auxiliem o administrador no controle de acesso à recursos da infraestrutura, impedindo que um cliente que não esteja em conformidade possa se conectar a redes críticas.

- Deve ser possível aplicar um patch automático com base no nível de criticidade definido, tal como atualizar automaticamente patches considerados críticos.
- A console central deve possuir funcionalidade de rastreamento de vulnerabilidades a nível de endpoint, permitindo ainda definir o rastreamento no momento do registro, quando ocorrer uma atualização de uma assinatura vulnerável, bem como patches e atualizações de segurança a nível de sistema operacional. Além disso, deve ser possível agendar quando o rastreamento deve ocorrer ou vinculá-lo em conjunto com a janela de manutenção automática do Windows.
- Deve ser possível configurar o filtro de URL com base em caracteres curingas ou expressões regulares (regex) com as opções de permitir, bloquear ou monitorar.

4.6 . REQUISITOS DE ARQUITETURA TECNOLÓGICA

- Os requisitos de arquitetura tecnológica dos itens da contratação estão descritos nos itens 4.5, ao longo do termo de referência e no **Anexo -Especificações técnicas da solução de TIC.**

4.7 . REQUISITOS DE PROJETO E DE IMPLEMENTAÇÃO

- Os requisitos necessários de projeto e implementação estão descritos no tópico 4.5, ao longo do termo de referência e no Anexo - Especificações técnicas da solução de TIC.

4.8 . REQUISITOS DE EXPERIÊNCIA PROFISSIONAL E DE FORMAÇÃO DA EQUIPE

- Os profissionais que irão implantar a solução de TIC (Itens 01,03,05 e 06) devem ter experiência mínima de 03 anos em implantações/configurações da solução adquirida ou similar. Os atestados que comprovem essa experiência precisam ser apresentados formalmente. Os profissionais envolvidos deverão possuir certificado/certificação ou curso oficial fornecido pelo fabricante que o credencie na implantação da solução contratada ou similar.
- Para os itens 02,04,07 e 09 da contratação também é solicitado, no mínimo, 03 anos de experiência em soluções correlatas ou de maior complexidade. A contratada deve ter profissional(is), pelo menos 01(um) profissional, com certificação, certificado ou curso oficial do fabricante que comprove o conhecimento prático nos respectivos itens da contratação.
- Já para o item 08 (treinamento) , o instrutor deve ter formação comprovada através de certificação/certificado ou curso oficial do fabricante e experiência em treinamentos de no mínimo 02 anos, devendo ser comprovado formalmente com documentos oficiais.

4.9 . REQUISITOS SOCIAIS, AMBIENTAIS E CULTURAIS

- Durante a execução de tarefas no ambiente do MAPA, os funcionários da empresa contratada deverão observar, no trato com os servidores públicos e colaboradores em geral, a urbanidade e os bons costumes de comportamento, tais como: asseio, pontualidade, cooperação, respeito mútuo, discrição e zelo com o patrimônio público.
- A documentação e os manuais de operação da solução deverão ser apresentados preferencialmente no idioma Português (Brasil – PT-BR) e, em sua ausência, deverão ser apresentados em idioma Inglês;
- A abertura de chamados técnicos e encaminhamentos de demandas deverão ser realizados, preferencialmente, sob a forma eletrônica, evitando-se a impressão de papel. Além disso, as configurações de hardware e software deverão ser realizadas visando alto desempenho com a utilização racional de energia.
- Em conformidade com a IN SLTI/MPOG n. 01/2010, a contratada deverá cumprir com os seguintes requisitos de sustentabilidade ambiental, quando aplicável:
- Que os bens sejam constituídos, no todo ou em parte, por material reciclado, atóxico, biodegradável, conforme ABNT NBR – 15448-1 e 15448-2;
- Que sejam observados os requisitos ambientais para a obtenção de certificação do Instituto Nacional de Metrologia, Normalização e Qualidade Industrial – INMETRO como produtos sustentáveis ou de menor impacto ambiental em relação aos seus similares;
- Que os bens devam ser, preferencialmente, acondicionados em embalagem individual adequada, com o menor volume possível, que utilize materiais recicláveis, de forma a garantir a máxima proteção durante o transporte e o armazenamento;
- Que os bens não contenham substâncias perigosas em concentração acima da recomendada na diretiva RoHS (Restriction of Certain HazardousSubstances), tais como mercúrio (Hg), chumbo (Pb), cromo hexavalente (Cr (VI)), cádmio (Cd), bifenilpolibromados (PBBs), éteres difenil-polibromados (PBDEs).
- É dever da Contratada observar entre outras: o menor impacto sobre recursos naturais como flora, fauna, ar, solo e água; preferência para materiais, tecnologias e matériasprimas de origem local; maior eficiência na utilização de recursos naturais; maior geração de empregos; maior vida útil e menor custo de manutenção do bem; uso de inovações que reduzam a pressão sobre recursos naturais; e origem ambientalmente regular dos recursos naturais utilizados nos bens e serviços.

- O MAPA será a responsável pela verificação da aderência aos padrões de qualidade exigidos dos produtos entregues. A Contratada será responsável pelo fornecimento do software e gestão dos recursos humanos e materiais necessários para a prestação da garantia.

4.10 .REQUISITOS DE METODOLOGIA DO TRABALHO

- A execução dos serviços está condicionada ao recebimento pela contratada da ordem de serviço (OS) emitida pelo MAPA. A OS indicará o serviço, a quantidade e a localidade na qual os serviços deverão ser prestados.
- A solução deverá estar implementada no prazo estabelecido neste termo de referência.
- A equipe do MAPA, no que couber, poderá apoiar a implantação da solução como um todo.
- Todos os serviços prestados pela contratada deverão ser realizados nas dependências do Ministério da Agricultura e Pecuária. A execução do serviço deve ser acompanhado pela contratada, que dará ciência de eventuais acontecimentos ao MAPA. Quando remoto, a infraestrutura necessária deve ser de responsabilidade da contratada.
- A contratada deve fornecer meios para contato e registro de ocorrências da seguinte forma: com funcionamento 8 horas por dia e 5 dias por semana de maneira eletrônica e 7 horas por dia e 5 dias por semana por via telefônica.
- A execução do contrato será baseada no modelo, no qual a contratante é responsável pela gestão do contrato e pelo ateste dos resultados esperados e dos níveis mínimos de serviço exigidos frente aos serviços entregues, sendo a contratada responsável pelos serviços, gestão dos recursos humanos e físicos necessários, conforme termo de referência.
- A contratada deverá se responsabilizar pelos materiais, produtos, ferramentas, instrumentos e equipamentos disponibilizados para a execução dos serviços, não cabendo à CONTRATANTE qualquer responsabilidade por perdas decorrentes de roubo, furto ou outros fatos que possam vir a ocorrer.
- A CONTRATADA não poderá transferir a outrem, no todo ou em parte, o objeto do contrato.

4.11 . REQUISITOS DE SEGURANÇA DA INFORMAÇÃO E PRIVACIDADE

Na execução dos serviços contratados, a CONTRATADA deverá zelar, no que for de sua competência, pela garantia da disponibilidade, integridade, confidencialidade e autenticidade das informações custodiadas no ambiente gerenciado. Além disso, deve adotar e se responsabilizar por medidas efetivas quanto ao seguinte:

- A contratada deverá submeter-se à Política de Segurança da Informação e Comunicações e demais normas de segurança vigentes no MAPA. (Portaria MAPA Nº 136, de 25 de Maio de 2021).
- Abster-se, qualquer que seja a hipótese, de veicular publicidade ou qualquer outra informação acerca dos serviços, sem prévia autorização. Ademais, observar, rigorosamente, todas as normas e procedimentos de segurança implementados no ambiente de Tecnologia da Informação - TI do MAPA.
- Normas e instruções normativas do GSI/PR no que se aplicar à respectiva contratação.
- Assegurar o adequado tratamento de dados pessoais e informações classificadas dos quais venha a ter conhecimento ou manusear em razão da execução do objeto do contrato, nos termos da Lei Federal n° 13.709/2018 e em aderência aos requisitos de segurança da informação vigentes no ambiente do MAPA.
- Evitar vazamento de dados e fraudes digitais nos ambientes gerenciados sob sua responsabilidade técnica.
- A contratada deverá assinar o termo de compromisso de manutenção de sigilo para fins de segurança de dados e da prestação do serviço, conforme o modelo no Anexo-Termo de compromisso de Manutenção de Sigilo (https://www.gov.br/governodigital/pt-br/contratacoes/templates-e-listas-de-verificacao).
- Os colaboradores da contratada que atuarem nos serviços iniciais e durante toda a vigência do contrato e do prazo de suporte e garantia, deverão assinar o termo de ciência, conforme o modelo no Anexo-Termo de Ciência (https://www.gov.br/governodigital/pt-br/contratacoes/templates-e-listas-de-verificacao).
- A contratada deverá obedecer, quando aplicável, as normas de segurança da família ISO/IEC 27000.
- A contratada deverá manter sigilo, sob pena de responsabilidade civil, penal e administrativa, no que diz respeito a todo e qualquer assunto de interesse do MAPA ou de terceiros de que tomar conhecimento em razão da execução do objeto deste documento, devendo orientar seus empregados nesse sentido.
- A contratada deverá manter em caráter confidencial, mesmo após o término do prazo de vigência ou rescisão do contrato, as informações de que vier ter acesso durante a execução do contrato.
- A contratada deverá implementar processo de gestão de capacidade e recursos para redundância de forma que a utilização dos recursos seja monitorada, ajustada e as projeções das necessidades de capacidade futura sejam avaliadas para garantir o desempenho dos ativos relacionados ao objeto do contrato, assegurando também a disponibilidade e recuperação de dados e informações, em conformidade com um plano de continuidade relacionado ao objeto contratado, que garanta o nível requerido de continuidade para a segurança da informação durante uma situação adversa;
- A contratada deverá manter controles e procedimentos específicos para assegurar o nível adequado de segurança da informação às redes corporativas da Contratante e da Contratada, de forma a reduzir o nível de risco ao qual a Solução de TIC e a contratante estão expostos, considerando os critérios de aceitabilidade de riscos definidos pela contratante;
- A contratada deverá implementar e manter controles específicos para registro de eventos e rastreabilidade de forma a manter trilha de auditoria de segurança da informação e privacidade, aderente a disposto em dispositivo legal correlato publicado pelo GSI/PR, de forma a assegurar a rastreabilidade do tráfego por meio de logs de transações e acessos, conforme especificação de requisitos, e gerá-los e disponibilizá-los à contratante para fins de auditorias e inspeções;

- A contratada deverá utilizar recursos de segurança da informação e de tecnologia da informação de qualidade, eficiência e eficácia reconhecidas e em versões comprovadamente seguras e atualizadas, de forma reduzir o nível de risco ao qual o objeto do contrato e/ou a contratante está exposta, considerando os critérios de aceitabilidade de riscos definidos pela contratante;
- A contratada deverá implementar e manter controles e procedimentos específicos para assegurar completo e absoluto sigilo quanto a todos os dados e informações de que o preposto ou os demais empregados da contratada venham a tomar conhecimento em razão da execução do contrato, de forma a assegurar que seus empregados e outros profissionais sob sua direção e/ou controle respeitem o uso dos dados somente para as finalidades previstas em contrato e as restrições de uso dos ativos utilizado para desenvolvimento e/ou operação da Solução de TIC, cumprindo e fazendo cumprir o disposto nos Termo de Compromisso e Termo(s) de Ciência firmados respectivamente, pelo representante legal e pelo(s) empregado(s) da contratada.
- Todas as informações, documentos e especificações técnicas as quais a contratada tiver acesso em função da execução contratual deverão ser tratadas como confidenciais, sendo vedada sua reprodução, utilização ou divulgação à terceiros, devendo essa zelar pela manutenção do sigilo absoluto do conhecimento adquirido.

4.12 . REQUISITOS DE VISTORIA TÉCNICA

- A avaliação prévia do local de execução dos serviços é imprescindível para o conhecimento pleno das condições e peculiaridades do objeto a ser contratado, sendo assegurado ao interessado o direito de realização de vistoria prévia, acompanhado por servidor designado para esse fim, de segunda à sexta-feira, das 09:00 às 12:00 / 14:00 às 17:00 horas.
- Embora opcional, é recomendável a realização de visita técnica, e esta deve ser realizada até 03 (três) dias antes da data fixada para a sessão pública, mediante agendamento prévio de acordo com os contatos da Subsecretaria de Tecnologia da Informação do MAPA através dos e-mails: coseg@agro.gov.br e/ou cginfra.sti@agro.gov.br. (Telefone 3218-2208).
- A realização da visita técnica não se consubstancia em condição para a participação na licitação, ficando, contudo, as licitantes cientes de que após a apresentação das propostas não serão admitidas, em hipótese alguma, alegações no sentido da inviabilidade de cumprir com as obrigações, em face do desconhecimento dos serviços e de dificuldades técnicas não previstas.
- Para vistoria, o representante legal da empresa ou responsável técnico deverá estar devidamente identificado, apresentando documento de identidade civil e documento expedido pela empresa comprando sua habilitação para a realização da vistoria.
- O MAPA emitirá "Declaração de Realização de Vistoria Técnica", ao qual deverá ser apresentado junto a proposta de preços, conforme Anexo-Vistoria, deste Termo de Referência para os licitantes que fizerem a vistoria.
- Caso o licitante opte por não realizar a vistoria, deverá prestar declaração formal assinada pelo responsável técnico do licitante acerca do conhecimento pleno das condições e peculiaridades da contratação (Conforme anexo-Vistoria).
- A não realização da vistoria não poderá embasar posteriores alegações de desconhecimento das instalações, dúvidas ou esquecimentos de quaisquer detalhes dos locais da prestação dos serviços, devendo o contratado assumir os ônus dos serviços decorrentes.

4.13 . DEMAIS REQUISITOS APLICÁVEIS

- As empresas licitantes deverão apresentar declaração que ateste a não ocorrência do registro de oportunidade, de modo a garantir o princípio da competitividade e a seleção da proposta mais vantajosa para a Administração Pública, conforme disposto no art. 5º da Lei no 14.133, de 2021.

5. PAPÉIS E RESPONSABILIDADES

Seguem abaixo, as responsabilidades do contratante e da contratada:

5.1 . DEVERES E RESPONSABILIDADES DO CONTRATANTE

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

- Encaminhar formalmente a demanda, preferencialmente por meio de Ordem de Serviço, de acordo com os critérios estabelecidos neste Termo de Referência.
- Receber o objeto/serviço fornecido pela contratada que esteja em conformidade com a proposta aceita, conforme inspeções realizadas.
- Verificar minuciosamente, no prazo fixado, a conformidade dos bens recebidos provisoriamente com as especificações constantes do presente Termo de Referência e da proposta da contratada, para fins de aceitação e recebimento definitivo;
- Acompanhar e fiscalizar o cumprimento das obrigações da Contratada, através de comissão/servidor especialmente designado;
- Aplicar, observando o direito ao contraditório e ampla defesa, à contratada as sanções administrativas regulamentares e contratuais cabíveis.
- Liquidar o empenho e efetuar o pagamento à contratada, dentro dos prazos preestabelecidos em contrato.
- Comunicar à contratada todas e quaisquer ocorrências relacionadas com o fornecimento da Solução de Tecnologia da Informação.
- Disponibilizar para a contratada: legislação, normas, instruções e programas de trabalho de sua competência, com o objetivo de facilitar e orientar a execução dos serviços contratados.
- Permitir à contratada os acessos a todas as áreas, instalações e equipamentos necessários ao cumprimento das tarefas e serviços previstas neste Termo de Referência.
- Prestar à contratada, em tempo hábil, as informações disponíveis e necessárias à implantação/execução dos serviços.
- Exigir, a qualquer tempo, a comprovação das condições de habilitação da contratada que ensejaram sua contratação.
- Manter a contratada informada de quaisquer atos da Administração Pública que venham a interferir direta ou indiretamente nos serviços contratados.
- Por se tratar de solução de tecnologia da informação, todas as obrigações da contratante contidas na IN SGD/ME 94 /2022 deverão ser seguidas, incluindo a emissão do TRP (Termo de Recebimento Provisório) e o TRD (Termo de Recebimento Definitivo).

5.2 . DEVERES E RESPONSABILIDADES DA CONTRATADA

- Executar os serviços e iniciar a cobertura e a execução dos serviços conforme especificações deste Termo de Referência e de sua proposta comercial, com a disponibilidade dos empregados necessários ao perfeito cumprimento das cláusulas contratuais, na qualidade e quantidade especificadas.
- 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.
- O objeto deve estar acompanhado do manual do usuário, com uma versão em português do Brasil ou inglês.
- Responsabilizar-se pelos vícios e danos decorrentes da execução dos objetos, de acordo com os artigos 14 e 17 a 27, do Código de Defesa do Consumidor (Lei nº 8.078, de 1990), ficando a Contratante autorizada a descontar dos pagamentos devidos à Contratada, o valor correspondente aos danos sofridos.
- Utilizar empregados habilitados e com conhecimentos básicos dos serviços a serem executados, em conformidade com as normas e determinações em vigor.
- 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.
- Responsabilizar-se por todas as obrigações trabalhistas, sociais, previdenciárias, tributárias e as demais previstas em legislação específica, cuja inadimplência não transfere responsabilidade ao Contratante.
- Instruir seus empregados quanto à necessidade de acatar as normas internas da Administração.
- Instruir seus empregados a respeito das atividades a serem desempenhadas, alertando-os a não executar atividades não abrangidas pelo contrato, devendo a Contratada relatar à Contratante toda e qualquer ocorrência neste senti do, a fim de evitar desvio de função.
- Relatar ao Contratante toda e qualquer irregularidade verificada no decorrer da prestação dos serviços.
- Guardar sigilo sobre todas as informações obtidas em decorrência do cumprimento do Contrato.
- Manter-se, durante toda a execução do Contrato, em compatibilidade com as obrigações assumidas, todas as condições de habilitação e qualificação exigidas para a contratação.
- Responsabilizar-se integralmente pelo fiel cumprimento dos objetos contratados, prestando todos os esclarecimentos eventualmente solicitados pela contratante, obedecendo aos parâmetros e rotinas estabelecidos de acordo com as recomendações aceitas pela boa técnica, normas e legislação vigentes.
- Executar o objeto contratado conforme as condições estipuladas neste Termo de Referência e seus Anexos, na Proposta Comercial e no Contrato.
- Indicar formalmente, no período designado pelo termo de referência, preposto e substituto aptos a representá-la junto a Contratante, os quais devem responder pela fiel execução dos serviços contratados, orientar a Equipe da Contratada, bem como comparecer às dependências da Contratante sempre que convocados.
- Não transferir a outrem, no todo ou em parte, a execução do presente Contrato.
- Atender às solicitações dos membros da Equipe de Gestão do Contrato inerentes às obrigações contratuais e/ou à prestação e/ou à gestão dos serviços.

- Comunicar formal e imediatamente ao Gestor do Contrato todas as ocorrências anormais ou de comprometimento à execução do Contrato, bem como qualquer ocorrência relevante à execução contratual.
- Efetuar de imediato o afastamento do atendimento à Contratante de qualquer empregado cuja atuação, permanência ou comportamento sejam inadequados à execução do Contrato.
- Responsabilizar-se por quaisquer encargos, despesas, taxas, inclusive de seguro, decorrentes das operações necessárias à entrega do objeto contratado.
- Reparar quaisquer danos diretamente causados à Contratante ou a terceiros, por culpa ou dolo de seus representantes legais, prepostos ou empregados, em decorrência da presente relação contratual, não excluindo ou reduzindo essa responsabilidade a fiscalização ou o acompanhamento da execução dos serviços pela Contratante.
- Observar todas as normas de segurança adotadas pelo Contratante, inclusive no que diz respeito às normas referentes ao ambiente informatizado.
- Fornecer ao Contratante, sempre que requerido formalmente, acesso aos equipamentos e sistemas necessários ao atendimento do objeto do Contrato, para averiguação da conformidade dos serviços contratados.
- Cumprir as disposições do Termo de Compromisso de Sigilo e do Termo de Ciência.
- Responsabilizar-se por todos os custos, diretos e indiretos, inclusive de transporte e de pessoal, necessários à adequada prestação dos serviços, em plena conformidade com os termos e especificações, inclusive prazos e horários previstos neste Termo de Referência e seus anexos.
- Assegurar a disponibilidade, confidencialidade e integridade dos dados, informações e sistemas informatizados, inclusive de todas as suas alterações, manuais, programas fonte e objeto, bases de dados ou outros recursos, pertencentes ao Contratante, armazenados ou residentes na Contratada.
- Registrar, tempestivamente, mediante relatório circunstanciado, todos os casos que a eximam de responsabilidade, negligência, mau uso, instalações e outros.
- Propiciar todos os meios e facilidades necessárias à fiscalização da Solução de Tecnologia da Informação pela Contratante, cujo representante terá poderes para sustar o fornecimento, total ou parcialmente, em qualquer tempo, sempre que considerar a medida necessária.
- Aceitar, nas mesmas condições contratuais, os acréscimos ou supressões que se fizerem necessários até 25% (vinte e cinco por cento) do valor inicial atualizado do Contrato;
- Apresentar fatura no valor autorizado e condições do Contrato, apresentando-a ao Contratante para ateste e pagamento após a autorização de faturamento pelo Gestor do Contrato.
- Atender as determinações do Gestor do Contrato inerentes às obrigações contratuais e/ou à prestação e/ou gestão dos serviços.
- A Contratada não poderá divulgar projetos, serviços e soluções de TIC do MAPA e Ministérios demandantes, nem falar em nome do Contratante em nenhum tipo de mídia sem prévia autorização.
- Não disponibilizar qualquer informação de propriedade do Contratante, por qualquer meio, a qualquer terceiro e para qualquer finalidade, sem anuência expressa.
- Ceder os direitos de propriedade intelectual e direitos autorais da solução de TIC sobre os diversos artefatos e produtos produzidos em decorrência da relação contratual, sendo assim o caso, incluindo a documentação, os modelos de dados e as bases de dados à Administração.
- Assumir as despesas decorrentes do transporte, hospedagem e alimentação a ser executado em função do objeto do Contrato.
- Diante de situações de irregularidades de caráter urgente deverá comunicar, por escrito, ao Contratante, as informações sobre possíveis paralisações de serviços, a apresentação de relatório técnico ou razões justificadoras a serem apreciadas e decididas pelo agente designado.
- 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).
- Não veicular publicidade ou qualquer outra informação acerca da prestação dos serviços do contrato, sem prévia autorização da contratante.
- Não fazer uso das informações prestadas pela contratante para fins diversos do estrito e absoluto cumprimento do contrato em questão.
- Indicar formalmente e por escrito, no prazo máximo de 05 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.
- Em até 48 horas corridas, devem ser enviadas informações dos funcionários desligados que estejam prestando serviço ao MAPA.

6. MODELO DE EXECUÇÃO DO CONTRATO

O modelo de execução do contrato define como o contrato deverá produzir os resultados pretendidos desde o seu início até o seu encerramento, observando, os tópicos abaixo:

6.1 . CONDIÇÕES DE EXECUÇÃO E PROCEDIMENTOS DE FORNECIMENTO DA SOLUÇÃO DE TIC

6.1.1 . REUNIÃO INICIAL

Após a assinatura do contrato e a nomeação do gestos e dos fiscais de 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.

A reunião será realizada em conformidade com o previsto no inciso I do artigo 31 da IN SGD/ME Nº94, de 2022, e ocorrerá em até 10 úteis da assinatura do contrato, podendo ser prorrogada a critério da contratante.

A pauta desta reunião observará, pelo menos:

- Presença do representante legal da contratada, que apresentará o seu preposto. 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.
- Alinhar a forma de comunicação entre as partes, que deverá ocorrer preferencialmente entre o MAPA e o preposto da contratada.
- Definir as providências necessárias para inserção da contratada no ambiente de prestação dos serviços.
- Definir as providências de implantação dos serviços.
- Esclarecimentos relativos a questões operacionais, administrativas e de gestão do contrato.
- Apresentação formal da equipe de fiscalização do contrato e do preposto. (contratante e contratada)
- Repasse à contratada de conhecimentos necessários à execução dos serviços (contratante).
- Entrega, por parte da contratada, do termo de compromisso e dos termos de ciência devidamente assinados, conforme artigo 18, inciso V da IN SGD/ME Nº 94/2022.

Havendo necessidade outros assuntos de comum interesse, poderão ser tratados na reunião inicial, além dos anteriormente previstos. Todas as atas de reuniões e as comunicações entre o MAPA e a contratada, assim como todas as demais intercorrências contratuais, positivas ou negativas, serão arquivadas em processo próprio para fins de manutenção do histórico de gestão do contrato.

6.1.2 . PRAZOS, HORÁRIOS DE FORNECIMENTO DE BENS/PRESTAÇÃO DE SERVIÇOS E LOCAIS DE ENTREGA

- Além dos prazos já citados nos requisitos temporais (item 4.4) e citados abaixo, temos outros prazos que devem ser cumpridos:

ID	DESCRIÇÃO	PRAZO MÁXIMO DE ENTREGA (DIAS ÚTEIS)
1	Assinatura do contrato.(MAPA e Contratada)	Início dos prazos - D
2	Realização da reunião inicial contendo os elementos descritos no item 6.1.1 deste termo de referência. (MAPA e contratada).	D + 4
3	Entrega do projeto da implantação (Contratada).	D + 09
4	Análise e aprovação do projeto de implantação (contratante).	D + 14
5	Finalização da execução dos serviços e instalação dos bens. (Contratada)	D + 60
6	Início do treinamento.	10 dias após o ID 5 ou a depender da disponibilidade dos recursos do MAPA.
7	Termo de Recebimento Provisório.	05 dias após a finalização do ID 5.
8	Termo de Recebimento Definitivo.	10 dias após a finalização do treinamento e ID 05,06 e 07.
9	Relatórios mensais a partir do 2º mês de instalação com o detalhamento das manutenções preventivas.	Todo 5º dia útil do mês subsequente.

- O local para fornecimento dos bens físicos e prestação dos serviços é Brasília- Distrito Federal, Esplanada dos Ministérios, Ministério da Agricultura e Pecuária-MAPA, Anexo "B" e térreo.

- A entrega dos equipamentos físicos deverão ser realizados nos dias úteis, no horário de 09:00 às 12:00 e de 14:00 às 17: 00, devendo ser agendada previamente com o MAPA.
- O transporte dos equipamentos deverá ser realizado pela contratada, inclusive os procedimentos de seguro, embalagem e transporte até o espaço alocado pelo MAPA para guarda.
- Caberá ao MAPA rejeitar no total ou em parte, os materiais entregues em desacordo com o objeto deste Termo de Referência.
- O recebimento da solução de TIC será efetivado pela equipe designada pelo MAPA e darseá da forma provisória e definitiva, conforme prazos estabelecidos no tópico 7.1.2 deste termo de referência.
- Caso não seja possível conclusão do item 05 no tempo previsto, a empresa deverá comunicar as razões respectivas com pelo menos 10 dias de antecedência para que qualquer pleito de prorrogação de prazo seja analisado, ressalvadas situações de caso fortuito e força maior.

6.1.3 . DOCUMENTAÇÃO MÍNIMA EXIGIDA

No mínimo, a Contratada deverá fornecer:

- Manuais técnicos do usuário e de referência contendo todas as informações sobre os produtos com as instruções para instalação, configuração, operação e administração.
- Documentação completa de todos os itens da contratação, incluindo especificação do equipamento, características e funcionalidades implementadas, desenho lógico da implantação, comentários e configurações executadas;
- Relatório com o detalhamento do processo realizado ao final da implantação como requisito para o aceite definitivo.
- Relatórios mensais das manutenções preventivas e relatórios dos tickets executados e seu cumprimento com os níveis mínimos de serviço.

6.1.4 . PAPÉIS E RESPONSABILIDADES, POR PARTE DO CONTRATANTE E DA CONTRATADA

Os papéis a serem designados e necessários para essa contratação estão descritos no item 7.2.5 deste termo de referência.

6.1.5 . MATERIAIS A SEREM DISPONIBILIZADOS

Para a perfeita execução dos serviços, a contratada é responsável por todos os materiais, equipamentos, ferramentas e utensílios necessários para a instalação e configuração dos bens adquiridos.

6.1.6 . INFORMAÇÕES RELEVANTES PARA O DIMENSIONAMENTO DA PROPOSTA

A demanda do órgão tem como base as seguintes características: manter a mesma arquitetura atual de firewall (a topologia está omitida por segurança) e substituir os equipamentos atuais (8 Firewalls).

6.2 . QUANTIDADE DE BENS A SEREM FORNECIDOS

A quantidade de bens e serviços a serem fornecidos estão descritos e justificado em detalhes no item 3.2 desse termo de referência.

6.3 . MECANISMOS FORMAIS DE COMUNICAÇÃO

- Toda comunicação entre o MAPA e a contratada deverá ser sempre formal como regra, exceto em casos excepcionais que justifiquem outro meio de comunicação.
- Na reunião inicial, conforme já citado no item 6.1.1, a Contratada deverá indicar formalmente preposto apto a representá-la junto ao MAPA. Esse profissional fará a interação entre o MAPA e a Contratada, e será responsável por acompanhar a execução do contrato e atuar como interlocutor principal junto ao Contratante.
- Os seguintes instrumentos formais poderão ser utilizados para a troca de informações entre a Contratante e a Contratada, sendo eles: Ordem de Serviço e ofícios enviados via SEI, Ata de Reunião, Canal de abertura de chamados, Emails, Ferramentas de colaboração do Google, por exemplo, Chat/Spaces/Meet ou outra que venha a utilizada pelo MAPA, de acordo com a natureza da informação.

Algumas das comunicações corriqueiras podem ser exemplificadas abaixo:

- **Exemplo de comunicação 01:** Autorizar a execução dos serviços, fornecimento de bens ou entrega das Licenças.
  - Documento: Ordem de Serviço.
  - Emissor: Contratante – Gestor do Contrato e Fiscal Requisitante.
  - Destinatário: Contratada.
  - Meio: eletrônico.
- **Exemplo de comunicação 02:** Abertura de chamados de suporte técnico e garantia.
  - Documento: Solicitação de abertura de chamado de suporte técnico e garantia.

    - Emissor: Contratante.
    - Destinatário: Contratada.
    - Meio: E-mail, telefone ou site na internet.
- **Exemplo de comunicação 03:** Registro das reuniões realizadas entre o Contratante e a Contratada.
    - Documento: Ata de reunião.
    - Emissor: Contratada.
    - Destinatário: Contratante.
    - Meio: eletrônico.
- **Exemplo de comunicação 04:** Dirimir dúvidas e prestar esclarecimentos acerca de itens presentes no contrato firmado.
    - Documento: Ofício e/ou relatório mensal.
    - Emissor: Contratada ou contratante.
    - Destinatário: Contratada ou contratante.
    - Meio: eletrônico com confirmação de recebimento.

6.4 . MANUTENÇÃO DE SIGILO E NORMAS DE SEGURANÇA

6.4.1 . TERMO DE COMPROMISSO / TERMO DE CIÊNCIA DA DECLARAÇÃO DE MANUTENÇÃO DE SIGILO E DAS NORMAS DE SEGURANÇA NO MAPA

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

6.5 . FORMA DE TRANSFERÊNCIA DE CONHECIMENTO

- A transferência do conhecimento se dará através do item 07(Treinamento) desta contratação.

6.6 . PROCEDIMENTOS DE TRANSIÇÃO E FINALIZAÇÃO DO CONTRATO

- Não serão necessários procedimentos de transição e finalização do contrato devido às características do objeto. Caso o MAPA sinta necessidade de solicitação de qualquer outro durante o contrato relacionado ao objeto fornecido, não deve haver recusa da contratada em fornecer repasse de conhecimento.

7. MODELO DE GESTÃO DO CONTRATO

7.1. - O contrato deverá ser executado fielmente pelas partes, de acordo com as cláusulas avençadas e as normas da Lei nº 14.133, de 2021, e cada parte responderá pelas consequências de sua inexecução total ou parcial.

7.2. - Em caso de impedimento, ordem de paralisação ou suspensão do contrato, o cronograma de execução será prorrogado automaticamente pelo tempo correspondente, anotadas tais circunstâncias mediante simples apostila.

7.3. - As comunicações entre o órgão ou entidade e o contratado devem ser realizadas por escrito sempre que o ato exigir tal formalidade, admitindo-se o uso de mensagem eletrônica para esse fim.

7.4. - O órgão ou entidade poderá convocar representante da empresa para adoção de providências que devam ser cumpridas de imediato.

7.5 - FISCALIZAÇÃO CONTRATUAL

A execução do contrato deverá ser acompanhada e fiscalizada pelo(s) fiscal(is) do contrato, ou pelos respectivos substitutos (Lei nº 14.133, de 2021, art. 117, caput), nos termos do art. 33 da IN SGD nº 94, de 2022, no que for necessário, observando-se, em especial, as rotinas a seguir:

7.5.1 - FISCALIZAÇÃO TÉCNICA

7.5.1.1 - O fiscal técnico do contrato, além de exercer as atribuições previstas no art. 33, II, da IN SGD nº 94, de 2022, acompanhará a execução do contrato, para que sejam cumpridas todas as condições estabelecidas no contrato, de modo a assegurar os melhores resultados para a Administração. (Decreto nº 11.246, de 2022, art. 22, VI).

7.5.1.2 - O fiscal técnico do contrato anotará histórico de gerenciamento do contrato todas as ocorrências relacionadas à execução do contrato, com a descrição do que for necessário para a regularização das faltas ou dos defeitos observados. (Lei nº 14.133, de 2021, art. 117, §1º, e Decreto nº 11.246, de 2022, art. 22, II).

7.5.1.2 - Identificada qualquer inexatidão ou irregularidade, o fiscal técnico do contrato emitirá notificações para a correção da execução do contrato, determinando prazo para a correção. (Decreto nº 11.246, de 2022, art. 22, III);

7.5.1.3 - O fiscal técnico do contrato informará ao gestor do contato, em tempo hábil, a situação que demandar decisão ou adoção de medidas que ultrapassem sua competência, para que adote as medidas necessárias e saneadoras, se for o caso. (Decreto nº 11.246, de 2022, art. 22, IV).

7.5.1.4 - No caso de ocorrências que possam inviabilizar a execução do contrato nas datas aprazadas, o fiscal técnico do contrato comunicará o fato imediatamente ao gestor do contrato. (Decreto nº 11.246, de 2022, art. 22, V).

7.5.1.5 - O fiscal técnico do contrato comunicará ao gestor do contrato, em tempo hábil, o término do contrato sob sua responsabilidade, com vistas à renovação tempestiva ou à prorrogação contratual (Decreto nº 11.246, de 2022, art. 22, VII).

7.5.2 - FISCALIZAÇÃO ADMINISTRATIVA

7.5.2.1 - O fiscal administrativo do contrato, além de exercer as atribuições previstas no art. 33, IV, da IN SGD nº 94, de 2022, verificará a manutenção das condições de habilitação do Contratado, acompanhará o empenho, o pagamento, as garantias, as glosas e a formalização de apostilamento e termos aditivos, solicitando quaisquer documentos comprobatórios pertinentes, caso necessário (Art. 23, I e II, do Decreto nº 11.246, de 2022).

7.5.2.2 - Caso ocorram descumprimento das obrigações contratuais, o fiscal administrativo do contrato atuará tempestivamente na solução do problema, reportando ao gestor do contrato para que tome as providências cabíveis, quando ultrapassar a sua competência; (Decreto nº 11.246, de 2022, art. 23, IV).

7.5.3 - GESTÃO DO CONTRATO

7.5.3.1 - O gestor do contrato, além de exercer as atribuições previstas no art. 33, I, da IN SGD nº 94, de 2022, coordenará a atualização do processo de acompanhamento e fiscalização do contrato contendo todos os registros formais da execução no histórico de gerenciamento do contrato, a exemplo da ordem de serviço, do registro de ocorrências, das alterações e das prorrogações contratuais, elaborando relatório com vistas à verificação da necessidade de adequações do contrato para fins de atendimento da finalidade da administração. (Decreto nº 11.246, de 2022, art. 21, IV).

7.5.3.2 - O gestor do contrato acompanhará a manutenção das condições de habilitação do Contratado, para fins de empenho de despesa e pagamento, e anotará os problemas que obstem o fluxo normal da liquidação e do pagamento da despesa no relatório de riscos eventuais. (Decreto nº 11.246, de 2022, art. 21, III).

7.5.3.3 - O gestor do contrato acompanhará os registros realizados pelos fiscais do contrato, de todas as ocorrências relacionadas à execução do contrato e as medidas adotadas, informando, se for o caso, à autoridade superior àquelas que ultrapassarem a sua competência. (Decreto nº 11.246, de 2022, art. 21, II).

7.5.3.4 - O gestor do contrato emitirá documento comprobatório da avaliação realizada pelos fiscais técnico, administrativo e setorial quanto ao cumprimento de obrigações assumidas pelo Contratado, com menção ao seu desempenho na execução contratual, baseado nos indicadores objetivamente definidos e aferidos, e a eventuais penalidades aplicadas, devendo constar do cadastro de atesto de cumprimento de obrigações. (Decreto nº 11.246, de 2022, art. 21, VIII).

7.5.3.5 - O gestor do contrato tomará providências para a formalização de processo administrativo de responsabilização para fins de aplicação de sanções, a ser conduzido pela comissão de que trata o art. 158 da Lei nº 14.133, de 2021, ou pelo agente ou pelo setor com competência para tal, conforme o caso. (Decreto nº 11.246, de 2022, art. 21, X).

7.5.3.6 - O fiscal técnico do contrato comunicará ao gestor do contrato, em tempo hábil, o término do contrato sob sua responsabilidade, com vistas à tempestiva renovação ou prorrogação contratual. (Decreto nº 11.246, de 2022, art. 22, VII).

7.5.3.7 - O gestor do contrato deverá elaborará relatório final com informações sobre a consecução dos objetivos que tenham justificado a contratação e eventuais condutas a serem adotadas para o aprimoramento das atividades da Administração. (Decreto nº 11.246, de 2022, art. 21, VI).

A avaliação da qualidade dos produtos entregues, para fins de aceitação, consiste na verificação dos critérios relacionados a seguir:

7.6 . CRITÉRIOS DE ACEITAÇÃO DOS BENS FORNECIDOS

- Todos os equipamentos fornecidos deverão ser novos (incluindo todas as peças e componentes presentes nos produtos), de primeiro uso (sem sinais de utilização anterior), não recondicionados e em fase de comercialização normal através dos canais de venda do fabricante no Brasil (não serão aceitos produtos end-of-life).
- Todos os componentes do(s) equipamento(s) e respectivas funcionalidades deverão ser compatíveis entre si e do mesmo fabricante, conforme já dito ao longo do termo de referência, sem a utilização de adaptadores, frisagens, pinturas, usinagens em geral, furações, emprego de adesivos, fitas adesivas ou quaisquer outros procedimentos não previstos nas especificações técnicas ou, ainda, com emprego de materiais inadequados ou que visem adaptar forçadamente o produto ou suas partes que sejam fisicamente ou logicamente incompatíveis.
- O número de série de cada equipamento deve ser obrigatório e único, afixado em local visível, na parte externa do gabinete e na embalagem que o contém. Esse número deverá ser identificado pelo fabricante, como válido para o produto entregue e para as condições do mercado brasileiro no que se refere à garantia e assistência técnica no Brasil.
- Serão recusados os produtos que possuam componentes ou acessórios com sinais claros de oxidação, danos físicos, sujeira, riscos ou outro sinal de desgaste, mesmo sendo o componente ou acessório considerado como novos pelo fornecedor dos produtos.
- Os produtos, considerando a marca e modelo apresentados na licitação, não poderão estar fora de linha comercial, considerando a data de licitação (abertura das propostas). Os produtos devem ser fornecidos completos e prontos para a utilização, com todos os acessórios, componentes, cabos etc.
- A Contratante poderá optar por avaliar a qualidade de todos os equipamentos fornecidos ou será realizada verificação de amostra do objeto para averiguar se a Solução de TIC apresentada pela Licitante detém os requisitos mínimos necessários para realização dos serviços a serem contratados, de acordo com as funcionalidades, procedimentos e critérios objetivos descritos no Anexo- Especificação Técnica da solução de TI deste Termo de Referência.
- Só haverá o recebimento definitivo, após a análise da qualidade dos bens e/ou serviços, em face da aplicação dos critérios de aceitação, resguardando-se ao Contratante o direito de não receber o objeto cuja qualidade seja comprovadamente baixa ou em desacordo com as especificações definidas neste Termo de Referência – situação em que poderão ser aplicadas à contratada as penalidades previstas em lei, neste Termo de Referência e no contrato. Quando for o caso, a empresa será convocada a refazer todos os serviços rejeitados, sem custo adicional.
- Para ser aceita, a solução deverá atender fidedignamente os requisitos estabelecidos neste Termo de Referência, em especial quanto ao anexo I - Especificação Técnica da Solução de TIC.

7.6.1. - Qualquer item da contratação será recusada inteiramente nas seguintes condições:

- Caso seja entregue em desconformidade com as especificações técnicas constantes deste Temo de Referência e da proposta vencedora;
- Caso apresente defeitos, em qualquer de suas partes ou componentes, durante os testes de conformidade e verificação;
- Nos casos de recusa do produto, a empresa fornecedora terá o prazo de 05 (cinco) dias úteis para providenciar a sua substituição, contados a partir da comunicação oficial feita pelo MAPA.

RECEBIMENTO DO OBJETO

7.6.2. - O objeto contratado será recebido, de forma provisóriae definitiva, conforme prevê o artigo 140 da Lei Nº 14.133 e o art. 33da Instrução Normativa N°23/2022/SGD/ME, observando o disposto a seguir:

7.6.2.1. - TERMO DE RECEBIMENTO PROVISÓRIO

- Os serviços serão recebidos provisoriamente, no prazo de 05 dias, pelos fiscais técnico e administrativo, mediante termos detalhados, quando verificado o cumprimento das exigências de caráter técnico e administrativo. (Art. 140, I e II, a , da Lei nº 14.133 e Arts. 22, X e 23, X do Decreto nº 11.246, de 2022).
- O prazo da disposição acima será contado do recebimento de comunicação de cobrança oriunda do contratado com a comprovação da prestação dos serviços e bens a que se referem a parcela a ser paga.
- O fiscal técnico do contrato realizará o recebimento provisório do objeto do contrato mediante termo detalhado que comprove o cumprimento das exigências de caráter técnico. (Art. 22, X, Decreto nº 11.246, de 2022).
- O fiscal administrativo do contrato realizará o recebimento provisório do objeto do contrato mediante termo detalhado que comprove o cumprimento das exigências de caráter administrativo. (Art. 23, X, Decreto nº 11.246, de 2022)
- O Contratado fica obrigado a reparar, corrigir, remover, reconstruir ou substituir, às suas expensas, no todo ou em parte, o objeto em que se verificarem vícios, defeitos ou incorreções resultantes da execução ou materiais empregados, cabendo à fiscalização não atestar a última e/ou única medição de serviços até que sejam sanadas todas as eventuais pendências que possam vir a ser apontadas no Recebimento Provisório.
- O recebimento provisório também ficará sujeito, quando cabível, à conclusão de todos os testes de campo e à entrega dos Manuais e Instruções exigíveis.
- Os serviços e bens poderão ser rejeitados, no todo ou em parte, quando em desacordo com as especificações constantes neste Termo de Referência e na proposta, sem prejuízo da aplicação das penalidades.

- Quando a fiscalização for exercida por um único servidor, o Termo Detalhado deverá conter o registro, a análise e a conclusão acerca das ocorrências na execução do contrato, em relação à fiscalização técnica e administrativa e demais documentos que julgar necessários, devendo encaminhá-los ao gestor do contrato para recebimento definitivo.

7.6.2.2. - TERMO DE RECEBIMENTO DEFINITIVO

- Os serviços serão recebidos definitivamente no prazo de 10 dias, contados do recebimento provisório, por servidor ou comissão designada pela autoridade competente, após a verificação da qualidade e quantidade do serviço e consequente aceitação mediante termo detalhado, obedecendo os seguintes procedimentos:
- Emitir documento comprobatório da avaliação realizada pelos fiscais técnico, administrativo e setorial, quando houver, no cumprimento de obrigações assumidas pelo contratado, com menção ao seu desempenho na execução contratual, baseado em indicadores objetivamente definidos e aferidos, e a eventuais penalidades aplicadas, devendo constar do cadastro de atesto de cumprimento de obrigações, conforme regulamento (art. 21, VIII, Decreto nº 11.246, de 2022).
- Realizar a análise dos relatórios e de toda a documentação apresentada pela fiscalização e, caso haja irregularidades que impeçam a liquidação e o pagamento da despesa, indicar as cláusulas contratuais pertinentes, solicitando à Contratada, por escrito, as respectivas correções.
- Comunicar a empresa para que emita a Nota Fiscal ou Fatura, com o valor exato dimensionado pela fiscalização.
- Enviar a documentação pertinente ao setor de contratos para a formalização dos procedimentos de liquidação e pagamento, no valor dimensionado pela fiscalização e gestão.
- No caso de controvérsia sobre a execução do objeto, quanto à dimensão, qualidade e quantidade, deverá ser observado o teor do art. 143 da Lei nº 14.133, de 2021, comunicando-se à empresa para emissão de Nota Fiscal no que concerne à parcela incontroversa da execução do objeto, para efeito de liquidação e pagamento.
- Nenhum prazo de recebimento ocorrerá enquanto pendente a solução, pelo contratado, de inconsistências verificadas na execução do objeto ou no instrumento de cobrança.
- O recebimento provisório ou definitivo não excluirá a responsabilidade civil pela solidez e pela segurança do serviço nem a responsabilidade ético-profissional pela perfeita execução do contrato.
- Só haverá o recebimento definitivo, após a análise da qualidade dos bens e/ou serviços, em face da aplicação dos critérios de aceitação, resguardando-se ao Contratante o direito de não receber o objeto cuja qualidade seja comprovadamente baixa ou em desacordo com as especificações definidas neste Termo de Referência – situação em que poderão ser aplicadas à CONTRATADA as penalidades previstas em lei, neste Termo de Referência e no CONTRATO. Quando for o caso, a empresa será convocada a refazer todos os serviços rejeitados, sem custo adicional.
- O prazo para recebimento definitivo poderá ser excepcionalmente prorrogado, de forma justificada, por igual período, quando houver necessidade de diligências para a aferição do atendimento das exigências contratuais.

7.7 . PROCEDIMENTOS DE TESTE E INSPEÇÃO

7.7.1 . DEFINIÇÃO DE MECANISMOS DE INSPEÇÃO E AVALIAÇÃO DA SOLUÇÃO / DILIGÊNCIAS (INSPEÇÃO POR AMOSTRAGEM)

O acompanhamento e a fiscalização do objeto deste Termo de Referência, bem como o atesto da entrega dos materiais adquiridos, serão exercidos por servidor , em conformidade com o disposto no art. 117 da Lei n.º 14.1333 e com as normas e resoluções internas do Órgão. O acompanhamento e a fiscalização serão realizados sob o aspecto quantitativo e qualitativo, devendo ser anotadas em registro próprio dos fiscais as falhas detectadas.

As irregularidades detectadas pela fiscalização serão imediatamente comunicadas ao fornecedor, por escrito, para correção ou adequação.

7.7.2 . ORIGEM E FORMAS DE OBTENÇÃO DAS INFORMAÇÕES NECESSÁRIAS À GESTÃO E FISCALIZAÇÃO DO CONTRATO / ACOMPANHAMENTO DE INDICADORES

- A origem das informações necessárias à gestão e fiscalização do contrato serão as comunicações entre o preposto e a equipe de fiscalização técnica do contrato. Todas as demais informações geradas ao longo do contrato também servem de base para a fiscalização contratual.
- Não é necessário nenhum software específico para acompanhar os indicadores, sendo os relatórios e plataforma de abertura de tickets suficientes para uma fiscalização contratual eficaz.

7.7.3 . DEFINIÇÃO DE LISTAS DE VERIFICAÇÃO E DE ROTEIROS DE TESTES PARA SUBSIDIAR A AÇÃO DOS FISCAIS DO CONTRATO

- O MAPA reserva-se ao direito de promover avaliações, inspeções e diligências visando esclarecer quaisquer situações relacionadas à prestação dos serviços contratados, sendo obrigação da contratada acolhê-las.
- A inspeção nos equipamentos fornecidos será realizada por meio de comparação das especificações constantes dos prospectos do fabricante do equipamento.

7.7.4 . DISPONIBILIDADE DE RECURSOS HUMANOS NECESSÁRIOS ÀS ATIVIDADES DE GESTÃO E FISCALIZAÇÃO DO CONTRATO / PAPÉIS E RESPONSABILIDADES, POR PARTE DO CONTRATANTE E DA CONTRATADA

A execução do contrato deverá ser acompanhada e fiscalizada pelo(s) fiscal(is) do contrato, ou pelos respectivos substitutos (Lei nº 14.133, de 2021, art. 117, caput) nos termos do artigo 33 da IN SGD Nº 94 de 2022, e para cumprir as atividades de gestão e fiscalização do contrato, o MAPA designará servidores (titulares e substitutos) para executar os seguintes papéis:

7.7.4.1. - DO CONTRATANTE-MAPA

- **Gestor do Contrato: S**ervidor com atribuições gerenciais, preferencialmente da Área Requisitante da solução, designado para coordenar e comandar o processo de gestão e fiscalização da execução contratual, indicado por autoridade competente. Outras atribuições estão listadas no inciso I do artigo 33 da IN SGD/ME Nº 94/2022.
- **Fiscal Técnico:** Servidor representante da Área de Tecnologia da Informação, indicado pela autoridade competente dessa área para fiscalizar tecnicamente o contrato. Outras atribuições estão listadas no inciso II do artigo 33 da IN SGD /ME Nº 94/2022.
- **Fiscal Requisitante:** Servidor representante da Área Requisitante da Solução, indicado pela autoridade competente dessa área para fiscalizar o contrato do ponto de vista funcional da Solução de Tecnologia da Informação. Outras atribuições estão listadas no inciso III do artigo 33 da IN SGD/ME Nº 94/2022.
- **Fiscal administrativo:** Servidor representante da Área Administrativa, indicado pela autoridade competente dessa área para fiscalizar o contrato quanto aos aspectos administrativos. Outras atribuições estão listadas no inciso IV do artigo 33 da IN SGD/ME Nº 94/2022.

7.7.4.2. - DA CONTRATADA

- **Preposto:** Representante da contratada, responsável por 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. A indicação ou a manutenção do preposto da empresa poderá ser recusada pelo órgão ou entidade, desde que devidamente justificada, devendo a empresa designar outro para o exercício da atividade.
- **Profissionais da Contratada:** Funcionário(s) representante(s) da contratada, responsável(is) por executar as atividades /serviços contratados.

7.8 . PROCEDIMENTOS PARA RETENÇÃO OU GLOSA NO PAGAMENTO

7.8.1 . NÍVEIS MÍNIMOS DE SERVIÇO/INDICADORES

Para permitir que a gestão contratual esteja alinhada com a gestão da qualidade dos serviços prestados, foram estabelecidos indicadores de desempenho mínimos para a execução dos serviços contratados. Assim, os resultados serão medidos com base em indicadores vinculados a fórmulas de cálculo específicas, apurados temporalmente e continuamente monitorados, objetivando o cumprimento das metas estabelecidas. Este conceito vincula-se ao novo modelo de contratação de soluções de Tecnologia da Informação na Administração Pública Federal, no qual os serviços serão remunerados considerando parâmetros de qualidade e entrega efetiva de resultados.

Os indicadores são instrumentos práticos de aferição do cumprimento do alcance dos níveis mínimos de serviço, evidenciando de maneira objetiva e mensurável o desempenho e as tendências de um serviço demandado. Relaciona-se a seguir o conjunto mínimo de indicadores proposto para a presente contratação, pautado no incentivo para a redução de ocorrências que impactam o negócio do MAPA e também incentivem a boa prestação dos serviços:

INDICADOR A

TÓPICO	DESCRIÇÃO
Finalidade	Este indicador tem a finalidade de medir a carga horária completa do treinamento.
Meta a cumprir	Atender 100% da carga horária mínima do treinamento.
Instrumento de medição	Recebimento dos certificados pelo equipe de fiscalização contratual.
Periodicidade	Única.
Faixa de ajuste	

no pagamento	Redução de 5% sobre o valor do item 8 a cada 1 hora menor de treinamento.

Demais instrumentos de medição da qualidade de entrega do serviços estão destacados no item 7.6.

7.8.2 . PROCEDIMENTOS PARA APLICAÇÃO DE GLOSA NO PAGAMENTO

Nos termos do art. 19, inciso III da Instrução Normativa SGD/ME nº 94, de 2022, será efetuada a retenção ou glosa no pagamento, proporcional à irregularidade verificada, sem prejuízo das sanções cabíveis, nos casos em que o contratado:

- Não atingir os valores mínimos aceitáveis fixados nos critérios de aceitação, não produzir os resultados ou deixar de executar as atividades contratadas; ou
- Deixar de utilizar materiais e recursos humanos exigidos para fornecimento da solução de TIC, ou utilizá-los com qualidade ou quantidade inferior à demandada;

A aplicação de descontos/glosas em função do descumprimento de critérios de qualidade, avaliação de resultados e/ou níveis mínimos de serviço exigidos não concorre com a aplicação (concomitante ou não) das sanções administrativas previstas em contrato, inclusive daquelas previstas em função do reiterado descumprimento dos critérios de qualidade do serviço, sendo essa uma prerrogativa da Administração.

Além das reduções de valores relacionados aos indicadores, serão aplicadas glosas em função das pontuações diretamente atribuídas ao descumprimento dos termos de serviço determinados da tabela abaixo, sendo as ocorrências apuradas, sempre que necessário. As glosas serão aplicadas sem prejuízo de outras sanções administrativas por descumprimento de obrigações contratuais e estão incluídas no limite máximo de 30% do pagamento à contratada.

REDUÇÃO NO PAGAMENTO DE ACORDO COM OS REQUISITOS GERAIS DO TERMO DE REFERÊNCIA			
ID	**DESCRIÇÃO**	**REFERÊNCIA**	**GLOSA**
01	Atraso de qualquer prazo descrito nos requisitos temporais.	Por ocorrência.	1ª ocorrência - Glosa de 0,2% por dia de atraso sobre o valor total do contrato.
02	Atraso na resolução de atendimento de ticket superior ao prazo estabelecidos em mais de 07 dias úteis.	Por ocorrência.	1ª ocorrência - Glosa de 0,2% por dia de atraso sobre o valor total do contrato. 2ª ocorrência - Glosa de 0,4% por dia de atraso sobre o valor total do contrato.
03	Não utilizar mão de obra qualificada e tecnicamente habilitada para o atendimento.	Por ocorrência.	1ª ocorrência - Glosa de 0,25% sobre o valor total do contrato. 2ª ocorrência - Glosa de 0,5% sobre o valor total do contrato. 3ª ocorrência - Glosa de 1,0% sobre o valor total do contrato.
04	Deixar de comunicar qualquer anormalidade técnica de caráter urgente para o contratante.	Por ocorrência.	1ª ocorrência - Glosa de 0,5% sobre o valor total do contrato. 2ª ocorrência - Glosa de 0,75% por dia de atraso sobre o valor total do contrato. 3ª ocorrência - Glosa de 1,0% por dia de atraso sobre o valor total do contrato.

05	Não comparecer, injustificadamente, à reunião inicial.	Por ocorrência.	1ª ocorrência - Glosa de 0,25% sobre o valor total do contrato. 2ª ocorrência - Glosa de 0,5% sobre o valor total do contrato.
06	Provocar a indisponibilidade dos equipamentos ou comprometer a confidencialidade, integridade e indisponibilidade da solução.	Por ocorrência.	1ª ocorrência - Glosa de 0,5% sobre o valor total do contrato. 2ª ocorrência - Glosa de 0,75% sobre o valor total do contrato. 3ª ocorrência - Glosa de 1,0% sobre o valor total do contrato.
07	Deixar de cumprir os requisitos de segurança.	Por ocorrência.	1ª ocorrência - Glosa de 0,5% sobre o valor total do contrato. 2ª ocorrência - Glosa de 0,75% sobre o valor total do contrato. 3ª ocorrência - Glosa de 1,0% sobre o valor total do contrato.
08	Não substituir os equipamentos 01, 03, 06 e 09 nos prazos máximos especificados.	Por ocorrência.	1ª ocorrência - Glosa de 0,5% sobre o valor total do contrato. 2ª ocorrência - Glosa de 0,75% sobre o valor total do contrato. 3ª ocorrência - Glosa de 2% sobre o valor total do contrato.
09	Em até 48 horas, enviar as informações dos funcionários que forem desligados da contratada.	Por ocorrência.	1ª ocorrência - Glosa de 0,5% sobre o valor total do contrato. 2ª ocorrência - Glosa de 0,75% sobre o valor total do contrato. 3ª ocorrência - Glosa de 1,0% sobre o valor total do contrato.
10	Não entregar e não cumprir 100% das atividades de manutenção preventiva mensal.	Por ocorrência.	1ª ocorrência - Glosa de 0,35% sobre o valor total do contrato. 2ª ocorrência - Glosa de 0,55% sobre o valor total do contrato. 3ª ocorrência - Glosa de 1,0% sobre o valor total do contrato.
11	Não atender 96% dos tickets de todas as severidades atendidos dentro do prazo.	Por ocorrência.	1ª ocorrência - Glosa de 0,5% sobre o valor total do contrato. 2ª ocorrência - Glosa de 0,75% sobre o valor total do contrato. 3ª ocorrência - Glosa de 1,0% sobre o valor total do contrato.

7.9 . SANÇÕES ADMINISTRATIVAS

A finalidade das sanções administrativas em licitações e contratos é reprovar a conduta praticada pelo sancionado, desestimular a sua reincidência, bem como prevenir sua prática futura pelos demais licitantes e contratados. As sanções podem ter caráter preventivo, educativo, repressivo ou visar à reparação de danos pelos responsáveis que causem prejuízos ao erário público. Trata-se, portanto, de um poder-dever da Administração que deve atuar visando impedir ou minimizar os danos causados pelos licitantes e contratados que descumprem suas obrigações.

As reduções previstas no período de adaptação não se estendem para as hipóteses de aplicação de sanções.As sanções administrativas fixadas nas normas, aplicadas aos licitantes e contratada, são as seguintes:

A) Advertência. B) Multa. C) Impedimento de licitar e contratar. D) Declaração de inidoneidade para licitar ou contratar.

As sanções “advertência”, “impedimento de licitar e contratar” e “declaração inidoneidade ou contratar” poderão ser aplicadas cumulativamente com a sanção de multa.

7.9.1 – ADVERTÊNCIA

A sanção de advertência será aplicada exclusivamente pela infração administrativa prevista no inciso I do caput do art. 155 desta Lei Nº 14.1333, quando não se justificar a imposição de penalidade mais grave.

7.9.2 - MULTA

A sanção de multa tem natureza pecuniária e sua aplicação se dará na gradação prevista neste instrumento quando houver atraso injustificado no cumprimento da obrigação contratual e em decorrência da inexecução parcial ou total do objeto da contratação nos termos do artigo 162 da Lei Nº 14.133. As sanções de advertência, suspensão e inidoneidade poderão ser aplicadas juntamente com a multa, conforme § 7º do art. 156 de Lei nº 14.133. As MULTAS serão aplicadas considerando os seguintes níveis de gradação:

GRAU DE INFRAÇÃO	**GRAVIDADE**	**MULTA CORRESPONDENTE**	**LIMITE DE INFRAÇÕES POR VIGÊNCIA CONTRATUAL**
INFRAÇÃO A	Conduta indesejada com baixo impacto na realização dos objetivos da contratação.	0,5% sobre o valor global do contrato.	Até 06 (seis) infrações, consecutivas ou não.
INFRAÇÃO B	Conduta prejudicial, impacta a prestação dos serviços de maneira leve, mas não compromete a realização dos objetivos da contratação.	1,0% sobre o valor global do contrato.	Até 04 (quatro) infrações, consecutivas ou não.
INFRAÇÃO C	Conduta danosa, impacta a prestação dos serviços de maneira mediana ou compromete a realização dos objetivos da contratação.	2,5% sobre o valor global do contrato.	Até 02 (duas) infrações, consecutivas ou não.
INFRAÇÃO D	Conduta grave, compromete fortemente a realização dos objetivos da contratação.	3,5 % sobre o valor global do contrato.	Até 01(uma) infração.
Importante: Ao exceder o limite máximo admitido de infrações durante a vigência contratual para o respectivo nível de gradação estabelecido, ou mediante o reiterado descumprimento de critérios de qualidade e/ou níveis mínimos de serviço exigidos, o MAPA deverá avaliar a possibilidade de promover a rescisão do contrato em função da inexecução total ou parcial do objeto, da perda de suas funcionalidades e da comprovada			

desconformidade com os critérios mínimos de qualidade exigidos – ressalvada a aplicação adicional de outras sanções administrativas cabíveis.

A contratada estará sujeita à aplicação de multa, de acordo com os respectivos níveis de gradação acima descritos, quando for observada a ocorrência dos seguintes eventos:

EVENTOS DE REFERÊNCIA PASSÍVEIS DE APLICAÇÃO DE MULTAS		
ITEM	**DESCRIÇÃO DO EVENTO INFRACIONAL**	**GRAU DA INFORMAÇÃO**
01	Dar causa à inexecução parcial do contrato.	INFRAÇÃO B
02	Dar causa à inexecução parcial do contrato que cause grave dano à Administração, ao funcionamento dos serviços públicos ou ao interesse coletivo.	INFRAÇÃO C
03	Dar causa à inexecução total do contrato.	INFRAÇÃO D
04	Deixar de entregar a documentação exigida para o certame.	INFRAÇÃO B
05	Não manter a proposta, salvo em decorrência de fato superveniente devidamente justificado.	INFRAÇÃO B
06	Não celebrar o contrato ou não entregar a documentação exigida para a contratação, quando convocado dentro do prazo de validade de sua proposta.	INFRAÇÃO C
07	Ensejar o retardamento da execução ou da entrega do objeto da licitação sem motivo justificado.	INFRAÇÃO C
08	Apresentar declaração ou documentação falsa exigida para o certame ou prestar declaração falsa durante a licitação ou a execução do contrato.	INFRAÇÃO D
09	Fraudar a licitação ou praticar ato fraudulento na execução do contrato.	INFRAÇÃO D
10	Comportar-se de modo inidôneo ou cometer fraude de qualquer natureza.	INFRAÇÃO D
11	Praticar atos ilícitos com vistas a frustrar os objetivos da licitação.	INFRAÇÃO D
12	Praticar ato lesivo previsto no art. 5º da Lei nº 12.846, de 1º de agosto de 2013.	INFRAÇÃO D

7.9.3 – IMPEDIMENTO DE LICITAR E CONTRATAR

A sanção prevista será aplicada ao responsável pelas infrações administrativas previstas nos incisos II, III, IV, V, VI e VII do **caput** do art. 155 Da Lei Nº 14.133, quando não se justificar a imposição de penalidade mais grave, e impedirá o responsável de licitar ou contratar no âmbito da Administração Pública direta e indireta do ente federativo que tiver aplicado a sanção, pelo prazo máximo de 3 (três) anos.

7.9.4 – DECLARAÇÃO DE INIDONEIDADE PARA LICITAR E CONTRATAR

A sanção prevista será aplicada ao responsável pelas infrações administrativas previstas nos incisos VIII, IX, X, XI e XII do **caput** do art. 155 da Lei Nº 14.133, bem como pelas infrações administrativas previstas nos incisos II, III, IV, V, VI e VII do **caput** do artigo 156 que justifiquem a imposição de penalidade mais grave que a sanção referida no § 4º deste mesmo artigo, e impedirá o responsável de licitar ou contratar no âmbito da Administração Pública direta e indireta de todos os entes federativos, pelo prazo mínimo de 3 (três) anos e máximo de 6 (seis) anos.

A sanção de "Declaração de inidoneidade para licitar ou contratar" será precedida de análise jurídica e observará as seguintes regras:

I - quando aplicada por órgão do Poder Executivo, será de competência exclusiva de ministro de Estado, de secretário estadual ou de secretário municipal e, quando aplicada por autarquia ou fundação, será de competência exclusiva da autoridade máxima da entidade.

7.10 . LIQUIDAÇÃO

- Recebida a Nota Fiscal ou documento de cobrança equivalente, correrá o prazo de dez dias úteis para fins de liquidação, na forma desta seção, prorrogáveis por igual período, nos termos do art. 7º, §2º da Instrução Normativa SEGES/ME nº 77 /2022.
- Para fins de liquidação, o setor competente deverá verificar se a nota fiscal ou instrumento de cobrança equivalente apresentado 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 respectivo de execução do contrato;
    - O valor a pagar; e
    - Eventual destaque do valor de retenções tributárias cabíveis.

- Havendo erro na apresentação da nota fiscal ou instrumento de cobrança equivalente, ou circunstância que impeça a liquidação da despesa, esta ficará sobrestada até que o contratado providencie as medidas saneadoras, reiniciando-se o prazo após a comprovação da regularização da situação, sem ônus ao contratante.
- A nota fiscal ou instrumento de cobrança equivalente deverá ser obrigatoriamente acompanhado 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. 68 da Lei nº 14.133, de 2021.
- A Administração deverá realizar consulta ao SICAF para: a) verificar a manutenção das condições de habilitação exigidas no edital; b) identificar possível razão que impeça a participação em licitação, no âmbito do órgão ou entidade, que implique proibição de contratar com o Poder Público, bem como ocorrências impeditivas indiretas.
- Constatando-se, junto ao SICAF, a situação de irregularidade do contratado, 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 do contratante.
- Não havendo regularização ou sendo a defesa considerada improcedente, o contratante deverá comunicar aos órgãos responsáveis pela fiscalização da regularidade fiscal quanto à inadimplência do contratado, 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.
- Persistindo a irregularidade, o contratante deverá adotar as medidas necessárias à rescisão contratual nos autos do processo administrativo correspondente, assegurada ao contratado a ampla defesa.
- Havendo a efetiva execução do objeto, os pagamentos serão realizados normalmente, até que se decida pela rescisão do contrato, caso o contratado não regularize sua situação junto ao SICAF.

7.11 . PRAZO DE PAGAMENTO

- O pagamento será efetuado no prazo de até 10 (dez) dias úteis contados da finalização da liquidação da despesa, conforme seção anterior, nos termos da Instrução Normativa SEGES/ME nº 77, de 2022.
- No caso de atraso pelo Contratante, os valores devidos ao contratado serão atualizados monetariamente entre o termo final do prazo de pagamento até a data de sua efetiva realização, mediante aplicação do índice de correção monetária através 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 efevo pagamento;
VP = Valor da parcela a ser paga.
I = Índice de compensação financeira = 0,00016438, assim apurado:

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

7.12 . FORMA DE PAGAMENTO

- Os itens 01,03,05,06 e 08 serão pagos depois da execução, comprovação e fiscalização dos serviços, após o Termo de recebimento definitivo, em parcela única. Os itens 02,04,07 e 09, no primeiro ano, terão pagamentos junto aos itens citados anteriormente. Entretanto, esses mesmos itens, a partir do segundo ano terão pagamento anuais.
- O pagamento será realizado por meio de ordem bancária, para crédito em banco, agência e conta corrente indicados pelo contratado.
- Será considerada data do pagamento o dia em que constar como emitida a ordem bancária para pagamento.
- Quando do pagamento, será efetuada a retenção tributária prevista na legislação aplicável.
- Independentemente do percentual de tributo inserido na planilha, quando houver, serão retidos na fonte, quando da realização do pagamento, os percentuais estabelecidos na legislação vigente.
- O contratado regularmente optante pelo Simples Nacional, nos termos da Lei Complementar nº 123, de 2006, não sofrerá a retenção tributária quanto aos impostos e contribuições abrangidos por aquele regime. No entanto, o pagamento ficará condicionado à apresentação de comprovação, por meio de documento oficial, de que faz jus ao tratamento tributário favorecido previsto na referida Lei Complementar.
- Comunicar a empresa para emissão de Nota Fiscal no que pertinente à parcela incontroversa da execução do objeto, para efeito de liquidação e pagamento, quando houver controvérsia sobre a execução do objeto, quanto à dimensão, qualidade e quantidade, conforme o art. 143 da Lei nº 14.133, de 2021.
- O valor relativo à parcela antecipada(caso seja necessário) e não executada do contrato será atualizado monetariamente pela variação acumulada do ICTI, ou outro índice que venha a substituí-lo, desde a data do pagamento da antecipação até a data da devolução.
- A liquidação ocorrerá de acordo com as regras do tópico respectivo deste instrumento.
- O pagamento será efetuado no prazo máximo de até 30 dias contados do recebimento do recebimento da nota fiscal.
- É admitida a cessão fiduciária de direitos creditícios com instituição financeira, nos termos e de acordo com os procedimentos previstos na Instrução Normativa SEGES/ME nº 53, de 8 de Julho de 2020, conforme as regras deste presente tópico.
    - As cessões de crédito não fiduciárias dependerão de prévia aprovação do contratante.

8. ESTIMATIVA DE PREÇOS DA CONTRATAÇÃO

8.1. - O custo estimado total da contratação é de **R$ 7.424.115,44** (Sete milhões, quatrocentos e vinte e quatro mil, cento e quinze reais e quarenta e quatro centavos centavos), conforme custos unitários apostos na tabela abaixo:

GRUPO	ITEM	ESPECIFICAÇÃO	QTDE	VALOR UNITÁRIO Estimado
ÚNICO	**1**	Appliances físicos - Firewall - Solução de plataforma de segurança, denominada Next Generation Firewall (NGFW), com licenciamento incluso.	01	R$ 1.462.696,00
	2	Suporte, garantia e manutenção do item 01.	01	R$ 1.502.986,12
	3	Appliances físicos - Firewall - Solução de plataforma de segurança, denominada Next Generation Firewall (NGFW).	03	R$ 559.120,00 (Valor Unitário) R$ 1.677.360,00 (valor total do item 3)
	4	Suporte, garantia e manutenção do item 03.	01	R$ 2.106.985,12
	5	Serviço de instalação e configuração dos firewalls NGFW dos itens 01 e 03.	01	R$ 223.237,26
	6	Appliance - Plataforma de gestão e monitoramento centralizado, com licenciamento, instalação e	01	R$ 118.072,29

		configuração.		
	7	Suporte, garantia e Manutenção do item 06.	01	R$ 52.986,32
	8	Treinamento ministrado por profissional certificado pelo fabricante.	01	R$ 62.896,12
	9	Plataforma de ZTNA - Zero Trust Network Access.	01	R$ 216.896,21
Valor total estimado para o primeiro ano de contrato (Sete milhões, quatrocentos e vinte e quatro mil, cento e quinze reais e quarenta e quatro centavos)				**R$ 7.424.115,44**
Do segundo ano até o quinto, apenas os itens 02,04,07 e 09 serão pagos de forma anual, conforme estimativas constantes no item cronograma físico-financeiro. (Quatro milhões, cento e doze mil, seiscentos e quarenta e cinco reais)				**R$ 4.112.645,00**

9. ADEQUAÇÃO ORÇAMENTÁRIA E CRONOGRAMA

9.1. - As despesas decorrentes da presente contratação correrão à conta de recursos específicos consignados no Orçamento Geral da União.

9.2. - A contratação será atendida pela seguinte dotação:

- Programa de Governo: 0032 - Programa de Gestão e Manutenção do Poder Executivo Federal.
- Ação Orçamentária: 2000 - Administração da Unidade
- Plano Orçamentário: 0009 - Gestão e Manutenção de Soluções e Processos de Tecnologia da Informação
- Fonte Orçamentária: 100
- Plano Interno: PROGESTÃO

9.3. - Cronograma Físico Financeiro

A seguir, estima-se o cronograma de execução Físico-Financeira:

GRUPO	**ITEM**	**DESCRIÇÃO**	**QTDE**	**PREVISÃO DE DESEMBOLSO**				
				1º ANO	**2º ANO**	**3º ANO**	**4º ANO**	**5º ANO**
ÚNICO	**1**	Appliance físico - Firewall - Solução de plataforma de segurança em cluster, denominada Next Generation Firewall (NGFW), com licenciamento incluso.	01	R$ 1.462.696,00	-	-	-	-
	2	Suporte, garantia e manutenção do item 01.	01	R$ 1.502.986,12	R$ 1.593.165,29	R$ 1.688.755,20	R$ 1.790.080,52	R$ 1.897.485,35
	3	Appliance físico - Firewall - Solução de plataforma de segurança em cluster, denominada Next Generation Firewall (NGFW), com licenciamento incluso.	03	R$ 1.677.360,00	-	-	-	-
	4	Suporte, garantia e manutenção do item 03.	01	R$ 2.106.985,12	R$ 2.2233.404,23	R$ 2.367.408,48	R$ 2.509.452,99	R$ 2.660.020,17
	5	Serviço de instalação e configuração dos firewalls NGFW dos itens 01 e 03.	01	R$ 223.237,26	-	-	-	-
	6	Appliance- Plataforma de gestão e monitoramento centralizado, com licenciamento, instalação e configuração.	01	R$ 118.072,29	-	-	-	-
	7	Suporte, garantia e manutenção do item 06.	01	R$ 52.986,32	R$ 56.165,50	R$ 59.535,43	R$ 63.107,55	R$ 66.894,01
	8	Treinamento ministrado por profissional certificado pelo fabricante.	01	R$ 62.896,12	-	-	-	-

	9	Plataforma de ZTNA - Zero Trust Network Access.	01	R$ 216.896,21	R$ 229.909,98	R$ 243.704,58	R$ 258.326,86	R$ 273.826,47
TOTAL POR ANO ESTIMADO				**R$ 7.424.115,44**	**R$ 4.112.645,00**	**R$ 4.359.403,70**	**R$ 4.620.967,92**	**R$ 4.898.225,99**
TOTAL ESTIMADO PARA 05 ANOS				**R$ 25.415.358,04**				
Os pagamentos serão conforme os requisitos temporais, recebimento do objeto e critérios de aceitação de bens fornecidos, tópicos estes discriminados ao longo do termo de referência. Não há como determinar com exatidão as datas acima. Para as estimativas de desembolsos do segundo ao quinto ano, estamos considerando um reajuste anual do ICTI de 6%.								

10. REAJUSTE CONTRATUAL

10.1 - Os preços inicialmente contratados são fixos e irreajustáveis no prazo de um ano contado da data do orçamento estimado em 30.06.2023.

10.2 - Após o interregno de um ano, e independentemente de pedido do contratado, os preços iniciais serão reajustados, mediante a aplicação, pelo contratante, do Índice de Custos de Tecnologia da Informação - ICTI, mantido pela Fundação Instituto de Pesquisa Econômica Aplicada - IPEA, exclusivamente para as obrigações iniciadas e concluídas após a ocorrência da anualidade.

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

10.4 - No caso de atraso ou não divulgação do(s) índice (s) de reajustamento, o Contratante pagará ao Contratado a importância calculada pela última variação conhecida, liquidando a diferença correspondente tão logo seja(m) divulgado(s) o(s) índice(s) definitivo(s).

10.5 - Nas aferições finais, o(s) índice(s) utilizado(s) para reajuste será(ão), obrigatoriamente, o(s) definitivo(s).

10.6 - Caso o(s) índice(s) estabelecido(s) para reajustamento venha(m) a ser extinto(s) ou de qualquer forma não possa(m) mais ser utilizado(s), será(ão) adotado(s), em substituição, o(s) que vier(em) a ser determinado(s) pela legislação então em vigor.

10.7 - 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.

10.8 - O reajuste será realizado por apostilamento.

11. CRITÉRIOS DE SELEÇÃO DO FORNECEDOR

11.1 . REGIME E MODALIDADE DA CONTRATAÇÃO

- A contratação para execução indireta de serviços será realizada pelo regime de "**empreitada por preço global"**, quando se contrata a execução da obra ou do serviço por preço certo e total – conforme descrito na alínea a do inc. II do artigo 46 da Lei Nº 14.133.
- A adjudicação por preço global se deve ao fato de que todos os equipamentos e serviços estão intrinsecamente relacionados. A execução dos serviços por mais de uma empresa acarretaria elevado custo de administração e uma complexa rede de coordenação entre os projetos e, certamente, comprometeria a qualidade e efetividade dos resultados para o MAPA. A divisão do objeto a ser licitado em itens pode acarretar prejuízos quanto à instalação, configuração e operacionalização de todo o sistema, bem como sua manutenção, uma vez que se exige total compatibilidade entre os equipamentos da solução a ser adquirida, ou seja, a instalação tem que ser uniforme.
- O Item levou em consideração questões técnicas, sem prejuízo a ampla competitividade, uma vez que existem no mercado várias empresas com capacidade de fornecer os produtos na forma em que estão agrupados neste TR.
- Ademais, não será aplicado o disposto no Art. 8º do Decreto nº 8.538 de 06 de outubro de 2015, considerando a inviabilidade técnica e econômica para o parcelamento do objeto da presente contratação, bem como consideradas as suas respectivas peculiaridades, interdependência e natureza acessória entre as parcelas do objeto.

11.1.1 . NATUREZA DOS SERVIÇOS

- Os serviços a serem contratados enquadram-se nos pressupostos do Decreto Nº 9.507 de 21 de Setembro de 2018, constituindo-se em " serviços auxiliares, instrumentais ou acessórios " à área de competência legal do órgão licitante, não inerentes às categorias funcionais abrangidas por seu respectivo plano de cargos.

- Ainda, o objeto deste termo de referência se caracteriza como serviço de natureza continuada em função da sua essencialidade e habitualidade para o MAPA, ou seja, uma eventual paralisação desses serviços pode implicar sérios prejuízos às atividades do MAPA. Nos termos do art. 15 da IN 05/SEGES/MPDG de 26/05/2017, "os serviços prestados de forma contínua são aqueles que, pela sua essencialidade, visam atender à necessidade pública de forma permanente e contínua, por mais de um exercício financeiro, assegurando a integridade do patrimônio público ou o funcionamento das atividades finalísticas do órgão ou entidade, de modo que sua interrupção possa comprometer a prestação de um serviço público ou o cumprimento da missão institucional".
- Quanto ao tipo de serviço, em conformidade com a lei Nº 14.133, com o Decreto n° 5.450/2005 e com o art. 14 da IN 05 /SEGES/MPDG de 26/05/2017, o objeto pretendido enquadra-se como "**Serviço 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".
- Por fim, a prestação de serviços não envolve "dedicação exclusiva de mão de obra" – nos termos do art. 17 da IN 05 /SEGES/MPDG de 26/05/2017 – uma vez que a contratada poderá compartilhar os recursos humanos e materiais disponíveis para execução simultânea de outros contratos – embora para a execução de determinados itens do serviço seja exigida a Presencialidade do executor ,o atendimento aos requisitos de adequada capacitação profissional, entre outros. A prestação dos serviços não gera vínculo empregatício entre os empregados da contratada e a Administração, vedando-se qualquer relação entre estes que caracterize pessoalidade e subordinação direta**.**

11.1.2 . TIPO DA CONTRATAÇÃO/CRITÉRIO DE JULGAMENTO

- Considerando a natureza dos serviços e o disposto no § único do art. 25 da IN SGD/ME n°94 de 23 de dezembro de 2022,, a licitação será realizada na modalidade **PREGÃO, sob a forma ELETRÔNICA, tendo como critério de julgamento, menor preço (Valor nominal, literal, expresso)** para a seleção da proposta mais vantajosa, utilizado para compras e serviços de modo geral e para contratação de bens e serviços de informática**.** A fundamentação pauta-se na premissa que a contratação de serviços se baseia em padrões de desempenho e qualidade claramente definidos no Termo de Referência, havendo diversos fornecedores capazes de prestá-los, caracterizando-se como "serviço comum" conforme Art. 9º, §2º do Decreto 7.174/2010.
- O modo de disputa deverá ser **ABERTO** com lances decrescentes respeitando o descrito na Lei 14.133, de 2021 em seu artigo 56, § 3º.

11.3 . JUSTIFICATIVA PARA A APLICAÇÃO DO DIREITO DE PREFERÊNCIA E MARGENS DE PREFERÊNCIA

- Não se aplica o disposto no art. 6º do Decreto nº 8.538/2015, que regulamenta a LC nº 123/2006, para fins de exclusividade de participação de microempresas e empresas de pequeno porte, tendo em vista que o valor previsto para a presente licitação excede o valor estipulado no decreto supra.
- No tocante aos critérios de desempate previstos na LC nº 123/2006, regulamentada pelo Decreto nº 8.538/2015, estes serão observados e disciplinados no edital.
- Em atenção ao Acórdão 1352/2018 – TCU – Plenário, que orienta aos órgãos integrantes do Sistema de Serviços Gerais (Sisg), quando da contratação de serviços de tecnologia da informação associados ao fornecimento ou locação de bens, que devem ser aplicadas as regras de preferência dispostas no Decreto nº 7.174, de 12 de maio de 2010, tais critérios serão observados e disciplinados no edital.

EXIGÊNCIAS DE HABILITAÇÃO

Para fins de habilitação, deverá o licitante comprovar os seguintes requisitos abaixo:

11.4 . CRITÉRIOS DE QUALIFICAÇÃO TÉCNICA PARA A HABILITAÇÃO

- Todas as especificações técnicas dos itens 01 ao 09 do Anexo – Especificação Técnica da Solução de TI 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.
- As empresas deverão comprovar a 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, nos termos definidos a seguir:
- **Atestado de capacidade técnicaoperacional ou a Declaração** emitida pelo fabricante do equipamento, comprovando que a licitante é apta a instalar, configurar, prestar garantia/manutenção e ministrar treinamentos das soluções referente a esta contratação. Além disso, Considerando que além da declaração específica do fabricante atestando que a licitante é distribuidora ou revenda autorizada a comercializar os itens da contratação, também é possível apresentar outra forma de comprovação, tais como contratos de adesão que autorizem a venda ou a transferência dos direitos de uso ((TCU-Acórdão/Plenário nº 3031/2008).
- **Atestado de capacidade técnicaoperacional**, em nome da licitante, expedido por pessoa jurídica de direito público ou privado, que comprovem a execução de no mínimo 36 meses, em contrato único ou separado, serviços de solução de

segurança de perímetro contemplando o hardware, software, licenciamento, implantação, configuração, treinamento, garantia, atualizações e suporte técnico, conforme exigências deste Termo de Referência e seus anexos.

- Declaração de que possuirá durante a vigência do contrato, 02 (dois) profissionais com a certificação de Engenheiro da solução de Firewall ou superior.
- Os atestados deverão referirse a serviços prestados no âmbito de sua atividade econômica principal ou secundária especificadas no contrato social vigente.
- A empresa licitante deverá apresentar atestado(s) que comprove, no mínimo, atendimento à 50% dos quantitativos previstos para o item 03, envolvendo suporte, garantia e manutenção. (e 50% em relação ao Threat Protection Throughput ou nome equivalente em relação aos itens 01 e 03).
- A licitante deverá comprovar experiência mínima de 3 (três) anos nas soluções de Next Generation Firewall, podendo ser aceito o somatório de atestados de períodos diferentes, não havendo obrigatoriedade do período de três anos ser ininterrupto.
- Ter fornecido Next Generation Firewall similar ao ofertado, solução de acesso remoto seguro similar ao ofertado, solução de gerência centralizada similar ao ofertado e treinamento oficial similar à solução ofertada. Por solução similar, entende-se por solução do mesmo fabricante com características similares ao da contratação em questão. O modo de comprovação deve ser por meio de atestados.

a) Entende-se, para fins deste Termo de Referência, como pertencente ao quadro permanente do licitante, na data prevista para entrega da proposta, o sócio que comprove seu vínculo por intermédio de contrato/estatuto social; o administrador ou o diretor; o empregado devidamente registrado em Carteira de Trabalho e Previdência Social; e o prestador de serviços com contrato escrito firmado com o licitante, ou com declaração de compromisso de vinculação futura, caso o licitante se sagre vencedor do certame.

- É facultada a instauração de diligência destinada a esclarecer ou a confirmar a veracidade das informações prestadas pela licitante constantes de sua Comprovação de Capacidade Técnica, Proposta de Preços e de eventuais documentos anexados.
- A 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 VIIA da IN SEGES/MPDG n. 5 /2017.

Por fim, A licitante será considerada tecnicamente habilitada se restar inequivocamente comprovado atender integralmente ao disposto nos critérios técnicos de habilitação, dessa forma:

1. Tenha apresentado proposta de preços em conformidade com o atendimento dos requisitos estabelecidos no item 12.6;
2. Tenha apresentado Declaração de vistoria técnica ou declaração de opção por não realização de vistoria técnica em conformidade com o atendimento dos requisitos estabelecidos no item 4.12 .
3. Tenha comprovado sua capacidade técnico-operacional através da apresentação de Atestados de capacidade técnica que atendam aos requisitos estabelecidos no item 12.4.

11.5 - QUALIFICAÇÃO ECONÔMICA-FINANCEIRA

11.5.1 - Certidão negativa de falência expedida pelo distribuidor da sede do fornecedor - Lei nº 14.133, de 2021, art. 69, caput, inciso II).

11.5.2 - Balanço patrimonial, demonstração de resultado de exercício e demais demonstrações contábeis dos 2 (dois) últimos exercícios sociais, comprovando;

- Índices de Liquidez Geral (LG), Liquidez Corrente (LC), e Solvência Geral (SG) superiores a 1 (um);
- As empresas criadas no exercício financeiro da licitação deverão atender a todas as exigências da habilitação e poderão substituir os demonstrativos contábeis pelo balanço de abertura.
- Os documentos referidos acima limitar-se-ão ao último exercício no caso de a pessoa jurídica ter sido constituída há menos de 2 (dois) anos;
- Os documentos referidos acima deverão ser exigidos com base no limite definido pela Receita Federal do Brasil para transmissão da Escrituração Contábil Digital - ECD ao Sped.

11.5.3 - As empresas criadas no exercício financeiro da licitação deverão atender a todas as exigências da habilitação e poderão substituir os demonstrativos contábeis pelo balanço de abertura. (Lei nº 14.133, de 2021, art. 65, §1º).

11.5.4 - O atendimento dos índices econômicos previstos neste item deverá ser atestado mediante declaração assinada por profissional habilitado da área contábil, apresentada pelo fornecedor.

11.5.5 - As empresas criadas no exercício financeiro da licitação deverão atender a todas as exigências da habilitação e poderão substituir os demonstrativos contábeis pelo balanço de abertura. (Lei nº 14.133, de 2021, art. 65, §1º).

11.6 . HABILITAÇÃO FISCAL, SOCIAL E TRABALHISTA

- Prova de inscrição no Cadastro Nacional de Pessoas Jurídicas ;
- 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 de outubro de 2014, do Secretário da Receita Federal do Brasil e da Procuradora-Geral da Fazenda Nacional.
- Prova de regularidade com o Fundo de Garantia do Tempo de Serviço (FGTS);
- 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;
- Prova de inscrição no cadastro de contribuintes Distrital relativo ao domicílio ou sede do fornecedor, pertinente ao seu ramo de atividade e compatível com o objeto contratual;
- Prova de regularidade com a Fazenda Distrital do domicílio ou sede do fornecedor, relativa à atividade em cujo exercício contrata ou concorre;
- Caso o fornecedor seja considerado isento dos tributos Distrital relacionados ao objeto contratual, deverá comprovar tal condição mediante a apresentação de declaração da Fazenda respectiva do seu domicílio ou sede, ou outra equivalente, na forma da lei.
- O fornecedor 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.

11.7 . PROPOSTA

- A proposta de preços não deverá ter prazo de validade inferior a 60 (sessenta) dias corridos, a partir da data da sessão pública.
- 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 bem como toda a documentação necessária para comprovação dos requisitos que trata o anexo-Especificação Técnica da Solução de TI.
- A licitante deverá declarar, no momento de sua proposta, que possui capacidade técnica adequada para executar o objeto da licitação, atendendo aos critérios de qualidade e aos níveis de serviço exigidos, e também cumprindo os requisitos especificados para a presente contratação.
- Nos preços cotados deverão estar incluídas todas as despesas direta e indiretamente envolvidas na execução dos serviços, tais como transporte, seguros, salários, encargos sociais, encargos fiscais e taxas comerciais, impostos, taxas de contribuição, tarifas públicas e quaisquer outros custos, quando aplicáveis, necessários ao integral cumprimento do objeto contratado. Deverão estar contidos ainda todos os custos marginais referentes aos profissionais designados para a prestação dos serviços, tais como deslocamentos, hospedagens, treinamentos etc.
- A proposta deverá ser redigida em Língua Portuguesa (pt-BR), salvo quanto às expressões técnicas de uso corrente, sem emendas, rasuras ou entrelinhas, devidamente datada, sendo clara e precisa, sem alternativas de preços ou qualquer outra condição que induza o julgamento a ter mais de um resultado, com todos os preços expressos em REAIS (R$) e declaração expressa de que os serviços ofertados atendem aos requisitos técnicos especificados no termo de referência.
- Se houver indícios de que as propostas de preços apresentadas pelas Licitantes tornem o contrato inexequível em todas ou em parte das exigências de cumprimento de obrigações contratuais, ou em caso da necessidade de esclarecimentos complementares, caberá à contratante, ao longo do processo licitatório ou a qualquer tempo, solicitar às mesmas Licitantes a demonstração de exequibilidade do contrato. Estas deverão apresentar justificativas e comprovações em relação aos custos do projeto, embasando, portanto, a decisão do MAPA a respeito da desclassificação da proposta. Caso a demonstração da exequibilidade seja insuficiente, o MAPA poderá adotar os procedimentos previstos no Anexo II da IN Nº 05/2017 - SLTI/MPDG.
- A comprovação da capacidade de atendimento a este percentual representa o mínimo razoável e compatível, em quantidades e características, para demonstrar a capacidade técnica do futuro fornecedor em prestar a integralidade dos serviços, de forma simultânea, assegurando a quantidade necessária de recursos e pessoas qualificadas para atendimento ao volume previsto nesta contratação, com garantia da qualidade e dos níveis mínimos de serviço desejados, nos termos dos incisos I e II, art. 67 da Lei nº 14.133, sendo permitido o somatório de atestados, conforme já exposto.
- Descrever individualmente e com clareza a marca, o modelo, Part Numbers, as quantidades, os valores e outras informações aplicáveis e necessárias à perfeita caracterização de cada um dos itens ofertados, assim como de todos os seus componentes expansíveis, opcionais ou que possam oferecer variação de configuração de forma a permitir a correta identificação destes na documentação técnica apresentada, obedecidas as especificações contidas neste termo de referência e seus Anexos.
- Para a solução ofertada devem ser enviados: manuais, catálogos, folhetos, impressos ou publicações originais do fabricante, formando formulário para avaliação técnica, constando a identificação e página do documento onde se encontra descrita cada uma das funcionalidades e características técnicas descritas neste termo de referência.

11.8 . PARTICIPAÇÃO DE CONSÓRCIOS E COOPERATIVAS

- É vedada a participação de empresas em consórcio ou cooperativas; qualquer que sua forma de constituição, considerando as características específicas da contratação dos serviços a serem fornecidos, que não pressupõem multiplicidade de atividades empresariais distintas para execução do objeto.

11.9 . ADMISSIBILIDADE E LIMITES DA SUBCONTRATAÇÃO

- É vedada a subcontratação em parte ou total do objeto licitado.

11.10 . VERIFICAÇÃO DE AMOSTRA DO OBJETO

- A possibilidade de verificação de amostra, tem previsão no artigo 17, §3º, artigo 41, inciso II, e artigo 42, §2º, todos da Lei nº 14.133, de 2021, e no artigo 12, § 1º da IN SGD/ME nº 94, de 2022. Portanto, como são equipamentos de altos valores, o Ministério poderá solicitar amostra se assim desejar.
- Para fins de aceitação pelo MAPA, este Ministério poderá solicitar amostra para aferir as funcionalidades dos equipamentos em testes de bancada. Os itens de performance serão comprovados mediante datasheet ou declaração do fabricante em casos excepcionais. Os testes de bancada são destinados, exclusivamente, a dirimir dúvidas dos demais participantes do certamente licitatório, quando suscitadas, sobre as capacidades dos equipamentos que serão entregues pelo participante vencedor do certame. Os testes de bancadas consistirão em:
    - Aferição da capacidade de throughput de tráfego descriptografado pelo equipamento a ser testado.
    - Aferição da capacidade de trhoughput de inspeção de tráfego SSL do equipamento a ser testado.
    - Aferição das especificações técnicas (portas de comunicação, capacidade de processamento, memórias estáticas e volátil) do equipamento a ser testado.
    - Capacidades do software do equipamento a ser testado.

- Os critérios mínimos de aceitação serão os seguintes:

    - Relativamente aos testes de throughput, o equipamento testado deve apresentar, no mínimo, 95% da capacidade declarada, considerado o fato de que se trata de uma simulação em ambiente controlado.
    - Todas as funcionalidades de software devem corresponder às declaradas pelo fabricante em sua plenitude.
- O ambiente para realização dos testes, bem como os cenários de testes, serão providenciados pelo vencedor do certamente, e devem ser passíveis de inspeção quanto às configurações e capacidades por todos os atores envolvidos – Mapa e demais licitantes interessados. O vencedor do certamente deverá assegurar que todos os interessados possam realizar a inspeção do ambiente e acompanhar os testes in-loco.
- Caso seja comprovado o não atendimento das especificações mínimas nos testes de bancada, serão considerados inabilitados e sujeitos às sanções previstas em lei.
- Apresentação e avaliação da amostra seja oportunizada na fase de julgamento, podendo gerar a desclassificação do licitante provisoriamente classificado em primeiro lugar se a amostra não for apresentada no prazo ou se for reprovada nos testes de bancada.
- Para fins de comprovação de atendimento das especificações técnicas, a empresa declarada provisoriamente vencedora do certame licitatório deverá realizar a demonstração do teste de bancada em sua dependência preferencialmente em Brasília, o equipamento para ser testado no prazo de até 30 (trinta) dias corridos após a realização do processo licitatório.
    - Caso os testes não sejam realizados em Brasília, cabe a empresa provisoriamente classificada em primeiro lugar, arcar com as despesas de viagem do time de avaliação do MAPA.
- Estes testes visam verificar se o produto ofertado atende às especificações requeridas no ambiente de produção real.
- A proponente classificada deverá indicar na sua proposta comercial, após o final da disputa de lances, a composição da sua equipe técnica. Tal equipe será a responsável pela realização do teste de conformidade e deverá ser composta por até 5 (cinco) técnicos ou representantes legais da proponente, do fabricante da solução ou de empresa especializada na realização de testes de bancada. As demais licitantes participantes do pregão poderão acompanhar os testes de bancada. Para isso, deverão informar previamente ao MAPA, indicando até 2 (dois) técnicos ou representantes legais (seus ou do fabricante da solução), sendo de sua responsabilidade acompanhar os prazos e datas junto ao MAPA.
- Não será permitida a substituição de qualquer dos componentes da equipe técnica da proponente convocada ou da equipe técnica de acompanhamento sem a autorização prévia do MAPA. O Firewall, gerenciamento e demais equipamentos necessários à execução do teste de bancada deverão ser instalados, configurados, operados e acessados pela Equipe Técnica da licitante convocada, sempre acompanhada e supervisionada por analistas e técnicos da Tecnologia da Informação (TI) do MAPA.
- Para qualquer dúvida que surja deverá ser utilizada a especificação do edital e termo de referência para dirimi-la. A não observância do item acima poderá acarretar no reinício do Teste de Bancada, sem concessão de prazo adicional, ou mesmo na reprovação da solução ofertada.
- Os testes devem ser realizados com uma unidade do firewall, não sendo permitido utilizar duas caixas para atingir o dobro de performance.

- Se a equipe técnica da proponente não conseguir ativar alguma funcionalidade solicitada durante os testes de bancada, o equipamento será considerado reprovado.
- Todo e qualquer custo de equipamento, software e equipe técnica disponibilizados para a realização dos testes é de responsabilidade da proponente.
- O conceito de amostra para o referido teste é o conjunto que consiste em um firewall NGFW de modelo igual ao da solução de alta disponibilidade ofertada, mais a solução de gerenciamento centralizado que compõe a solução, com todos os módulos licenciados e habilitados.
- A proponente deve prover, além da amostra, toda a infraestrutura necessária (equipamentos e cabos de conectividade de rede, equipamentos de geração de tráfego e ameaças, appliances, servidores de virtualização, desktops, todos os softwares e licenças de utilização e demais acessórios) para a completa instalação e execução do teste de bancada.
- Todos os equipamentos e produtos que compõem a amostra da solução ofertada deverão estar acompanhados de seus respectivos programas, CDs, manuais, guias de instalação e demais documentos necessários para dirimir dúvidas, a fim de que possam ser realizados procedimentos de verificação de conformidade com as especificações técnicas constantes do edital.
- O conjunto de equipamentos especializados de geração de tráfego e ameaças deve ser capaz de simular pelo menos 100 aplicações.
- A licitante convocada deverá fornecer, em meio eletrônico ou digital, juntamente com a proposta comercial e a documentação obrigatória, a relação de ameaças (ataques, vírus, malwares, etc.) e aplicações (Skype, TeamViewer, BitTorrent, etc.) que podem ser detectados pela solução ofertada, em sua versão mais atualizada, incluindo suas classificações de severidade e de precisão e esforço de detecção.
- Preparação inicial, a ser realizada no início da fase de execução:
    - A amostra deve ser inicialmente submetida a procedimento de “factory reset”, “factory default” ou equivalente.
    - A amostra deve então ser atualizada para a versão mais atual de firmware, software, listas de assinaturas e afins disponíveis pelos canais oficiais de suporte técnico do fabricante da solução. Caso a versão do sistema operacional atual tenha menos de 4 (quatro) meses de liberação de uso para o mercado, será admitida a utilização da versão imediatamente anterior.
    - Deverão ser aplicadas todas as correções, patches, fixes e afins recomendados pelo fabricante da solução em seus canais oficiais de suporte técnico. Não serão aceitas versões, correções ou afins em estágios de testes (versões alfa e beta, release candidates, early availability, etc.).
- Não serão aceitas correções, patches, fixes e afins que não tenham previsão de serem incorporados em futuras versões do firmware ou software da solução ofertada.
- O firewall e demais equipamentos devem ser instalados e configurados de forma a simular uma arquitetura de rede.

12. GARANTIA CONTRATUAL

12.1. - O adjudicatário, no prazo de 10 (dez) dias após a assinatura do termo de contrato, prestará garantia no valor correspondente a 6,5% (seis e meio por cento) do valor global do contrato, que será liberada de acordo com as condições previstas neste Edital, conforme disposto no art. 100 da Lei Nº 14.133 de 2021, desde que cumpridas as obrigações contratuais.

12.2. - O CONTRATADO apresentará, no prazo máximo de 10 (dez) dias úteis, prorrogáveis por igual período, a critério do contratante, contado da assinatura do contrato, comprovante de prestação de garantia, podendo optar por caução em dinheiro ou títulos da dívida pública ou, ainda, pela fiança bancária, em valor correspondente a 6,5% (seis e meio por cento) do valor anual do contrato.

12.3. - 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). O atraso superior a 25 (vinte e cinco) dias autoriza o MAPA a promover a rescisão do contrato por descumprimento ou cumprimento irregular de suas cláusulas, conforme disposto na Lei nº 14.133.

12.4. - 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/MPDG nº 5/2017. A garantia assegurará, qualquer que seja a modalidade escolhida, o pagamento de:
a) Prejuízos advindos do não cumprimento do objeto do contrato ou multas;
b) Prejuízos diretos causados à Administração decorrentes de culpa ou dolo durante a execução do contrato; Multas moratórias e punitivas aplicadas pela Administração à contratada.

12.5. - A modalidade seguro-garantia somente será aceita se contemplar todos os eventos indicados no item anterior, observada a legislação que rege a matéria. O garantidor não é parte legítima para figurar em processo administrativo instaurado pelo MAPA com o objetivo de apurar prejuízos e/ou aplicar sanções à contratada (cfe. IN nº 05/2017).

12.6. - A garantia em dinheiro deverá ser efetuada em favor do MAPA. 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 MAPA, e avaliados pelos seus valores econômicos, conforme definido pelo Ministério da Fazenda. No caso de garantia na modalidade de fiança bancária, deverá constar expressa renúncia do fiador aos benefícios do artigo 827 do Código Civil.

12.7. - 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. 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 05 (cinco) dias úteis, contados da data em que for notificada.

12.8. - O MAPA executará a garantia na forma prevista na legislação que rege a matéria. Será considerada extinta a garantia:
a) Com a devolução da apólice, carta fiança ou autorização para o levantamento de importâncias depositadas em dinheiro a título de garantia, acompanhada de declaração do MAPA, mediante termo circunstanciado, de que a contratada cumpriu todas as cláusulas do contrato;
b) 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 "h" do item 3.1 do Anexo VII-F da IN SEGES/MP n° 05/2017.

12.9. A contratada autoriza o MAPA a reter, a qualquer tempo, a garantia, na forma prevista neste termo de referência e no contrato.

13. EQUIPE DE PLANEJAMENTO DA CONTRATAÇÃO

13.1. - A Equipe de Planejamento da Contratação foi instituída pela Portaria nº 18, de 28 de março de 2023 CGAQ/MAPA (SEI Nº 27579550).

13.2. - Certificamos que as diretrizes estabelecidas no termo de referência são as adequadas ao atendimento do interesse público envolvido, estando compatíveis com o estudo técnico preliminar da contratação. Além disso, o instrumento contém todos os elementos necessários para a caracterização da contratação, conforme disposição do art. 3º, inciso XI do Decreto nº 10.024, de 2019.

13.3. - Além disso, certificamos, ainda, que as especificações técnicas previstas neste Termo de Referência atendem às premissas contidas na IN SGD/ME Nº 04, de 23 de Dezembro de 2022.

13.4. - Por fim, conforme o §6º do art. 12 da IN SGD/ME Nº 94 de 2022, o Termo de Referência será assinado pela Equipe de Planejamento da Contratação, pela autoridade máxima da Área de TIC e aprovado pela autoridade competente.

14. Responsáveis

Todas as assinaturas eletrônicas seguem o horário oficial de Brasília e fundamentam-se no §3º do Art. 4º do Decreto nº 10.543, de 13 de novembro de 2020.

THIAGO PEREIRA DA COSTA

Membro da comissão de contratação

Assinou eletronicamente em 18/09/2023 às 15:20:36.

MARCO ANTONIO BITTENCOURT SUCUPIRA

Membro da comissão de contratação

Assinou eletronicamente em 19/09/2023 às 10:29:34.

CARLA CRISTIANE DE ABREU OLIVEIRA

Membro da comissão de contratação

Assinou eletronicamente em 19/09/2023 às 14:28:37.

CAMILO MUSSI

Autoridade competente

Assinou eletronicamente em 19/09/2023 às 15:23:00.

Lista de Anexos

Atenção: Apenas arquivos nos formatos ".pdf", ".txt", ".jpg", ".jpeg", ".gif" e ".png" enumerados abaixo são anexados diretamente a este documento.

- Anexo I - Ordem de Serviço.docx (32.03 KB)
- Anexo II - Termo de Ciência.docx (29.51 KB)
- Anexo III - Termo de Recebimento Provisório.docx (32.81 KB)
- Anexo IV - Termo de Recebimento Definitivo.docx (34.06 KB)
- Anexo V - Anexo-Vistoria.docx (8.61 KB)
- Anexo VI - Termo-de-compromisso-de-manutencao-do-sigilo.pdf (229.65 KB)
- Anexo VII - Anexo-Especificação Técnica da Solução de TI 05.09.2023.pdf (164.08 KB)

<ESPAÇO DESTINADO À IDENTIFICAÇÃO DO ÓRGÃO/ENTIDADE>

ATENÇÃO!

< Os trechos marcados em vermelho neste documento são editáveis, notas explicativas ou exemplos, devendo ser substituídos ou excluídos, conforme necessidade>.

<Conforme **ACÓRDÃO 172/2021 – TCU -PLENÁRIO**, os órgãos e entidades federais têm o dever legal de realizar o planejamento prévio de cada contratação de TIC, inclusive daquelas viabilizadas mediante adesão a ARPs, que vai além do mero preenchimento formal dos artefatos previstos na legislação>.

ORDEM DE SERVIÇO OU DE FORNECIMENTO DE BENS

INTRODUÇÃO
Por intermédio da Ordem de Serviço (OS) ou Ordem de Fornecimento de Bens (OFB) será solicitado formalmente à Contratada a prestação de serviço ou o fornecimento de bens relativos ao objeto do contrato. O encaminhamento das demandas deverá ser planejado visando a garantir que os prazos para entrega final de todos os bens e serviços estejam compreendidos dentro do prazo de vigência contratual. **Referência: Art. 32 IN SGD Nº 94/2022.**

1 – IDENTIFICAÇÃO			
Nº da OS/OFB	xxxx/aaaa	**Data de emissão**	<dd/mm/aaaa>
CONTRATO/NOTA DE EMPENHO 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>		

<ESPAÇO DESTINADO À IDENTIFICAÇÃO DO ÓRGÃO/ENTIDADE>

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 – <INSTRUÇÕES/ESPECIFICAÇÕES> COMPLEMENTARES
<Incluir instruções complementares à execução da OS/OFB> <Ex.: Contatar a área solicitante para agendamento do horário de entrega> <Ex.: Conforme consta no Termo de Referência, o recebimento provisório está condicionado à entrega do código no ambiente de homologação, e a documentação do software no repositório oficial de gestão de projetos>

4 – 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>

5 – ARTEFATOS / PRODUTOS	
Fornecidos	**A serem gerados e/ou atualizados**

<ESPAÇO DESTINADO À IDENTIFICAÇÃO DO ÓRGÃO/ENTIDADE>

5 – ASSINATURA E ENCAMINHAMENTO DA DEMANDA

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

_____	_____
<Nome >	<Nome >
<Responsável pela demanda/ Fiscal Requisitante>	**Gestor do Contrato**
Matr.: <Nº da matrícula>	Matr.: <Nº da matrícula>

<Local>, xx de xxxxxxxxx de xxxx

<ESPAÇO DESTINADO À IDENTIFICAÇÃO DO ÓRGÃO/ENTIDADE>

Histórico de Revisões

Data	Versão	Descrição	Autor
DD/MM/AAAA	1.0	Primeira versão do documento.	XXXXXXXXXXX

ATENÇÃO!

< Os trechos marcados em vermelho neste documento são editáveis, notas explicativas ou exemplos, devendo ser substituídos ou excluídos, conforme necessidade>.

<Conforme **ACÓRDÃO 172/2021 – TCU -PLENÁRIO**, os órgãos e entidades federais têm o dever legal de realizar o planejamento prévio de cada contratação de TIC, inclusive daquelas viabilizadas mediante adesão a ARPs, que vai além do mero preenchimento formal dos artefatos previstos na legislação>.

<ESPAÇO DESTINADO À IDENTIFICAÇÃO DO ÓRGÃO/ENTIDADE>

TERMO DE CIÊNCIA

INTRODUÇÃO
O Termo de Ciência visa obter o comprometimento formal dos empregados da Contratada diretamente envolvidos na contratação quanto ao conhecimento da declaração de manutenção de sigilo e das normas de segurança vigentes no órgão/entidade. No caso de substituição ou inclusão de empregados da contratada, o preposto deverá entregar ao Fiscal Administrativo do Contrato os Termos de Ciência assinados pelos novos empregados envolvidos na execução dos serviços contratados. **Referência: Art. 18, Inciso V, alínea "b" da IN SGD/ME Nº 94/2022.**

1 – IDENTIFICAÇÃO			
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.**	xxxxxxxxxxxxx

2 – CIÊNCIA

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

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

<Local>, <dia> de <mês> de <ano>.

<ESPAÇO DESTINADO À IDENTIFICAÇÃO DO ÓRGÃO/ENTIDADE>

Histórico de Revisões

Data	Versão	Descrição	Autor
DD/MM/AAAA	1.0	Primeira versão do documento.	XXXXXXXXXXX

ATENÇÃO!

< Os trechos marcados em vermelho neste documento são editáveis, notas explicativas ou exemplos, devendo ser substituídos ou excluídos, conforme necessidade>.

<Conforme **ACÓRDÃO 172/2021 – TCU -PLENÁRIO**, os órgãos e entidades federais têm o dever legal de realizar o planejamento prévio de cada contratação de TIC, inclusive daquelas viabilizadas mediante adesão a ARPs, que vai além do mero preenchimento formal dos artefatos previstos na legislação>.

<Nas contratações de licenciamento de softwares, é imprescindível verificar se toda a documentação entregue pela contratada está completa e corresponde exatamente ao que foi especificado no TR. É fundamental certificar-se de que todas as licenças, suporte e/ou garantia entregues estejam de acordo com os **part numbers** especificados no TR>.

<ESPAÇO DESTINADO À IDENTIFICAÇÃO DO ÓRGÃO/ENTIDADE>

TERMO DE RECEBIMENTO PROVISÓRIO – COMPRAS DE TIC

INTRODUÇÃO
O Termo de Recebimento Provisório declarará, de forma sumária, que as compras foram entregues, para verificação posterior da conformidade do material com as exigências contratuais, baseada nos requisitos e nos critérios de aceitação definidos no Modelo de Gestão do Contrato. **Referência: Inciso XXI, art. 2º, e alínea "i", inciso II, art. 33 da IN SGD/ME Nº 94/2022.**

1 – IDENTIFICAÇÃO			
CONTRATO/NOTA DE EMPENHO Nº	xx/aaaa		
CONTRATADA	<Nome da Contratada>	**CNPJ**	xxxxxxxxxxxx
Nº DA OFB	<xxxx/aaaa>		
DATA DA EMISSÃO	<dd/mm/aaaa>		

2 – ESPECIFICAÇÃO DOS PRODUTO(S)/BEM(S) E VOLUMES DE EXECUÇÃO			
SOLUÇÃO DE TIC			
<Descrição da solução de TIC solicitada relacionada ao contrato anteriormente identificado>			
ITEM	**DESCRIÇÃO DO BEM OU SERVIÇO**	**MÉTRICA**	**QUANTIDADE**
1	<Descrição igual ao da OFB de abertura>	<Ex.: UNID.>	<n>
...	...	...	...
...	...	...	...
...	...	...	...
TOTAL DE ITENS			

<ESPAÇO DESTINADO À IDENTIFICAÇÃO DO ÓRGÃO/ENTIDADE>

3 – RECEBIMENTO

Para fins de cumprimento do disposto no art. 33, inciso II, alínea "i", da IN SGD/ME nº 94/2022, por este instrumento ATESTO que os <bem(s)/produto(s)> correspondentes à <OFB> acima identificada, conforme definido no Modelo de Execução do contrato supracitado, foram entregues, estando sujeitos à avaliação específica para verificação do atendimento às demais exigências contratuais, de acordo com os Critérios de Aceitação previamente definidos no Modelo de Gestão do contrato.

Ressaltamos que o recebimento definitivo destes <bem(s)/produto(s)> ocorrerá somente após a verificação desses requisitos e das demais condições contratuais, desde que não se observem inconformidades ou divergências quanto às especificações constantes do Termo de Referência e do Contrato acima identificado que ensejem correções por parte da **CONTRATADA**. Por fim, reitera-se que o objeto poderá ser rejeitado, no todo ou em parte, quando estiver em desacordo com o contrato.

4 – ASSINATURA

FISCAL TÉCNICO

_____
<Nome do Fiscal Técnico do Contrato>
Matrícula: xxxxxx

<Local>, <dia> de <mês> de <ano>.

PREPOSTO

_____
<Nome do Preposto do Contrato>
Matrícula: xxxxxx

<Local>, <dia> de <mês> de <ano>.

<ESPAÇO DESTINADO À IDENTIFICAÇÃO DO ÓRGÃO/ENTIDADE>

Histórico de Revisões

Data	Versão	Descrição	Autor
DD/MM/AAAA	1.0	Primeira versão do documento.	XXXXXXXXXXX

ATENÇÃO!

< Os trechos marcados em vermelho neste documento são editáveis, notas explicativas ou exemplos, devendo ser substituídos ou excluídos, conforme necessidade>.

<Conforme **ACÓRDÃO 172/2021 – TCU -PLENÁRIO**, os órgãos e entidades federais têm o dever legal de realizar o planejamento prévio de cada contratação de TIC, inclusive daquelas viabilizadas mediante adesão a ARPs, que vai além do mero preenchimento formal dos artefatos previstos na legislação>.

<Nas contratações de licenciamento de softwares, é imprescindível verificar se toda a documentação entregue pela contratada está completa e corresponde exatamente ao que foi especificado no TR. É fundamental certificar-se de que todas as licenças, suporte e/ou garantia entregues estejam de acordo com os **part numbers** especificados no TR>.

<ESPAÇO DESTINADO À IDENTIFICAÇÃO DO ÓRGÃO/ENTIDADE>

TERMO DE RECEBIMENTO DEFINITIVO

INTRODUÇÃO
O Termo de Recebimento Definitivo declarará formalmente à Contratada que os serviços prestados ou que os bens fornecidos foram devidamente avaliados e atendem às exigências contratuais, de acordo com os requisitos e critérios de aceitação estabelelcidos. **Referência: Inciso XXII, Art. 2º e alínea "h" inciso I do art. 33, da IN SGD/ME Nº 94/2022.**

1 – IDENTIFICAÇÃO			
CONTRATO/NOTA DE EMPENHO Nº	xx/aaaa		
CONTRATADA	<Nome da Contratada>	**CNPJ**	xxxxxxxxxxxx
Nº DA OS/OFB	<xxxx/aaaa>		
DATA DA EMISSÃO	<dd/mm/aaaa>		

2 – ESPECIFICAÇÃO DOS PRODUTO(S)/BEM(S)/SERVIÇOS E VOLUMES DE EXECUÇÃO				
SOLUÇÃO DE TIC				
<descrição da solução de TIC solicitada relacionada ao contrato anteriormente identificado>				
ITEM	**DESCRIÇÃO DO BEM OU SERVIÇO**	**MÉTRICA**	**QUANTIDADE**	**TOTAL**
1	<descrição igual à da OS/OFB de abertura>	<Ex.: PF>	<n>	<total>
...				
TOTAL DE ITENS				

3 – ATESTE DE RECEBIMENTO

Para fins de cumprimento do disposto no art. 33, inciso II, alínea "h", da IN SGD/ME nº 94/2022, por este instrumento ATESTO/ATESTAMOS que o(s) <serviço(s)/ bem(s)> correspondentes à <OS/OFB> acima identificada foram <prestados/entregues> pela **CONTRATADA** e ATENDEM às exigências contratuais, discriminadas abaixo, de acordo com os Critérios de Aceitação previamente definidos no Modelo de Gestão do

<ESPAÇO DESTINADO À IDENTIFICAÇÃO DO ÓRGÃO/ENTIDADE>

Contrato acima indicado.

ITEM	EXIGÊNCIA CONTRATUAL	ATENDIMENTO	OBSERVAÇÃO
1	<exigência contratual estabelecida no TR >	...	.....
...	...	...	.....
...	...	...	.....
...	...	...	.....

4 – DESCONTOS EFETUADOS E VALOR A LIQUIDAR

De acordo com os critérios de aceitação e demais termos contratuais, <não> há incidência de descontos por desatendimento dos indicadores de níveis de serviços definidos.

<Não foram / Foram> identificadas inconformidades técnicas ou de negócio que ensejam indicação de glosas e sanções, <cuja instrução corre em processo administrativo próprio (nº do processo)>.

Por conseguinte, o valor a liquidar correspondente à <OS/OFB> acima identificada monta em R$ <valor> (<valor por extenso>).

Referência: <Relatório de Fiscalização nº xxxx ou Nota Técnica nº yyyy>.

5 – ASSINATURA

GESTOR DO CONTRATO

_____

<Nome do Gestor do Contrato>
Matrícula: xxxxxxxx

<Local>, <dia> de <mês> de <ano>.

<ESPAÇO DESTINADO À IDENTIFICAÇÃO DO ÓRGÃO/ENTIDADE>

<As seções seguintes podem constar em documento diverso, pois dizem respeito à autorização para o faturamento, a cargo do Gestor do Contrato, e a respectiva ciência do preposto quanto a esta autorização>.

5 – AUTORIZAÇÃO PARA FATURAMENTO
GESTOR DO CONTRATO
Nos termos da alínea "n", inciso I, art. 33, da IN SGD/ME nº 94/2022, AUTORIZA-SE a **CONTRATADA** a <faturar os serviços executados / apresentar as notas fiscais dos bens entregues> relativos à supracitada <OS/OFB>, no valor discriminado no item 4, acima. _____ <Nome do Gestor do Contrato> **Matrícula:** xxxxxxxx <Local>, <dia> de <mês> de <ano>

7 – CIÊNCIA
PREPOSTO
_____ <Nome do Preposto do Contrato> **Matrícula**: xxxxxxx <Local>, <dia> de <mês> de <ano>

ANEXO- MODELO DE DECLARAÇÃO DE REALIZAÇÃO DA VISTORIA TÉCNICA OU OPÇÃO POR NÃO REALIZAÇÃO

DECLARAÇÃO DE REALIZAÇÃO DA VISTORIA TÉCNICA

DECLARAMOS, para fins de participação no Pregão Eletrônico n° ____/2023, que a empresa <Razão Social da Empresa>, registrada no CNPJ/MF <CNPJ>, representada por seu Responsável Técnico abaixo identificado, realizou VISTORIA TÉCNICA nas instalações da Coordenação-Geral de Infraestrutura, Cibersegurança e Serviços de TI da Subsecretaria de Tecnologia da Informação do Ministério da Agricultura e Pecuária, tomando ciência de informações e instruções necessárias ao atendimento do objeto da presente licitação e à eventual elaboração de sua PROPOSTA.

Data

Nome

Cargo

Assinatura

DECLARAÇÃO DE NÃO REALIZAÇÃO DA VISTORIA TÉCNICA

DECLARAMOS, para fins de participação no Pregão Eletrônico n° ____/2023, que a empresa <Razão Social da Empresa>, registrada no CNPJ/MF <CNPJ>, em conformidade com a previsão contida no item 4.12 do Termo de Referência, manifestamos nossa opção por **não realização** da Vistoria Técnica.

Data

Nome

Cargo

Assinatura

<ESPAÇO DESTINADO À IDENTIFICAÇÃO DO ÓRGÃO/ENTIDADE>

Histórico de Revisões

Data	Versão	Descrição	Autor
DD/MM/AAAA	1.0	Primeira versão do documento.	XXXXXXXXXXX

ATENÇÃO!

< Os trechos marcados em vermelho neste documento são editáveis, notas explicativas ou exemplos, devendo ser substituídos ou excluídos, conforme necessidade>.

<Conforme **ACÓRDÃO 172/2021 – TCU -PLENÁRIO**, os órgãos e entidades federais têm o dever legal de realizar o planejamento prévio de cada contratação de TIC, inclusive daquelas viabilizadas mediante adesão a ARPs, que vai além do mero preenchimento formal dos artefatos previstos na legislação>.

<ESPAÇO DESTINADO À IDENTIFICAÇÃO DO ÓRGÃO/ENTIDADE>

TERMO DE COMPROMISSO DE MANUTENÇÃO DE SIGILO

INTRODUÇÃO
O Termo de Compromisso de Manutenção de Sigilo registra o comprometimento formal da Contratada em cumprir as condições estabelecidas no documento relativas ao acesso e utilização de informações sigilosas da Contratante em decorrência de relação contratual, vigente ou não. **Referência: Art. 18, Inciso V, alínea "a" da IN SGD/ME Nº 94/2022.**

Pelo presente instrumento o <NOME DO ÓRGÃO>, sediado em <ENDEREÇO>, CNPJ n° <Nº do 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.

1 – OBJETO

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

[...]

[...]

[...]

<ESPAÇO DESTINADO À IDENTIFICAÇÃO DO ÓRGÃO/ENTIDADE>

2 – CONCEITOS E DEFINIÇÕES

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

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

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

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

[...]

[...]

[...]

3 – DA INFORMAÇÃO SIGILOSA

Serão consideradas como informação sigilosa, toda e qualquer informação classificada ou não nos graus de sigilo ultrassecreto, secreto e reservado. O TERMO abrangerá toda informação escrita, verbal, ou em linguagem computacional em qualquer nível, ou de qualquer outro modo apresentada, tangível ou intangível, podendo incluir, mas não se limitando a: *know-how*, técnicas, especificações, relatórios, compilações, código fonte de programas de computador na íntegra ou em partes, fórmulas, desenhos, cópias, modelos, amostras de 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.

[...]

[...]

[...]

4 – DOS LIMITES DO SIGILO

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

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

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

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

[...]
[...]
[...]

5 – DIREITOS E OBRIGAÇÕES

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

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

Parágrafo Segundo – A CONTRATADA compromete-se a dar ciência e obter o aceite formal da direção e empregados que atuarão direta ou indiretamente na execução do CONTRATO PRINCIPAL sobre a existência deste TERMO bem como da natureza sigilosa das informações.

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

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

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

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

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

da execução do CONTRATO PRINCIPAL.

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

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

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

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

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

[...]

[...]

[...]

6 – VIGÊNCIA

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

[...]

7 – PENALIDADES

A quebra do sigilo e/ou da confidencialidade das INFORMAÇÕES, devidamente comprovada, possibilitará a imediata aplicação de penalidades previstas conforme disposições contratuais e legislações em vigor que tratam desse assunto, podendo até culminar na rescisão do CONTRATO PRINCIPAL firmado entre as PARTES. Neste caso, a CONTRATADA, estará sujeita, por ação ou omissão, ao pagamento ou recomposição de todas as perdas e danos sofridos pela CONTRATANTE, inclusive as de ordem moral, bem como as de responsabilidades civil e criminal, as quais serão apuradas em regular processo administrativo ou judicial, sem prejuízo das demais sanções legais cabíveis, conforme previsto nos arts. 155 a 163 da Lei nº. 14.133, de 2021.

<ESPAÇO DESTINADO À IDENTIFICAÇÃO DO ÓRGÃO/ENTIDADE>

[...]
[...]
[...]

8 – DISPOSIÇÕES GERAIS

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

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

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

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

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

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

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

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

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

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

VII – O acréscimo, complementação, substituição ou esclarecimento de qualquer uma das informações, conforme definição do item 3 deste documento, disponibilizadas para a CONTRATADA, serão incorporados a este TERMO, passando a fazer dele parte integrante, para todos os fins e efeitos, recebendo também a mesma proteção descrita para as informações iniciais disponibilizadas, sendo necessário a formalização de TERMO aditivo ao CONTRATO PRINCIPAL;

<ESPAÇO DESTINADO À IDENTIFICAÇÃO DO ÓRGÃO/ENTIDADE>

VIII – Este TERMO não deve ser interpretado como criação ou envolvimento das Partes, ou suas filiadas, nem em obrigação de divulgar INFORMAÇÕES para a outra Parte, nem como obrigação de celebrarem qualquer outro acordo entre si.

[...]
[...]
[...]

9 – FORO

A CONTRATANTE elege o foro da Justiça Federal da Seção Judiciária do Distrito Federal, onde está localizada a sede da CONTRATANTE, para dirimir quaisquer dúvidas originadas do presente TERMO, com renúncia expressa a qualquer outro, por mais privilegiado que seja.

[...]

10 – ASSINATURAS

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

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

<Local>, <dia> de <mês> de <ano>.

ITEM 1 – Uma (01) Solução de plataforma de segurança em alta disponibilidade denominada Next Generation Firewall (NGFW).

CAPACIDADES

- Deve suportar operação em cluster ativo-ativo sem a necessidade de licenças adicionais.
- **A unidade** da solução contratada deve operar em cluster e ter as seguintes capacidades:
- Throughput de, no mínimo, **23** (Vinte e três) Gbps, com as funcionalidades de firewall, prevenção de intrusão, controle de aplicação, filtro de URL, antivírus, Anti-Bot e prevenção de ameaças avançadas de dia zero. (Threat Protection ou nome equivalente).
- Deve suportar a performance considerando as funcionalidades de Next Generation firewall de **34** (Trinta e quatro) Gbps.
- Througupt de no mínimo, **43** (Quarenta e três) Gbps de IPS.
- Suportar , no mínimo, **32**.000.000 (Trinta e dois milhões) de conexões simultâneas.
- Suportar , no mínimo, **550**.000 (Quinhentas e Cinquenta mil) novas conexões por segundo.
- Suportar e estar licenciado para acesso remoto Client-to-site ilimitado ou com a licença de maior capacidade;
- Fonte de alimentação redundante e hot-swappable.
- Suportar , no mínimo, **16** (Dezesseis) interfaces de rede 10Gbps SFP (SFP+,SFP28, QSFP+, QSFP28).
- Suportar, no mínimo, **02** (**Duas**) interfaces de rede 100/1000 Base-T.
- Possuir pelo menos 2 (duas) interfaces de rede dedicada para sincronismo;
- Possuir pelo menos 2 (duas) interfaces de rede dedicadas ao gerenciamento, não sendo permitido utilizar qualquer outra interface para exercer a função de gerenciamento do equipamento.
- Possuir pelo menos 2 (duas) interfaces do tipo console ou similar.
- Possuir interfaces dedicadas e físicas para gerenciamento dos equipamentos fora de banda. Essas interfaces devem ser um canal de gerenciamento que funcione mesmo quando o dispositivo não responde. Caso os equipamentos não possuam essa interface física/dedicada, deverá ser composta com outro equipamento de terceiro onde faça essa função. Não sendo permitido qualquer tipo de configuração via software ou uso da interface dedicada de gerenciamento.
- Os equipamentos devem possuir arquitetura modular de interfaces de rede, permitindo a substituição de interfaces por outras com tipo de conexão e velocidades diferentes.
- Cada solução da plataforma de proteção de rede deve possuir discos Solid State Drive (SSD) redundantes com, no mínimo, 480 GB de capacidade de armazenamento para o Sistema Operacional.
- Para IPv6, deve suportar roteamento estático e dinâmico (OSPFv3).
- Suporte a RFC 4291 de Arquitetura de endereçamento IPv6.
- Deve suportar Dual stack ipv4/ipv6 e NAT64.
- Deve suportar NAT64 e NAT46.
- Deve implementar Network Prefix Translation (NPTv6) ou NAT66, prevenindo problemas de roteamento assimétrico.
- Cada regra deve, obrigatoriamente, funcionar nas versões de endereço IP v4 e v6 sem duplicação da base de objetos e regras.
- O Throughput e as interfaces solicitadas neste item deverão ser comprovados através de datasheet públicos na internet. Não serão aceitas declarações de fabricantes informando números de performance e interfaces.
- Todas as interfaces fornecidas nos appliances devem estar licenciadas e habilitadas para uso imediato, incluindo seus transceivers/transceptores. Caso sejam fornecidas interfaces além das exigidas, todas as interfaces devem ser fornecidas com todos os transceivers/transceptores necessários para a plena utilização.

FUNCIONALIDADES DE FIREWALL (COMUM PARA OS ITENS 01 E 03 DA CONTRATAÇÃO)

- A solução deve consistir em appliances de proteção de rede com funcionalidades de proteção de próxima geração.
- As funcionalidades de proteção de rede que compõem a plataforma de segurança, podem funcionar em múltiplos appliances desde que obedeçam a todos os requisitos desta especificação técnica.
- O hardware e software que executem as funcionalidades de proteção de rede deve ser do tipo appliance. Não serão aceitos equipamentos servidores e sistema operacional de uso genérico.
- A solução de segurança deve usar Stateful Inspection com base na análise granular de comunicação e de estado do aplicativo para monitorar e controlar o fluxo de rede.
- Realizar upgrade via SCP, SFTP e https via interface WEB.
- Os dispositivos de proteção de rede devem possuir pelo menos as seguintes funcionalidades: ◦ Suporte a, no mínimo, 1024 VLAN Tags 802.1q, agregação de links 802.3ad, policy based routing ou policy based forwarding, roteamento multicast, DHCP Relay, DHCP Server e Jumbo Frames.
  ◦ Deverá suportar VXLAN.
- Deve suportar os seguintes tipos de NAT:
  ◦ Nat dinâmico (Many-to-1), Nat estático (1-to-1), Tradução de porta (PAT), NAT de Origem, NAT de Destino e suportar NAT de Origem e NAT de Destino simultaneamente. ◦ Deve possuir um mecanismo de busca por comandos no gerenciamento via SSH, facilitando a localização de comandos.
  ◦ As regras de NAT devem suportar “hit count” para monitorar a quantidade de conexões que deram matches em cada regra.
  ◦ Deverá permitir a criação de regras de firewall e NAT utilizando nos campos de origem e destino, objetos de serviços online atualizáveis de forma dinâmica, por exemplo: Google Cloud Plataform, Office 365, AWS, Azure e outros. Objetos dinâmicos que não se caracterizam como FQDN.
- Enviar logs para sistemas de monitoração externos, simultaneamente.
- Prover mecanismo contra ataques de falsificação de endereços (IP Spoofing), através da especificação da interface de rede pela qual uma comunicação deve se originar baseado na topologia. Não sendo aceito soluções que utilizem tabela de roteamento para esta proteção.
- Deve realizar roteamentos unicast e multicast simultaneamente em uma única instância(contexto) de firewall.
- Para IPv4, deve suportar roteamento estático e dinâmico (RIPv2, BGP e OSPFv2).
- Suportar OSPF graceful restart.
- Deve suportar roteamento ECMP (equal cost multi-path).
- Para o ECMP, a solução deve suportar o balanceamento do roteamento de forma simultânea usando os seguintes parâmetros: Origem, Destino, Porta de Origem, Porta de Destino e Protocolo.
- Autenticação integrada via Kerberos.
- A solução deve possuir mecanismo para dedicar processamento no equipamento de segurança para funções / ações de gerenciamento, mesmo que o equipamento esteja com alto processamento de CPU. Assim evitando a falta de acesso do administrador para qualquer mitigação de problema e aplicação de política para solução de problemas. Entre as funções, deve suportar no mínimo: acesso SSH, FTP, acesso WEB, alterações de política, comunicação SNMP.
- As regras Firewall devem suportar “hit count” para monitorar a quantidade de conexões que deram matches em cada regra.
- Não serão aceitas soluções nas quais as interfaces de origem e destino tenham que ser obrigatoriamente explicitadas ou obrigatoriamente listadas.
- A solução deve ter a capacidade de operar através de uma única instância de Firewall de forma simultânea mediante o uso das suas interfaces físicas nos seguintes modos: transparente, mode sniffer (monitoramento e análise o tráfego de rede), camada 2 (L2) e camada 3 (L3).
- A solução deve permitir salvar as configurações das políticas para serem aplicadas em horários pré-definidos.
- Deve possuir mecanismo de ativação de validade da regra com período customizado.

● Deverá suportar redundância e balanceamento de links, tendo capacidade de no mínimo 3 links de internet. Deverá suportar configurar um valor de threshold baseando-se em critérios mínimos como fator de decisão nas regras de balanceamento.
● Deve permitir a configuração do tempo de checagem para cada um dos links.

CONTROLE DE APLICAÇÕES (COMUM PARA OS ITENS 01 E 03 DA CONTRATAÇÃO)

● Controle de políticas por aplicações, grupos de aplicações e categorias de aplicações.
● Controle de políticas por usuários, grupos de usuários, IPs e redes.
● Deve descriptografar tráfego de entrada e saída em conexões negociadas com TLS 1.2 e TLS 1.3.
● Suportar a atribuição de agendamento às políticas com o objetivo de habilitar e desabilitar políticas em horários pré-definidos automaticamente.
● Deve ser possível a liberação e bloqueio de aplicações sem a necessidade de liberação de portas e protocolos.
● Reconhecer pelo menos 6.000 (seis mil) aplicações diferentes, incluindo, mas não limitado: a tráfego relacionado a peer-to-peer, redes sociais, acesso remoto, update de software, protocolos de rede, voip, áudio, vídeo, proxy, mensageiros instantâneos, compartilhamento de arquivos, e-mail.
● A checagem de assinaturas deve determinar se uma aplicação está utilizando a porta padrão ou não.
● Para inspeção SSL, ou HTTPS Inspection, a solução deve oferecer suporte ao Perfect Forward Secrecy (conjuntos de cifras PFS, ECDHE).
● Para tráfego criptografado (SSL), deve de-criptografar pacotes a fim de possibilitar a leitura do payload para checagem de assinaturas de aplicações conhecidas.
● Deve realizar decodificação de protocolos com o objetivo de detectar aplicações encapsuladas dentro do protocolo e validar se o tráfego corresponde com a especificação do protocolo.
● A fim de otimização do tempo operacional dos administradores, a solução deverá possuir pelo menos 150 categorias de aplicações WEB pré-definidas pelo fabricante.
● Para solução de filtro de conteúdo e controle web, deve ser capaz de bloquear na mesma aplicação um conteúdo específico sem bloquear a aplicação principal (Ex.: Whatsapp Web, Whatsapp voice e Whatsapp file transfer.).
● Possui mecanismo de controle de aplicação web e URL que possui configuração de bloqueio e liberação da aplicação principal e/ou as suas sub-categorias. Quando o administrador da solução desejar bloquear apenas as sub-categorias do facebook, como facebook, chat, video, game, compartilhamento de arquivos ou outros. Ou seja, não deve ser bloqueado toda a categoria como “Facebook” ou "Redes sociais" que também pode implicar o bloqueio não só do Facebook, mas também bloqueará tudo que estiver relacionado às redes sociais, como LinkedIn, Twitter, YouTube, etc. A solução precisa ser baseada em bloqueio de aplicações WEB que a própria base possui, assim a inspeção ocorrerá em camada 7 analisando o payload do pacote.
● A decodificação de protocolo deve também identificar comportamentos específicos dentro da aplicação.
● Atualizar a base de assinaturas de aplicações automaticamente e Limitar a banda (download/upload) usada por aplicações, baseado no IP de origem, usuários e grupos do LDAP/AD.
● Os dispositivos de proteção de rede devem possuir a capacidade de identificar de forma transparente o usuário de rede com integração ao Microsoft Active Directory, sem a necessidade de instalação de agente no controlador de domínio, nem nas estações dos usuários. Assim, permitindo a criação de políticas de segurança baseadas nas informações coletadas entre elas usuários, IP, grupos de usuários do sistema do Active Directory.
● Deve suportar múltiplos métodos de identificação e classificação das aplicações, por pelo menos checagem de assinaturas, decodificação de protocolos ou análise heurística.
● Permitir nativamente a criação de assinaturas personalizadas para reconhecimento de aplicações proprietárias, sem a necessidade de ação do fabricante, mantendo a confidencialidade das aplicações do órgão.
● Deve possibilitar que o controle de portas seja aplicado para todas as aplicações.
● A plataforma de segurança deve possuir as seguintes funcionalidades de filtro de URL: ◦ Permitir especificar política por tempo, com definição de regras para um determinado horário ou período (dia,

mês, ano, dia da semana e hora).

◦ Deve ser possível a criação de políticas por Usuários, Grupos de Usuários, IPs e Redes. ◦ Deverá incluir a capacidade de criação de políticas baseadas na visibilidade e controle de quem está utilizando quais URLs através da integração com serviços de diretório, autenticação via Active Directory e base de dados local.

◦ Suportar a capacidade de criação de políticas baseadas no controle por URL e Categoria de URL.

◦ Suportar armazenamento, na própria solução, de URLs, evitando delay de comunicação/validação das URLs.

◦ Deve bloquear o acesso a sites com conteúdo indevido ao utilizar a busca em sites como Google, Bing e Yahoo, mesmo que a opção "Safe Search" esteja desabilitada no navegador do usuário. ◦ Suportar base ou cache de URLs local no appliance, evitando atrasos de comunicação e validação das URLs. Caso a solução ofertada não suporte localmente, será aceito produto externo desde que não seja solução de software livre.

◦ Suportar a criação de categorias de URLs customizadas e a exclusão de URLs do bloqueio, por categoria.

◦ Permitir a customização de página de bloqueio.

◦ Deve possuir integração com Microsoft Active Directory para identificação de usuários e grupos permitindo granularidade de controle/políticas baseadas em usuários e grupos de usuários, sem a necessidade de instalar nenhum cliente nos servidores Active Directory ou em outra máquina da rede.

◦ Deve suportar o recebimento eventos de autenticação de controladoras wireless, dispositivos 802.1x e soluções NAC via Radius ou API's ou Syslog, para a identificação de endereços IP e usuários.

◦ Deve permitir o controle, sem instalação de cliente de software, em máquinas/computadores que solicitem saída à internet para que antes de iniciar a navegação, expanda-se um portal de autenticação residente no Firewall (Captive Portal).

PREVENÇÃO CONTRA AMEAÇAS (COMUM PARA OS ITENS 01 E 03 DA CONTRATAÇÃO)

● Para proteção do ambiente contra ataques, os dispositivos de proteção devem possuir módulo de IPS e suportar os módulos de: Antivírus e Anti-Malware integrados no próprio equipamento de firewall.

● Possuir capacidade de detecção de, no mínimo, 7.000 (sete mil) assinaturas de ataques pré-definidos.

● Deve sincronizar as assinaturas de IPS, Antivírus, Anti-Malware quando implementado em alta disponibilidade ativo/ativo.

● Deve suportar granularidade nas políticas de Antivírus e Anti-malware, possibilitando a criação de diferentes políticas por endereço de origem, endereço de destino, serviço e a combinação de todos esses itens.

● A fim de não criar indisponibilidade no appliance de segurança, a solução de IPS deve possuir mecanismo de fail-open baseado em software, configurável baseado em thresholds de CPU e memória do dispositivo.

● Deverá possuir os seguintes mecanismos de inspeção de IPS:

◦ Análise de padrões de estado de conexões, análise de decodificação de protocolo, análise para detecção de anomalias de protocolo, IP Defragmentation, remontagem de pacotes de TCP e bloqueio de pacotes malformados.

◦ Detectar e bloquear a origem de portscans.

◦ Bloquear ataques conhecidos, permitindo ao administrador acrescentar novos padrões de assinaturas e customizações.

◦ Possuir assinaturas para bloqueio de ataques de buffer overflow.

◦ Suportar o bloqueio de malware em, pelo menos, os seguintes protocolos: HTTP, HTTPS e SMTP.

◦ Suportar bloqueio de arquivos por tipo.

◦ Identificar e bloquear comunicação com botnets.
◦ Deve suportar referência cruzada com CVE.
● Em cada proteção de segurança, deve estar incluso informações como:
◦ Código CVE (Common Vulnerabilities and Exposures), não sendo aceito outro codigo de referência.
◦ Severidade.
◦ Tipo de ação a ser executada.
● O IPS deve fornecer um mecanismo automatizado para ativar ou gerenciar novas assinaturas vindas de atualizações.
● O IPS deve suportar exceções de rede com base na origem, destino, serviço ou uma combinação dos três.
● O IPS deve incluir um modo de solução de problemas que defina o perfil em uso para detectar apenas, sem modificar as proteções individuais.
● O administrador deve poder ativar automaticamente novas proteções, com base em parâmetros configuráveis (impacto no desempenho, gravidade da ameaça, nível de confiança, proteção do cliente, proteção do servidor).
● Registrar na console de monitoração as seguintes informações sobre ameaças identificadas: ◦ O nome da assinatura e do ataque, aplicação, usuário, origem e o destino da comunicação, além da ação tomada pelo dispositivo de proteção.
● Deve suportar a captura de pacotes (PCAP), em assinatura de IPS e Anti-Malware, através da console de gerência centralizada.
● Na própria interface de gerência, a solução de IPS deverá apresentar sumário de todos os equipamentos que estão sendo gerenciados, assim como, qual o tipo de perfil assinalado, de forma individual.
● A solução de IPS, deve possuir mecanismo de análise baseado nas conexões realizadas para as aplicações, que aponta quais assinaturas que estão em modo detecção deve ser alterada para modo prevenção, assim evitando qualquer tipo de ataque para aplicações que estão expostas no ambiente.
● O administrador deve ser capaz de configurar quais comandos FTP são aceitos e quais são bloqueados na funcionalidade de IPS.
● A solução deverá possuir pelo menos dois perfis pré configurados pelo fabricante que permitam sua utilização assim que o equipamento for configurado.
● A solução deve permitir que o administrador possa configurar quais métodos e comandos HTTP são permitidos e quais são bloqueados.
● Deve incluir proteção contra vírus em conteúdo ActiveX e applets Java e worms. ● Solução deve proteger contra os ataques do tipo DNS Cache Poisoning, e impedir que os usuários acessem endereços de domínios bloqueados.
● O gerenciamento centralizado via interface gráfica, deve possibilitar a configuração de captura dos pacotes por regras individuais, visando aperfeiçoar o desempenho do equipamento. ● A solução de IPS deve possuir engine onde irá determinar de forma automática, onde qualquer nova assinatura que for baixada na base local deverá atuar em modo de prevenção ou detecção, assim evitará qualquer tipo de alteração na base de assinatura atual.
● O antivírus deve oferecer suporte à verificação de links dentro de e-mails.
● A solução de anti-malware deve ser capaz de detectar e interromper o comportamento anormal suspeito da rede quando usuário estiver conectado com ambiente externo malicioso. ● A solução deve permitir criar regras de exceção de acordo com a proteção, a partir do log visualizado na interface gráfica da gerência centralizada.
● Para melhor administração a solução deve possuir a granularidade na classificação das proteções de IPS através de: severidade, nível de confiança da proteção, impacto da performance, referência de indústria terceira e status de download recente.
● A solução deve permitir a criação de White list baseado no MD5 do arquivo.
● Os eventos devem identificar o país de onde partiu a ameaça.
● A funcionalidade de IPS e anti-bot, deve possuir capacidade de correlacionar em seus logs a visibilidade de acordo com o framework ATT&CK Mitre Matrix, pontuando características de

técnicas de acordo com a ameaça detecada/bloqueada pela solução. Caso a solução não possua determinada capacidade, poderá ser integrada com outra solução de mercado, não sendo ela soluções abertas.

- Suportar rastreamento de vírus em arquivos pdf.
- Deve suportar a inspeção em arquivos comprimidos (zip, gzip,etc.).
- Em caso de falha no mecanismo de inspeção do Anti-Vírus, deve ser possível configurar se as conexões serão permitidas ou bloqueada.
- A solução de Antivírus e Anti-Malware deve funcionar de forma independente, ou seja, caso sejam desabilitadas, elas não podem causar a interrupção de outras funcionalidades de segurança como prevenção de ameaças avançadas (zero-day.
- A solução Antivírus deverá suportar análise de arquivos que trafegam dentro do protocolo CIFS/SMB, de forma a conter malwares se espalhando horizontalmente pela rede.
- Suportar a criação de políticas por Geo Localização, permitindo que o tráfego de determinado País/Países seja bloqueado.
- Deve possibilitar a visualização dos países de origem e destino nos logs dos acessos.
- Deverá possuir a função resolução de endereços via DNS, para que conexões com destino a domínios maliciosos, sejam resolvidas pelo Firewall com endereços previamente definidos, para interceptar a comunicação e bloquear o acesso do usuário.
- A solução de Anti-malware deve ser capaz de detectar e interromper o comportamento anormal suspeito da rede.
- A solução deve possuir funcionalidade de identificação de bloqueio de tráfego malicioso comunicando com C&C (command & Control).
- A solução Antivírus deverá suportar a análise de links no corpo de emails.

FUNCIONALIDADES DE CONTROLE DE QUALIDADE DE SERVIÇO (COMUM PARA OS ITENS 01 E 03 DA CONTRATAÇÃO)

- Objetivando controlar aplicações e tráfego cujo consumo possa impactar o desempenho de rede, como streaming de mídias, a solução, além de permitir ou negar esse tipo de aplicação, deve ter a capacidade de limitá-las por políticas de controle de taxa de transmissão, quando solicitadas por diferentes usuários ou aplicações, tanto de streaming de áudio como de vídeo.
- Suportar a criação de políticas de QoS por Endereço de origem, Endereço de destino, Por usuário e grupo do LDAP/AD, Por porta; e Por tipo de tráfego.
- As funcionalidades de QoS e Traffic Shaping devem possibilitar a definição de classes por: Banda garantida, Banda máxima por usuário, Banda máxima por aplicação e Fila de prioridade.
- Suportar priorização em tempo real de protocolos de voz (VOIP) como H.323, SIP, SCCP, MGCP, dentre outros.
- Suportar marcação de pacotes diffserv.
- Deverá permitir o monitoramento do uso que as aplicações fazem por bytes, sessões e por usuário.

FILTRO DE DADOS (COMUM PARA OS ITENS 01 E 03 DA CONTRATAÇÃO)

- Permitir a criação de filtros para arquivos e dados pré-definidos.
- Os arquivos devem ser identificados por extensão e assinaturas.
- Suportar a identificação de arquivos compactados e a aplicação de políticas sobre o conteúdo desses tipos de arquivos.
- Permitir listar o número de aplicações suportadas para controle de dados e Permitir listar o número de tipos de arquivos suportados para controle de dados.
- Deve possibilitar a priorização em tempo real de protocolos de voz (VoIP) como H.323, SIP e SCCP. 14.214. 14.215. 14.216. 14.217. 14.218.

ALTA DISPONIBILIDADE E BALANCEAMENTO DE CARGA (COMUM PARA OS ITENS 01 E 03 DA CONTRATAÇÃO)

- Permitir a configuração dos appliances em modo de alta disponibilidade, com suporte mínimo aos seguintes modos de configuração: Ativo-Ativo.
- A alternância entre os dispositivos configurados em modo de alta disponibilidade deve se dar no mínimo pelos seguintes parâmetros de detecção de anomalia:
  - Falha de funcionamento do dispositivo.
  - Falha de link, seja por falha no tráfego (path monitoring) quanto por falha no tráfego das suas interfaces (Interface Monitoring).
- Deverá ter a capacidade de testar o funcionamento de rotas estáticas e rota default com a definição de um endereço IP de destino, que deverá estar comunicável através da rota. Caso haja falha na comunicação, o firewall deverá ter a capacidade de usar alternativa para restabelecer a comunicação.
- Operando em alta disponibilidade, os dispositivos deverão, no mínimo, sincronizar as seguintes informações entre si:
  - Certificados digitais, informações registradas em sua Forwarding Information Base(FIB), configurações registradas em suas políticas de firewall incluindo em seus objetos de rede, configurações de NAT e possuir administração através de linha de comando através de SSH versão 2 e através de interface WEB.
- A solução de balanceamento deve possuir a capacidade de, automaticamente, por meio de definições de thresholds, executar a realocação de equipamentos entre os clusters, ou o redirecionamento do tráfego sem a necessidade de intervenção física para este redirecionamento.

DETECÇÃO E TRATAMENTO POR MALWARES DESCONHECIDOS (COMUM PARA OS ITENS 01 E 03 DA CONTRATAÇÃO)

- Ser capaz de detectar e analisar malwares desconhecidos, ou seja, que não estejam na base de registro de assinaturas da solução, utilizando-se para tal de recursos avançados, como o uso de sandbox para isolamento e tratamento de ameaças.
- Monitorar os arquivos trafegados na internet em protocolos HTTP, HTTPS e SMTP.
- Monitorar os arquivos trafegados internamente entre servidores de arquivos usando SMB em todos os modos de implementação: sniffer, transparente e Layer 3.
- Prevenir através do bloqueio efetivo do malware desconhecido (Dia Zero), oriundo da comunicação Web (HTTP e HTTPS) e E-mail (SMTP/TLS) via MTA durante análise completa do arquivo no ambiente sandbox, sem que o mesmo seja entregue parcialmente ao cliente.
- A análise de malwares não conhecidos em ambiente controlado (sandbox) também deve ser realizada em arquivos tipo executáveis, DLLs,arquivos compactados RAR, .zip e 7-ZIP, arquivos do pacote MS Office (.doc, .docx, .xls, .xlsx, .ppt, .pptx), arquivos PDF, arquivos JAVA (.jar e class), arquivos DMG,arquivos ELF e arquivos APK.
- Ser capaz de detectar e analisar arquivos suspeitos em ambiente Sandbox simulando, no mínimo, os sistemas operacionais Windows 7 e superiores e Office 2003 e superiores.
- Realizar o envio automático de arquivos trafegados na rede MAPA para análise Sandbox, onde o arquivo será executado e simulado em ambiente controlado.
- Permitir o envio para análise em Sandbox de malwares bloqueados pelo antivírus da solução.
- A seleção dos arquivos para envio para análise deverá se dar por meio políticas granulares de segurança, considerando-se parâmetros opicos da solução Firewall NGFW, como endereço IP de origem/destino, usuário/grupo de usuários, aplicação, protocolo/porta, URL e categoria de URL, tipo de arquivo.
- Diferenciar os arquivos analisados em pelo menos três categorias:
  - Malicioso.
  - Não maliciosos.
  - Não maliciosos, mas com características indesejáveis.

    - Entende-se como “não malicioso, mas com características indesejáveis”; softwares que causem problemas de performance em dispositivos, tais como lentidão na execução do sistema operacional, ou que alterem parâmetros de sistema, como alterações no registro do Windows.
- Suportar a análise Sandbox de arquivos executáveis, DLLs, compactados (.zip, .rar, .7-zip etc.) e criptografados em tráfego SSL.
- Suportar a análise Sandbox de arquivos do pacote Microsoft Office (.doc, .docx, .xls, .xlsx, .ppt, .pptx), arquivos java (.jar e .class), e arquivos do sistema operacional Android.
- Capacidade de análise de links em Sandbox, com registro posterior na base de filtro de URL da solução, caso o link analisado em Sandbox for classificado em categorias maliciosas, como “phishing”.
- Permitir o envio de arquivos e links para análise no ambiente controlado de forma automática via API.
- Permitir exportar, a partir da própria console de gerenciamento da solução, o resultado das análises de malwares do tipo “Zero Day” em arquivo tabulado, como .txt; .csv ou .pdf.

SEGURANÇA EM TRÁFEGO CRIPTOGRAFADO (COMUM PARA OS ITENS 01 E 03 DA CONTRATAÇÃO)

- O controle, inspeção e de-criptografia de SSL por política para tráfego de entrada (Inbound) e de saída (Outbound);
- O “offload” de certificado em inspeção de conexões SSL de entrada (Inbound).
- Descriptografar o tráfego Inbound e Outbound em conexões negociadas com TLS v 1.3 ou superior.
- Inspeção e de-criptografia de SSH com base em políticas de segurança.
- Deverá possibilitar a identificação e o bloqueio de tráfego, caso o protocolo esteja sendo usado como técnica evasiva para burlar os controles de segurança;
- Descriptografar sites e aplicações que utilizam certificados ECC, incluindo Elliptical Curve Digital Signature Algorithm (ECDSA);
- Deverá permitir o espelhamento de tráfego descriptografado (SSL e TLS) para análise por meio de soluções externas de segurança, por exemplo, soluções de análise forense de rede, ferramentas de auditoria, Data Loss Prevention, etc.

SEGMENTAÇÃO E ENDEREÇAMENTO DE REDE (COMUM PARA OS ITENS 01 E 03 DA CONTRATAÇÃO)

- Cada dispositivo Firewall NGFW, deve permitir as seguintes configurações mínimas de segmentação e endereçamento de rede:
    - Ao menos 50 (cinquenta) zonas de segurança.
    - Suporte a pelo menos 10 (dez) roteadores virtuais.
    - Permitir a criação de sub-interfaces lógicas Ethernet.
    - Suportar a criação de pelo menos 3.000 (três mil) VLANs (802.1q tags) por dispositivo e por interface.
- Suportar agregação de links por meio de implementação 802.3ad Link Aggregation e Link Aggregation Control Protocol (LACP).
- Permitir configuração de balanceamento de link através de, no mínimo, uma das seguintes opções:
    - Por políticas aplicadas a usuário ou grupos de usuários do LDAP/Active Directory ou ○ Por políticas configuradas por aplicação e porta de destino.
- Permitir a configuração de interfaces nos seguintes modos:
    - Sniffer: Monitoramento e análise de tráfego por espelhamento de porta local (SPAN) ou remota (RSPAN).
    - Layer 2 switching, com ou sem utilização de VLAN’s.
    - Layer 3 routing.
    - Modo transparente ou “virtual wire” (interconexão de portas do Firewall NGFW).

○ Agrupamento de interfaces (IEEE 802.1AX link aggregation).
○ Misto: Mais de um modo de configuração de interface no mesmo appliance.

- Permitir o roteamento ou encaminhamento de pacotes baseado em políticas (PBF - Policy Based Forwarding).
- Implementar recursos de Network Address Translation (NAT) em redes IPv4 e IPv6, incluindo implementação em rede híbrida (NAT64), com suporte mínimo aos seguintes recursos: ○ NAT de Origem e de NAT de Destino, configurados isolada ou simultaneamente. ○ NAT estático do tipo "One-to-One", bidirecional "One-to-One" e "Many-to-Many". ○ NAT dinâmico do tipo "Many-to-One" e "Many-to-Many".
  ○ NAT Overload com tradução de endereço de porta (PAT).
  ○ NAT para interfaces conectadas virtualmente (Virtual Wire), com implementações mínimas de NAT Estático, NAT de Origem e NAT de Destino.

VPN (COMUM PARA OS ITENS 01 E 03 DA CONTRATAÇÃO)

- Suportar VPN Site-to-Site.
- Suportar IPSEC VPN.
- A VPN IPSEC deve suportar:
  - 3DES, Autenticação MD5 e SHA-1, Diffie-Hellman Group 1, Group 2, Group 5 e Group 14, Algoritmo Internet Key Exchange (IKE), AES 128 e 256 (Advanced Encryption Standard) e Autenticação via certificado IKE PKI.
- Suportar SSL VPN o qual deve:
  - Permitir que o usuário realize a conexão por meio de cliente instalado no sistema operacional do equipamento ou por meio de interface WEB.
  - A funcionalidades de VPN SSL devem ser atendidas com ou sem o uso de agente.
- Suportar autenticação via AD/LDAP, certificado e base de usuários local.
- Suportar leitura e verificação de CRL (certificate revocation list).
- O agente de VPN SSL client-to-site deve ser compatível com pelo menos:
  - Windows, Linux e Mac OS X.
- Deve suportar duplo fator de autenticação para a conexão VPN.
- Suportar no mínimo 1.000 conexões simultâneas.

ACESSÓRIOS (COMUM PARA OS ITENS 01 ao 06 e 08 DA CONTRATAÇÃO) Além dos cabos de alimentação de energia, o equipamento deve ser acompanhado também dos seguintes acessórios obrigatórios:

- Trilhos deslizantes e demais itens necessários para instalação em rack padrão 19 polegadas.
- Cabos fibre channel com conectores LC/LC com no mínimo 5 (cinco) metros de comprimento, na mesma quantidade de transceivers SFP/SFP+ ofertados na solução, ou seja, no mínimo 16 (dezesseis) cabos;
- Cabos e interfaces de interconexão entre os appliances físicos para configuração da solução em modo de "alta disponibilidade", considerando-se que os firewalls NGFW ficarão próximos um do outro na rack, com distância entre eles de até 02 (dois) U;
- Todos os drivers, softwares e licenças necessários para o perfeito funcionamento de todos os componentes da solução;
- Documentação com a especificação técnica dos equipamentos;
- Manuais de instalação, operação e gerenciamento;
- Todos os documentos e manuais deverão ser confeccionados preferencialmente em língua portuguesa e fornecidos no momento da entrega do equipamento por meio de mídia física ou digital.

ITEM 3 – 3 (três) soluções de plataforma de segurança em alta disponibilidade denominada Next Generation Firewall (NGFW).

CAPACIDADES

- Cada uma das três soluções deve operar em modo cluster ativo-ativo sem a necessidade de licenças adicionais.

  Cada uma das três unidades da solução contratada deve ter as seguintes capacidades:

  - Throughput de, no mínimo, **11** (Onze) Gbps por solução, com as funcionalidades de firewall, prevenção de intrusão, controle de aplicação, filtro de URL, antivírus, Anti-Bot e prevenção de ameaças avançadas de dia zero. (Threat Protection ou nome equivalente).
- Deve suportar a performance considerando as funcionalidades de Next Generation firewall de **25** (vinte e cinco) Gbps.
- Throughput de no mínimo, **30** (Trinta) Gbps de IPS.
- Suportar, no mínimo, **8**.000.000 (Oito milhões) de conexões simultâneas.
- Suportar, no mínimo, **340**.000 (Trezentos e quarenta mil) novas conexões por segundo;
- Suportar e estar licenciado para acesso remoto Client-to-site ilimitado ou com a licença de maior capacidade;
- Fonte de alimentação redundante e hot-swappable;
- Suportar, no mínimo, **08** (Oito) interfaces de rede 10Gbps SFP (SFP+,SFP28,QSFP+,QSFP28).
- No mínimo, **04** (Quatro) interfaces de rede 100/1000 base-T.
- Possuir, no mínimo, 2 (Duas) interfaces de rede dedicadas para sincronismo.
- Possuir, no mínimo, 2 (Duas) interfaces de rede dedicadas ao gerenciamento, não sendo permitido utilizar qualquer outra interface para exercer a função de gerenciamento do equipamento.
- Possuir pelo menos 2 (duas) interfaces do tipo console ou similar.
- Possuir interfaces dedicadas e físicas para gerenciamento do equipamento fora de banda. Essas interfaces devem ser um canal de gerenciamento que funcionem mesmo quando o dispositivo não responde. Caso o equipamento não possua essa interface física/dedicada, deverá ser composta com outro equipamento de terceiro onde faça essa função. Não sendo permitido qualquer tipo de configuração via software ou uso da interface dedicada de gerenciamento.
- Os equipamentos devem possuir arquitetura modular de interfaces de rede, permitindo a substituição de interfaces por outras com tipo de conexão e velocidades diferentes.
- Cada solução da plataforma de proteção de rede deve possuir discos Solid State Drive (SSD) redundantes com no mínimo 480 (quatrocentos e oitenta) GB de capacidade de armazenamento para o Sistema Operacional.
- Para IPv6, deve suportar roteamento estático e dinâmico (OSPFv3).
- Suporte a RFC 4291 de Arquitetura de endereçamento IPv6.
- Deve suportar Dual stack ipv4/ipv6 e NAT64.
- Deve suportar NAT64 e NAT46.
- Deve implementar Network Prefix Translation (NPTv6) ou NAT66, prevenindo problemas de roteamento assimétrico.
- Cada regra deve, obrigatoriamente, funcionar nas versões de endereço IP v4 e v6 sem duplicação da base de objetos e regras.
- O Throughput e as interfaces solicitadas neste item deverão ser comprovados através de datasheet públicos na internet. Não serão aceitas declarações de fabricantes informando números de performance e interfaces.
- Todas as interfaces fornecidas nos appliances devem estar licenciadas e habilitadas para uso imediato, incluindo seus transceivers/transceptores. Caso sejam fornecidas interfaces além das exigidas, todas as interfaces devem ser fornecidas com todos os transceivers/transceptores necessários para a plena utilização.

Estudo Técnico Preliminar 92/2023

1. Informações Básicas

Número do processo: 21000.020025/2023-02

2. Introdução

O Estudo Técnico Preliminar – ETP é o documento constitutivo da primeira etapa do planejamento de uma contratação, que caracteriza o interesse público envolvido e a sua melhor solução. Ele serve de base ao Termo de Referência a ser elaborado, caso se conclua pela viabilidade da contratação.

Este estudo técnico preliminar em questão tem o objetivo de identificar e analisar os cenários para o atendimento da demanda que consta no Documento de Formalização da Demanda SEI Nº 27476908, bem como demonstrar a viabilidade técnica e econômica das soluções identificadas. Além disso, também descreve as análises realizadas em relação às condições da contratação em termos de necessidades, requisitos, alternativas, , justificativas técnicas e econômica, comparativo de custos e resultados pretendidos, com o objetivo de fornecer as informações necessárias para subsidiar o respectivo processo de contratação.
Referência: Inciso XI, do artigo 2º e artigo 11 da IN SGD/ME Nº 94/20

2.1 - GLOSSÁRIO

- **Ministério Provedor -** Ministério da Agricultura e Pecuária.
- **Ministérios Demandantes:**
  - Ministério da Aquicultura e Pesca. Ministério da Desenvolvimento Agrário e Agricultura Familiar.
- **NGFW** - Next Generation Firewall.
- **LGDP** - Lei Geral de Proteção de Dados Pessoais.

3. Descrição da necessidade

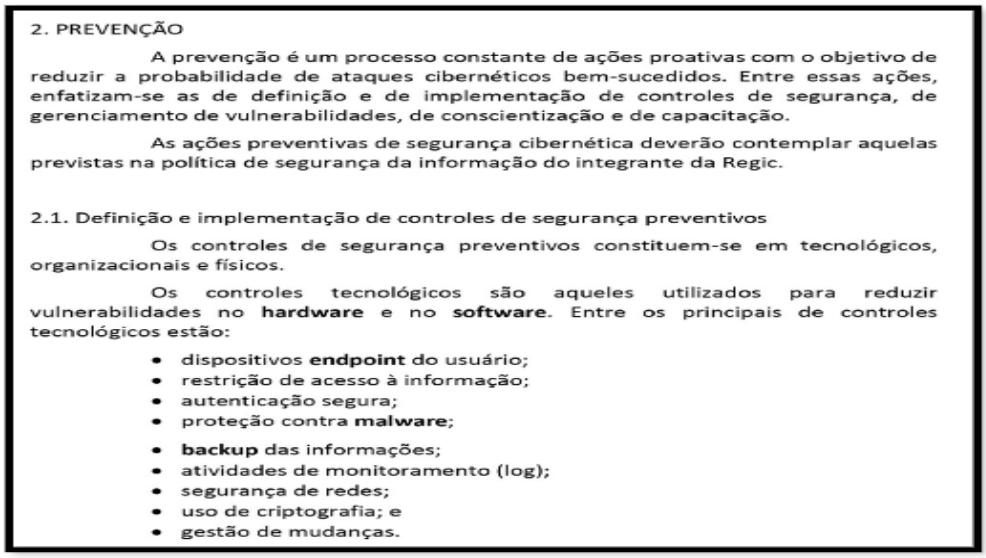
3.1 - CONTEXTUALIZAÇÃO, JUSTIFICATIVA E DESCRIÇÃO DA NECESSIDADE

Os constantes ataques cibernéticos, a necessidade de continuidade do negócio e a evolução de ameaças das mais variadas espécies criam a necessidade de contratação de uma solução eficaz que proteja as informações dos órgãos públicos (MAPA e Ministérios demandantes) e diminua os riscos de acesso indevido às mesmas. Essa crescente disseminação de ataques, em especial à Administração Pública, vem sendo alvo de ações maliciosas com destaque para invasões de sites oficiais, indisponibilidade de recursos e serviços, exposição de vulnerabilidades e consequentes vazamentos de informações, causando assim prejuízos não só ao erário, mas também reflexos negativos no atendimento aos cidadãos , empresas e demais entes envolvidos.

Devido ao aumento significativo dessas ameaças, é imprescindível implementar inteligência e automatização no gerenciamento das soluções de segurança. As ferramentas adotadas para o cenário de outrora tornaram-se insuficientes, uma vez que as tecnologias de mercado evoluíram e o ambiente se expandiu consistentemente. Assim, é prudente acompanhar a evolução e adotar as atualizações tecnológicas necessárias para fornecer serviços adequados e mais seguros. Além disso, em um contexto dinâmico de constante evolução tecnológica e em um curto intervalo de tempo, os equipamentos destinados à segurança da informação podem se tornar obsoletos a tal ponto de não suportarem o aumento do tráfego de internet e dados, o crescimento de novos usuários/novas ameaças e tentativas de invasões das redes corporativas. As tecnologias voltadas à segurança da informação estão em constante evolução, e os fabricantes buscam soluções eficazes para obter o melhor desempenho dos firewalls e ao mesmo tempo prover inteligência proativa, reunindo as mais diversas funcionalidades.

À medida que a dependência do MAPA por sistemas e serviços de informação aumenta, crescem também as ameaças cibernéticas que, muitas vezes, resultam em falhas de segurança críticas que, por sua vez, podem gerar centenas de milhões de reais de prejuízo aos cidadãos, além de causar grandes danos à imagem dos Ministérios (provedor e demandantes).

O Gabinete de Segurança Institucional da Presidência da República (GSI/PR) responsável por coordenar as atividades de segurança da informação e das comunicações no governo federal, em sua portaria PORTARIA GSI/PR Nº 120, DE 21 DE DEZEMBRO DE 2022 (https://www.in.gov.br/en/web/dou/-/portaria-gsi/pr-n-120-de-21-de-dezembro-de-2022-452767918) deixa claro as orientações para proteção das entidades publicas do executivo federal, ao qual destacamos:



2. PREVENÇÃO

A prevenção é um processo constante de ações proativas com o objetivo de reduzir a probabilidade de ataques cibernéticos bem-sucedidos. Entre essas ações, enfatizam-se as de definição e de implementação de controles de segurança, de gerenciamento de vulnerabilidades, de conscientização e de capacitação.

As ações preventivas de segurança cibernética deverão contemplar aquelas previstas na política de segurança da informação do integrante da Regic.

2.1. Definição e implementação de controles de segurança preventivos

Os controles de segurança preventivos constituem-se em tecnológicos, organizacionais e físicos.

Os controles tecnológicos são aqueles utilizados para reduzir vulnerabilidades no **hardware** e no **software**. Entre os principais de controles tecnológicos estão:

- dispositivos **endpoint** do usuário;
- restrição de acesso à informação;
- autenticação segura;
- proteção contra **malware**;
- **backup** das informações;
- atividades de monitoramento (log);
- segurança de redes;
- uso de criptografia; e
- gestão de mudanças.

Ainda com relação à portaria citada acima, os controles físicos tem por finalidade prevenir ou evitar o acesso não autorizado à área ou material sensível, bem como os danos e interferências às áreas que contenham informações críticas ou sensíveis. Entre os principais controles físicos estão:

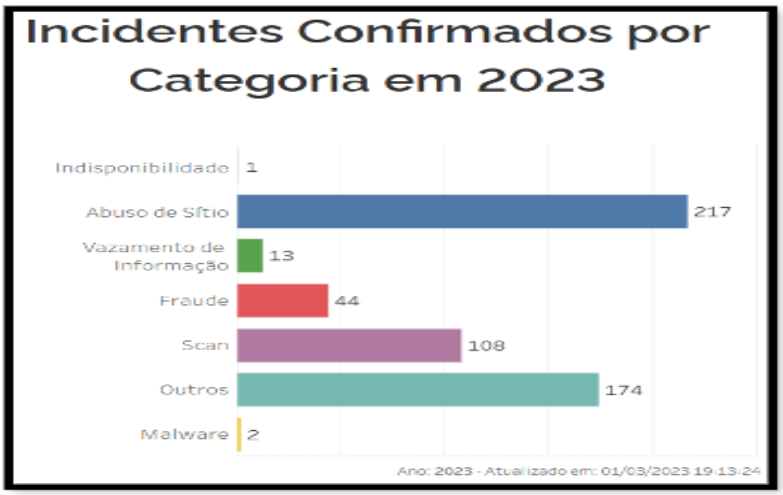
- Definição dos perímetros de segurança física.
- Monitoramento de segurança física.
- Proteção contra ameaças físicas e ambientais.
- Localização e proteção de equipamentos.
- Segurança de ativos fora das instalações da organização e
- Manutenção dos ativos.

Ainda nesta linha o Centro de Prevenção , Tratamento e Resposta a Incidentes Cibernéticos de Governo, entidade que está enquadrada na categoria "CSIRT de responsabilidade nacional de coordenação" publica regularmente relatórios sobre a quantidade de incidentes descobertos (https://www.gov.br/ctir/pt-br/assuntos/ctir-gov-em-numeros/visao-geral) . Vejamos alguns dados importantes:

2019	2020	2021	2022	2023
23.674	24.300	22.298	18.489	3.254
10.716	5.257	4.910	3.786	559
1.201	2.270	3.917	3.189	680

Atualizado em: 01/03/2023 19:13:24

Notificações Incidentes Vulnerabilidades



Percebe-se que a quantidade de incidentes no âmbito do governo federal é extremamente relevante. Em relação à proteção de perímetro, temos que esta é uma das proteções mais importantes em uma instituição, e que se atualizam constantemente por meio de soluções que são conhecidas no mercado como NGFW.

A aquisição de um Next-Generation Firewall (NGFW) pode trazer vários benefícios para uma organização. Entre elas:

- **Proteção avançada contra ameaças:** Um NGFW oferece recursos de segurança avançados que podem proteger contra ameaças cibernéticas, como malware, phishing, ransomware e ataques de dia zero. Isso inclui recursos como detecção de intrusões, filtragem de URL, antivírus, inspeção de tráfego SSL/TLS e muito mais.
- **Controle de acesso a aplicativos:** Um NGFW permite que uma organização controle o acesso a aplicativos específicos, permitindo ou bloqueando o acesso com base em políticas de segurança definidas. Isso ajuda a proteger contra o uso indevido de aplicativos e reduz o risco de violações de dados.
- **Visibilidade e controle de tráfego:** um NGFW fornece uma visão completa do tráfego de rede, permitindo que as organizações monitorem e controlem o tráfego de entrada e saída. Isso pode ajudar a identificar e mitigar atividades suspeitas e proteger contra vazamentos de dados.
- **Gerenciamento centralizado:** um NGFW pode ser gerenciado de forma centralizada, permitindo que as organizações gerenciem políticas de segurança, implementem atualizações e monitorem o tráfego de rede em vários locais a partir de um único console.

Com a Medida Provisória Nº 1.154, de 1º de janeiro de 2023, o compartilhamento de atividades de administração patrimonial, de material, de gestão de pessoas, de serviços gerais, de orçamento e finanças, de contabilidade, de logística, de contratos, **de tecnologia da informação**, de planejamento governamental e gestão estratégica e de outras atividades de suporte administrativo deve ser realizada por meio de arranjos colaborativos entre **Ministérios ou modelos centralizados**, por isso essa contratação também irá atender os Ministérios da Pesca e Aquicultura e Ministério do Desenvolvimento Agrário e Agricultura Familiar. As despesas executadas para a prestação de serviços administrativos compartilhados serão assumidas pelo Ministério demandante, sem necessidade de celebração de termo de execução descentralizada, nos termos do inciso II do § 3º do art. 3º do Decreto nº 10.426, de 16 de julho de 2020.

Dentro do contexto analisado, a substituição da solução de TIC relacionada ao firewall do MAPA e demais Ministérios demandantes (MPA e MDA) é essencial, uma vez que regula o tráfego de dados entre redes distintas e impede a transmissão e recepção de informações a partir de acessos nocivos ou não autorizados na rede, além de trazer outros inúmeros benefícios que serão detalhados ao longo do estudo técnico preliminar quanto no termo de referência.

3.2 - ALINHAMENTO ESTRATÉGICO

ALINHAMENTO AO PAC

UASG	Nº ITEM	TIPO DE ITEM	SUBITEM	CÓDGIO DO ITEM	DESCRIÇÃO	VALOR TOTAL ESTIMADO R$
130005	274	Soluções de TIC.	Serviço de TIC.	22993	Informática - Suporte Técnico (Software Equipamentos)	R$ 2.800.000,00

ALINHAMENTO AO PDTIC/PLANEJAMENTO ESTRATÉGICO DO MAPA

META 7	NECESSIDADE 5	INDICADOR	OBJETIVO ESTRATÉGICO 23
Tornar as informações, dados e conectividade protegidos e 100% compatível com Normativos de Segurança, incluindo a Lei Geral de Proteção de Dados.	Proteger dados, comunicações e ativos que sejam considerados estratégicos ou identifiquem pessoas físicas e jurídicas.	Aderência à LGPD.	Adequar a capacidade da tecnologia da informação aos novos desafios da transformação digital.

4. Área requisitante

Área Requisitante	Responsável
Coordenação Geral de Infraestrutura, Cibersegurança e Serviços de TI - CGINFRA	Marco Antônio Bittencourt Sucupira

5. Necessidades de Negócio

A definição dessas características representa o detalhamento do objeto a ser contratado. A seguir, temos alguns requisitos que devem ser cumpridos.

5.1 - REQUISITOS DE NEGÓCIO (NECESSIDADES E ASPECTOS FUNCIONAIS DA SOLUÇÃO DE TIC)

- Aquisição de solução de segurança de perímetro contemplando o hardware, software, licenciamento, implantação, configuração, treinamento, garantia, atualizações e suporte técnico, em atendimento à solicitação (Documento de oficialização de demanda SEI Nº 27476908 da Cooordenação-Geral de Infraestrutura, Cibersegurança e Serviços da Subsecretaria de Tecnologia da Informação do MAPA e demais Ministérios demandantes (Ministério da Aquicultura e Pesca / Ministério da Desenvolvimento Agrário e Agricultura Familiar.)
- Melhorar e garantia o perfeito funcionamento da infraestrutura de rede do Ministério da Agricultura e Pecuária(MAPA) e seus Ministérios demandantes.
- Prover e Garantir a segurança das informações como também a continuidade dos serviços de TIC.
- Assegurar a confidencialidade, disponibilidade e integridades das informações do MAPA e seus Ministérios demandantes em conformidade com a LGPD.
- Melhorar a identificação e o rastreamento das tentativas de invasão às redes.
- Melhoria na implementação de regras e políticas de seguranças relacionados ao uso da rede computacional.
- Melhorar o nível de qualidade e segurança dos serviços e aplicações internas dos Ministérios (Ministério Provedor e demandantes).
- Melhorar a proteção da infraestrutura de TIC de modo a impedir que a rede seja utilizada para outros fins (por exemplo: Mineração de bitcoins, links de internet utilizados para download de conteúdo ilícito , ataques de negação de serviço-DDOS, entre outros).
- Melhoria no reconhecimento e controle da aplicação para detectar e bloquear aplicativos nocivos.
- Melhorar o tempo de resposta aos ataques com automação de segurança.

5.2 - REQUISITOS LEGAIS (NORMAS COM AS QUAIS A SOLUÇÃO DE TIC DEVE ESTAR EM CONFORMIDADE)

A presente contratação sujeita-se à legislação pertinente, mormente aos diplomas a seguir elencados, bem como às demais normas gerais que se apliquem, considerando-se a legislação consolidada com as respectivas alterações subsequentes:

5.2.1 - LEIS

- Lei Nº 14.133, de 1º de Abril de 2021.
- Lei Nº 13.709, de 14 de Agosto de 2018 e Lei Nº 13.853, de 08 de julho de 2019. (LGPD).

5.2.2 - DECRETOS

- Decreto Nº 10.024/2019: Regulamenta a licitação, na modalidade pregão, na forma eletrônica, para a aquisição de bens e a contratação de serviços comuns, incluídos os serviços comuns de engenharia, e dispõe sobre o uso da dispensa eletrônica, no âmbito da administração pública federal.

- Decreto Nº 9.507/2018: Dispõe sobre a execução indireta, mediante contratação, de serviços da administração pública federal direta, autárquica e fundacional e das empresas públicas e das sociedades de economia mista controladas pela União.
- Decreto Nº 7.174/2010: Regulamenta a contratação de bens e serviços de informática e automação pela administração pública federal, direta ou indireta, pelas fundações instituídas ou mantidas pelo Poder Público e pelas demais organizações sob o controle direto ou indireto da União.
- Decreto-Lei Nº 200, de 25 de fevereiro de 1967 - dispõe sobre a organização da Administração Federal, estabelece diretrizes para a Reforma Administrativa.
- Decreto Nº10.947, de 25 de Janeiro de 2022. (Regulamenta o inciso VII do caput do art. 12 da Lei nº 14.133, de 1º de abril de 2021, para dispor sobre o plano de contratações anual e instituir o Sistema de Planejamento e Gerenciamento de Contratações no âmbito da administração pública federal direta, autárquica e fundacional.)

5.2.3 - INSTRUÇÕES NORMATIVAS

- Instrução Normativa SGD/ME Nº 94, de 23 de Dezembro de 2022 (Dispõe sobre o processo de contratação de soluções de Tecnologia da Informação e Comunicação - TIC pelos órgãos e entidades integrantes do Sistema de Administração dos Recursos de Tecnologia da Informação - SISP do Poder Executivo Federal).
- Instrução Normativa Nº 5 de 25 de maio de 2017 (Dispõe sobre as regras e diretrizes do procedimento de contratação de serviços sob o regime de execução indireta no âmbito da Administração Pública federal direta, autárquica e fundacional.)
- Instrução Normativa SEGES/ME Nº 65, de 7 de Julho de 2021-Dispõe sobre o procedimento administrativo para a realização de pesquisa de preços para aquisição de bens e contratação de serviços em geral, no âmbito da administração pública federal direta, autárquica e fundacional.
- Boas práticas, orientações e vedações para contratação de Ativos de TIC - Versão 4. Orientações específicas para a aquisição de Ativos de TIC. (Este guia está vinculado à Instrução Normativa SGD/ME nº 94, de 23 de dezembro de 2022, conforme § 2º do Art. 8º)
- Instrução Normativa SEGES Nº 58, de 08 de Agosto de 2022. - Dispõe sobre a elaboração dos Estudos técnicos preliminares-ETP, para a aquisição de bens e contratação de serviços e obras, no âmbito da administração pública federal direta, autárquica e fundacional, e sobre o ETP Digital.
- Instrução Normativa Nº 01, de 19 de Janeiro de 2010. (Dispõe sobre os critérios de sustentabilidade ambiental na aquisição de bens, contratação de serviços ou obras pela Administração Pública Federal direta, autárquica e fundacional e dá outras providências.)

5.2.4 - PORTARIAS

- Portaria MGI Nº 43, de 31 de Janeiro de 2023. (Disciplina o compartilhamento de atividades de administração patrimonial, de material, de gestão de pessoas, de serviços gerais, de orçamento e finanças, de contabilidade, de logística, de contratos, de tecnologia da informação, de planejamento governamental e gestão estratégica e de outras atividades de suporte administrativo realizadas por meio de arranjos colaborativos entre Ministérios ou modelos centralizados, e dispõe sobre medidas transitórias decorrentes da edição da Medida Provisória nº 1.154, de 1º de janeiro de 2023.)
- Portaria GSI/PR Nº 120, de 21 de Dezembro de 2022. (Aprova o Plano de Gestão de Incidentes Cibernéticos para a administração pública federal).
- Portaria MAPA Nº 136, de 25 de Maio de 2021 (Aprova a Política de Segurança da Informação do Ministério da Agricultura, Pecuária e Abastecimento - POSIC/MAPA.)
- Portaria MAPA Nº 499, de 17 de Outubro de 2022 - Política de Gestão de Vulnerabilidades Cibernéticas.

5.3 - REQUISITOS DE GARANTIA

- A garantia será prestada com vistas a manter os equipamentos fornecidos em perfeitas condições de uso, sem qualquer ônus ou custo adicional para o MAPA e órgãos demandantes (MPA e MDA).
- Segundo o item 1.4.5.1, "Para aquisição de servidores de rede, aplicação, equipamentos de backup, armazenamento, segurança, entre outros, deve-se considerar o tempo de vida útil mínimo de 5 (cinco) anos para fins de posicionamento da tecnologia e de garantia de funcionamento", do documento "Orientações específicas para a aquisição de Ativos de TIC" vinculado à Instrução Normativa SGD/ME nº 94, de 23 de dezembro de 2022, a garantia recomendada é de 60 meses para os equipamentos de segurança. Apesar de possivelmente ser tecnicamente mais vantajoso a realizar a contratação da garantia por 60 meses, pode ser que financeiramente não seja. Portanto, a garantia/vigência contratual dos itens da contratação será decidida após a realização da pesquisa de preços final conforme a instrução normativa SEGES /ME Nº 65, de 07 de Julho de 2021, diante de uma análise de simulação de cenários de pagamento e decisão da equipe de planejamento.
- Durante o prazo de garantia, deve ser possível realizar a atualização de sistema operacional dos equipamentos e demais licenças/firmwares/softwares fornecidos com o objetivo de obter novas funcionalidades e correção de bugs;
- Durante o prazo de garantia, deve ser possível realizar a atualização das assinaturas de proteção da solução;

- Os chamados poderão ser abertos diretamente com a contratada, autorizada oficial do fabricante ou com o próprio fabricante no Brasil através de ligação telefônica gratuita (0800) no idioma português, website e e-mail durante a vigência da garantia. O suporte deverá ser na modalidade de 24x7x365 (24 horas por dia, 7 dias por semana);
- A contratada deve fornecer garantia de reposição de hardware para situações que sejam identificados problemas constantes na solução fornecida.
- A garantia abrange a realização da manutenção corretiva dos bens pela própria Contratada, ou, se necessário, por meio de assistência técnica autorizada, de acordo com as normas técnicas específicas.
- O custo referente ao transporte dos equipamentos cobertos pela garantia será de responsabilidade da Contratada.

5.4 - REQUISITOS DE MANUTENÇÃO

- Em caso de falha do(s) hardware(s), caso não seja feita a troca imediata, a contratada deve disponibilizar hardware(s) reserva(s) que irá(ão) permanecer em ambiente de produção do MAPA até o retorno do(s) hardware(s) original(is) reparado ou novo em substituição, a critério do **MAPA e órgãos demandantes (MPA e MDA).**
- Deverá assegurar que o hardware substituto, em qualquer caso, seja igual ao contratado inicialmente ou que possua características superiores a este, desde que estejam homologadas pelo fabricante como parte compatível da solução;
- As peças de substituição devem ser novas, **não sendo aceitas peças usadas ou recondicionadas**;
- A substituição do hardware será considerada consumada no momento em que a solução voltar ao seu funcionamento normal e for aceita formalmente pela equipe técnica do **MAPA.**

- **Manutenção Preventiva**

    - A **manutenção preventiva** será destinada a atualizar os componentes do software e a **realizar quaisquer operações que evitem uma parada parcial ou total da solução.**
    - Durante a manutenção preventiva, a contratada deverá analisar toda a solução, sua condição atual de funcionamento, seus logs de sistemas e sugerir mudanças para uma melhor prática de utilização de ferramenta. A equipe técnica do MAPA junto ao fiscal técnico decidirá sobre a aplicação ou não das recomendações.
    - A **manutenção preventiva deverá ser executada pelo menos 02 vezes por mês** conforme cronograma a ser definido entre o fiscal técnico e equipe técnica da contratada.
    - O cronograma anual poderá sofrer adequações durante o ano vigente , desde que a contratada e o MAPA estejam de acordo e que não seja descumprido o atendimento mensal.
    - Deverá ser gerado um **relatório mensal a cada manutenção preventiva**, que deverá ser entregue até **05(cinco) dias após a visita da contratada.**

- **Manutenção Corretiva**

    - A **manutenção corretiva** será destinada a remover os defeitos apresentados pelos componentes de software e hardware de toda solução de TIC do contrato, compreendendo também a atualização de versões e correções dos componentes de software e hardware que se fizerem necessários.
    - A **manutenção corretiva** será realizada **sempre** que a solução apresentar falha que impeça o seu funcionamento regular e necessite de uma intervenção técnica especializada e, caso necessário, a substituição dos componentes.
    - A **manutenção corretiva** pode ser **solicitada a qualquer moment**o em que o sistema apresente pane, deficiência ou dificuldade de operação.
    - As visitas para prestação dos serviços de manutenção preventiva e corretiva, independente da quantidade necessária, **NÃO deve implicar em custos adicionais para o MAPA.**

5.5 - REQUISITOS TEMPORAIS

- O serviço de substituição de hardware será prestado na modalidade 24x7x365, ou seja, estará disponível para acionamento 24 horas por dia, 7 dias por semana, devendo substituir quaisquer peças ou componentes defeituosos em um prazo máximo conforme último tópico estipulado no item 4.5.2.2.2, contados a partir da data de abertura do chamado (ticket de atendimento).
- O prazo indicado no subitem anterior, durante seu transcurso, poderá ser prorrogado uma única vez, por igual período, mediante solicitação escrita e justificada da Contratada, devidamente aceita pelo fiscal técnico do contrato.
- A entrega total , configuração e implantação completa de todos os bens e da solução de TIC deve ocorrer em no máximo 60 dias úteis a partir da assinatura da ordem de serviço, devendo ser agendada com antecedência mínima de 48 horas. Para itens de software, poderá ser fornecido sem mídia de instalação, desde que seja indicado local seguro para download dos arquivos de instalação.
- O treinamento deverá ser iniciado em no máximo 10 dias úteis após a instalação e configuração da solução de TIC contratada.
- A contratada deverá cumprir todos os prazos descritos neste estudo técnico preliminar, respeitando os prazos máximos estabelecidos.
- A seguir, segue um resumo de alguns requisitos temporais mais importantes:

ID	DESCRIÇÃO	PRAZO MÁXIMO (DIAS ÚTEIS)
1	Assinatura do contrato (MAPA e contratada)	Início dos prazos - D
2	Realização da reunião inicial(MAPA e contratada). Apresentação formal da equipe de fiscalização do contrato e do preposto. (contratante e contratada). Repasse à contratada dos conhecimentos necessários à execução dos serviços(MAPA). Entrega do termo de compromisso e de ciência devidamente assinados (contratada).	D + 4
3	Entrega do projeto da implantação (contratada)	D + 9
4	Análise e aprovação do projeto de implantação (MAPA)	D + 14
5	Finalização da execução dos serviços e instalação dos bens. (Contratada)	D
6	Início do treinamento	10 dias após o ID 5 ou a depender da disponibilidade dos recursos do MAPA.

5.6 - REQUISITOS DE SEGURANÇA

Na execução dos serviços contratados, a CONTRATADA deverá zelar, no que for de sua competência, pela garantia da disponibilidade, integridade, confidencialidade e autenticidade das informações custodiadas no ambiente gerenciado. Além disso, deve adotar e se responsabilizar por medidas efetivas quanto ao seguinte:

- A contratada deverá submeter-se à Política de Segurança da Informação e Comunicações e demais normas de segurança vigentes no MAPA. (Portaria MAPA Nº 136, de 25 de Maio de 2021).
- Abster-se, qualquer que seja a hipótese, de veicular publicidade ou qualquer outra informação acerca dos serviços, sem prévia autorização. Ademais, observar, rigorosamente, todas as normas e procedimentos de segurança implementados no ambiente de Tecnologia da Informação - TI do MAPA.
- Normas e instruções normativas do GSI/PR no que se aplicar à respectiva contratação.
- Assegurar o adequado tratamento de dados pessoais e informações classificadas dos quais venha a ter conhecimento ou manusear em razão da execução do objeto do contrato, nos termos da Lei Federal n° 13.709/2018 e em aderência aos requisitos de segurança da informação vigentes no ambiente do MAPA.
- Evitar vazamento de dados e fraudes digitais nos ambientes gerenciados sob sua responsabilidade técnica;

Quanto ao acesso físico, a CONTRATADA:

- Deverá credenciar junto ao MAPA os seus profissionais, caso seja necessário o acesso às instalações da Sede do MAPA e órgãos demandantes (MPA e MDA). para prestação de serviços.
- A contratada deverá apresentar os empregados devidamente uniformizados e identificados por meio de crachá.

5.7 - REQUISITOS SOCIAIS, AMBIENTAIS E CULTURAIS

- Durante a execução de tarefas no ambiente do MAPA, os funcionários da empresa contratada deverão observar, no trato com os servidores públicos em geral, a urbanidade e os bons costumes de comportamento, tais como: asseio, pontualidade, cooperação, respeito mútuo, discrição e zelo com o patrimônio público.
- A documentação e os manuais de operação da solução deverão ser apresentados preferencialmente no idioma Português (Brasil – PT-BR) e, em sua ausência, deverão ser apresentados em idioma Inglês;
- A abertura de chamados técnicos e encaminhamentos de demandas deverão ser realizados, preferencialmente, sob a forma eletrônica, evitandose a impressão de papel. Além disso, as configurações de hardware e software deverão ser realizadas visando alto desempenho com a utilização racional de energia.
- Em conformidade com a IN SLTI/MPOG n. 01/2010, a CONTRATADA deverá cumprir com os seguintes requisitos de sustentabilidade ambiental, quando aplicável:
    - Que os bens sejam constituídos, no todo ou em parte, por material reciclado, atóxico, biodegradável, conforme ABNT NBR – 15448-1 e 15448-2;

- Que sejam observados os requisitos ambientais para a obtenção de certificação do Instituto Nacional de Metrologia, Normalização e Qualidade Industrial – INMETRO como produtos sustentáveis ou de menor impacto ambiental em relação aos seus similares;
- Que os bens devam ser, preferencialmente, acondicionados em embalagem individual adequada, com o menor volume possível, que utilize materiais recicláveis, de forma a garantir a máxima proteção durante o transporte e o armazenamento;
- Que os bens não contenham substâncias perigosas em concentração acima da recomendada na diretiva RoHS (Restriction of Certain HazardousSubstances), tais como mercúrio (Hg), chumbo (Pb), cromo hexavalente (Cr (VI)), cádmio (Cd), bifenilpolibromados (PBBs), éteres difenil-polibromados (PBDEs).

6. Necessidades Tecnológicas

Segue abaixo as especificações técnicas básicas que devem ser cumpridas pela solução de TIC:

REQUISITOS TÉCNICOS GERAIS DA SOLUÇÃO DE TIC

- A comunicação entre os appliances de segurança e o módulo de gerência deve ser através de meio criptografado. Não serão aceitos modelos em listas de end-of-sale, cuja data do fim de vendas seja anterior data da proposta.
- Não serão aceitos modelos em lista de end-of-support, cuja data do fim do suporte seja anterior ao fim da vigência do contrato e/ou do fim do período de garantia e suporte exigido no edital.
- A solução de balanceamento deverá ser fornecida em Alta Disponibilidade do tipo Ativo/Ativo. Transferir todas as regras e configurações dos Firewalls em produção atualmente.
- Tanto os dispositivos físicos (“appliance”) quanto seus softwares deverão ser novos, de primeiro uso, e disponibilizados em suas versões mais atualizadas.
- As funcionalidades de proteção de rede que compõe a plataforma de segurança, podem funcionar em múltiplos equipamentos do mesmo fabricante, desde que obedeçam a todos os requisitos desta especificação (por item/por equipamento). A solução deve suportar o balanceamento entre os appliances de Next generation Firewall ofertados, de modo a permitir que seus throughputs, suas capacidades de análise, capacidades de inspeção bem como todas as funcionalidades pedidas nos itens 01 e 03 e seus subitens sejam somados.
- Os equipamentos dos itens 01, 03 e 06 devem ser do mesmo fabricante, completamente interoperáveis, e devem ser capazes de fazer escalonamento de desempenho com movimentação de appliances dentro da topologia da rede. Autenticação de dois fatores, no que couber, principalmente na plataforma de gerenciamento (item 6 da contratação).
- A solução deve suportar a possibilidade de manutenção dinâmica de um equipamento de um grupo para outro, de acordo com a necessidade da arquitetura definida, sem que haja a perda do tráfego.
- A solução deverá possuir a quantidade de transceptores suficientes para conectar toda a solução à rede corporativa, o que inclui a gerência.

6.1 - REQUISITOS GERAIS DOS ITENS 01 E 03

- Solução integrada de proteção de rede do tipo “Next Generation Firewall” (NGFW), formada pelo conjunto de dispositivos ,obrigatoriamente físicos (appliances), interconectados e operando em modo de alta disponibilidade, com recursos de virtualização de sistemas, filtragem de pacotes, filtro de URL (web-filtering) com controle de transmissão de dados e de acesso à internet, controle de aplicação, controle por meio de identificação de usuários, controle de uso de largura debanda (QoS), VLAN, NAT, VPN, DHCP services (server, client e relay), sistema de prevenção de intrusão (IPS) e prevenção contra ameaças de vírus, spywares e malwares, incluindo os de tipo “Zero Day”.
- Conjunto de dispositivo físico (appliance) de proteção de rede com funcionalidades de Next Generation Firewall (NGFW), sistema operacional embarcado no dispositivo e software para sua gestão e monitoramento, permitindo o controle granular das políticas de segurança de rede, atuando além da camada 2 a 4 do modelo OSI, ou seja, além da filtragem por endereços MAC e endereços e portas TCP/IP, permitindo a configuração de políticas de segurança também por aplicações, incluindo seu conteúdo, usuários e tipos de tráfego de rede, recursos tipicamente executados em camada 7.
- O Firewall NGFW deve ser do tipo “rackmount”, permitindo sua instalação em racks de Datacenter , devendo consumir um espaço no rack de no máximo 4U por dispositivo.
- Não serão aceitos equipamentos servidores (“rack servers”) e sistemas operacionais de uso genérico, como Microsoft Windows ou distribuições Linux para usuários finais, adaptados para funcionar como “appliance” físico, ou seja, a solução como um todo de ser fabricada pelo mesmo fornecedor, tanto em seus componentes físicos de hardware quando seus softwares embarcados principais, sendo vedada solução de software livre.
- Todas as funcionalidades da solução Firewall NGFW deverão operar em caráter permanente, podendo ser utilizadas por tempo indeterminado, mesmo após o fim do contrato, e mesmo que o MAPA não tenha mais o direito de receber atualizações por descontinuidade da solução por parte da fabricante.

- A solução deve suportar a possibilidade de movimentação dinâmica de um equipamento de um grupo para outro, de acordo com a necessidade da arquitetura definida, sem que haja a perda do tráfego.
- A solução deverá ser provida de forma redundante, de modo que se houver a falha de um ou mais dispositivos, outro(s) possa(m) assumir totalmente o controle, sem que haja perda do tráfego.
- A solução deve ser compatível com SNMPv2 e Sv3. Os appliances devem permitir aceso ao equipamento via interface de comando(CLI), console, SSH, além de interface web HTTPS.
- Os appliances deverão vir acompanhados de todos os conectores, cabeamento e peças de fixação no Rack, necessários à sua instalação e funcionamento, conforme as especificações deste Termo de Referência.
- Todos os componentes devem ser próprios para montagem em rack “19” e deverão ser fornecidos pela Contratada, incluindo kit tipo trilho para adaptação, cabos de alimentação, suportes, gavetas e braços, se necessário.

6.2 - REQUISITOS GERAIS DOS ITENS 02 e 04

6.2.1 - REQUISITOS BÁSICOS DO ITEM 02 e 04

REQUISITOS DE SUPORTE/GARANTIA E MANUTENÇÃO

6.2.1.1 - GARANTIA

- A garantia será prestada com vistas a manter os equipamentos fornecidos e demais itens da solução de TIC em perfeitas condições de uso, sem qualquer ônus ou custo adicional para o MAPA e órgãos demandantes (MPA e MDA).
- Segundo o item 1.4.5.1, "Para aquisição de servidores de rede, aplicação, equipamentos de backup, armazenamento, segurança, entre outros, deve-se considerar o tempo de vida útil mínimo de 5 (cinco) anos para fins de posicionamento da tecnologia e de garantia de funcionamento", do documento "Orientações específicas para a aquisição de Ativos de TIC" vinculado à Instrução Normativa SGD/ME nº 94, de 23 de dezembro de 2022, a garantia recomendada é de 60 meses para os equipamentos de segurança. Portanto, a garantia contratual exigida dos bens será de no mínimo 60 meses para os itens 01,03 e 06 ,contada a partir do primeiro dia útil subsequente à data do recebimento definitivo do objeto. Para os itens 02,04,07 e 09, como é inviável realizar o pagamento de todos esses itens em uma parcela, eles terão pagamentos de garantia de forma anual.
- Durante o prazo de garantia, deve ser possível realizar a atualização de sistema operacional dos equipamentos e demais licenças/firmwares/softwares fornecidos com o objetivo de obter novas funcionalidades e correção de bugs. Durante o prazo de garantia, deve ser possível realizar a atualização das assinaturas de proteção da solução;
- Os chamados poderão ser abertos diretamente com a contratada, autorizada oficial do fabricante ou com o próprio fabricante no Brasil através de ligação telefônica gratuita (0800) no idioma português, website e e-mail durante a vigência da garantia. O suporte deverá ser na modalidade de 24x7x365 (24 horas por dia, 7 dias por semana); A contratada deve fornecer garantia de reposição de hardware, pelo prazo de vigência do contrato, para situações que sejam identificados problemas constantes na solução fornecida.
- A garantia abrange a realização da manutenção corretiva dos bens pela própria Contratada, ou, se necessário, por meio de assistência técnica autorizada, de acordo com as normas técnicas específicas.
- Todas as licenças, referentes aos softwares e drivers solicitados, devem estar registrados para utilização do Contratante, em modo definitivo (licenças perpétuas). Ao final do contrato, o MAPA deve ter as licenças mais recentes instaladas em modo definitivo (licenças perpétuas).

O custo referente ao transporte dos equipamentos cobertos pela garantia será de responsabilidade da Contratada. Os serviços de “Garantia” também incluem:

- Solução de problemas relativos à indisponibilidade da solução decorrentes de problemas de fabricação, desenvolvimento ou ocasionada pelo uso normal dos equipamentos.
- Solução de falhas ou defeitos no funcionamento, incluindo a instalação de arquivos para correção dos erros.
- Esclarecimento de dúvidas de alto nível.
- Instalação de novas versões ou atualizações e patches.

Os chamados abertos envolvendo garantia e manutenção deverão ser atendidos conforme os índices de criticidade que serão detalhados no termo de referência.

6.2.1.2 - MANUTENÇÃO

- Em caso de falha do(s) hardware(s), caso não seja feita a troca conforme prazo especificado, a contratada deve disponibilizar hardware(s) reserva(s) que irá(ão) permanecer em ambiente de produção do MAPA até o retorno do(s) hardware(s) original(is) reparado ou novo em substituição, a critério do MAPA e órgãos demandantes (MPA e MDA).
- Deverá assegurar que o hardware substituto, em qualquer caso, seja igual ao contratado inicialmente ou que possua características superiores a este, desde que estejam homologadas pelo fabricante como parte compatível da solução; As peças de substituição devem ser novas, não sendo aceitas peças usadas ou recondicionadas;

- A substituição do hardware será considerada consumada no momento em que a solução voltar ao seu funcionamento normal e for aceita formalmente pela equipe técnica do MAPA.

6.2.1.2.1 - MANUTENÇÃO PREVENTIVA

- A manutenção preventiva será destinada a atualizar os componentes do software e a realizar quaisquer operações que evitem uma parada parcial ou total da solução. Deve compreender a checagem da saúde e funcionamento da solução já implementada, permitindo diagnóstico preciso dos status da atual rede. Ao final de cada manutenção preventiva, deverá ser elaborado um relatório detalhado dos serviços executados.
- Durante a manutenção preventiva, a contratada deverá analisar toda a solução, sua condição atual de funcionamento, seus logs de sistemas e sugerir mudanças para uma melhor prática de utilização de ferramenta. A equipe técnica do MAPA junto ao fiscal técnico decidirá sobre a aplicação ou não das recomendações. A manutenção preventiva deverá ser executada pelo menos 02 vezes por mês conforme cronograma a ser definido entre o fiscal técnico e equipe técnica da contratada.
- O cronograma anual poderá sofrer adequações durante o ano vigente , desde que a contratada e o MAPA estejam de acordo e que não seja descumprido o atendimento mensal.
- A futura contratada deverá realizar manutenção preventiva, realizando: Análise de logs e configurações da solução, identificando possíveis erros, conflitos e as correções necessárias; Análise de desempenho do funcionamento da solução no que diz respeito ao uso de CPU e memória e recomendar ajustes; Análise física dos equipamentos, incluindo verificações de temperatura, ventilação e eventuais alertas de falhas de hardwares; Análise de vulnerabilidades e de pendências de atualizações de versões de firmwares, engines, assinaturas ou qualquer componente da solução passível de atualização e recomendar as ações necessárias para regularização.

6.2.1.2.2 - MANUTENÇÃO CORRETIVA

- A manutenção corretiva será destinada a resolver os defeitos apresentados pelos componentes de software e hardware de toda solução de TIC do contrato, compreendendo também a atualização de versões e correções dos componentes de software e hardware que se fizerem necessários. Ademais, entende-se por manutenção corretiva aquela destinada a corrigir os defeitos apresentados pelos bens, compreendendo a substituição de peças, a realização de ajustes, reparos e correções necessárias.
- Corresponde ao tratamento dos problemas encontrados na operação da solução, incluindo esclarecimentos de dúvidas relacionadas à instalação, configuração, uso e atualização, além de reposição de peças defeituosas.
- A manutenção corretiva será realizada sempre que a solução apresentar falha que impeça o seu funcionamento regular e necessite de uma intervenção técnica especializada e, caso necessário, a substituição dos componentes. A manutenção corretiva pode ser solicitada a qualquer momento em que o sistema apresente pane, deficiência ou dificuldade de operação.
- As visitas para prestação dos serviços de manutenção preventiva e corretiva, independente da quantidade necessária, não deve implicar em custos adicionais para o MAPA.
- Entende-se por "manutenção corretiva", toda atividade do tipo corretiva não periódica que variavelmente poderá ocorrer durante o período de garantia. A atividade corretiva possui suas causas em falhas e erros no software/hardware e trata da correção dos problemas atuais e não iminentes de fabricação dos equipamentos. Essa "garantia" inclui os procedimentos destinados a recolocar em perfeito estado de operação os serviços e produtos ofertados, tais como:
    - **Do hardware:** Desinstalação, reconfiguração ou reinstalação decorrente de falhas de fabricação no hardware, fornecimento de peças de reposição, substituição de hardware defeituoso por defeito de fabricação ou ocasionada pelo uso normal dos equipamentos, atualização da versão de drivers e firmwares, ajustes e reparos necessários, de acordo com os manuais e as normas técnicas específicas para os recursos utilizados.
    - **Do Software:** Desinstalação, reconfiguração ou reinstalação decorrente de falhas de desenvolvimento do software, atualização da versão de software, outros problemas envolvidos, de acordo com os manuais e as normas técnicas específicas do fabricante para os recursos utilizados. Quanto às atualizações pertinentes aos softwares, entende-se como atualização o provimento de toda e qualquer evolução de software, incluindo correções, patches, fixes, updates, service packs, novas releases, versions, builds, upgrades, englobando inclusive versões não sucessivas, nos casos em que a solicitação de atualização de tais versões ocorra durante o período de garantia.
- A contratada deverá substituir as peças quebradas, com defeito ou gastas pelo uso normal dos equipamentos, por outras de configuração igual ou superior, originais e novas, sem que isso implique acréscimo aos preços contratados. Substituir, temporária ou definitivamente, o equipamento defeituoso por outro de mesma marca e modelo e com as mesmas características técnicas, novo e de primeiro uso, quando então, a partir de seu efetivo funcionamento, ficará suspensa a contagem do prazo de reparo, nos casos em que não seja possível o reparo dentro dos prazos máximos estipulados.
- A CONTRATADA fornecerá e aplicará pacotes de correção, em data e horário a serem definidos pelo Contratante, sempre que forem encontradas falhas de laboratório (bugs) ou falhas comprovadas de segurança em software ou firmware dos aparelhos que integrem o objeto do contrato. O atendimento deste requisito está condicionado a liberação pelo fabricante dos pacotes de correção e/ou novas versões de software. Deverá fornecer, ainda, serviços de configuração, instalação, transferência de conhecimento, com licenciamento e garantia durante o período de 60 meses, ao

longo do qual deverão ser fornecidas sem custo adicional todas as correções (patches) e atualizações, inclusive de “firmware”, da solução, sempre que houver adição de novas funcionalidades ou correções.
- A contratada deverá substituir os appliances (itens 01, 03 e 06) componentes e/ou acessórios que apresentem defeitos, de forma definitiva, após a intervenção corretiva nos seguintes prazos:
    - Máximo de 15 dias úteis para os itens 01, 03 e 06.
    - Máximo de 20 dias úteis para os demais componentes e acessórios.

6.3 - REQUISITOS DE PROJETO, IMPLEMENTAÇÃO, IMPLANTAÇÃO E DEMAIS ASPECTOS TÉCNICOS REFERENTE AO ITEM 05

A contratada deverá prestar serviços de instalação e configuração da solução, que compreendem, entre outros, os seguintes procedimentos:

- Reunião de alinhamento para criação do escopo do projeto previamente a instalação.
- Instalação física de todos os equipamentos (hardware) e licenças (softwares) adquiridos no local determinado pela equipe responsável pelo projeto por parte do MAPA. Quando aplicável, considerar instalação em modo Alta Disponibilidade (ativo/passivo e ativo/ativo), a ser decidido no momento da instalação.
- Análise da topologia e arquitetura da rede, considerando todos equipamentos já existentes e instalados.
- Análise do acesso à Internet, sites remotos, serviços de rede oferecidos aos funcionários e aos usuários externos; Migração das regras de firewall existentes e aplicáveis à solução ofertada, considerando a adequação às políticas de aplicações em camada 7.
- Análise do posicionamento de qualquer outro equipamento ou sistema relevante na segurança de qualquer perímetro protegido pela solução.
- Configuração do sistema de firewall, IPS, Filtro URL, Antivírus e Anti-Malware de acordo com as exigências levantadas. Toda configuração do sistema deverá ser realizada de acordo com as melhores práticas recomendadas pelo fabricante da solução ofertada. O fabricante deverá disponibilizar ferramenta gratuita para acompanhamento da evolução da parametrização de proteção dos firewalls afim de garantir a melhor eficiência da solução durante o período de vigência das licenças.
- Configuração do sistema de gerenciamento centralizado considerando adição dos novos appliances.
- Todos os cabos de conexão, acessórios e itens relacionados ao completo funcionamento das soluções adquiridas devem ser fornecidos pela contratada.

6.4 - REQUISITOS REFERENTE AO ITEM 06

A utilização de um appliance físico de gerenciamento centralizado facilita as tarefas de gerenciamentos de regras e políticas em um firewall. Por meio desse gerenciamento centralizado é possível gerenciar diversos appliances por meio de uma única interface. Além disso, é possível acessar registros (logs) de diversos equipamentos. Características técnicas mínimas:

- A solução de gerência deverá ser separada dos appliances de segurança, que irá gerenciar políticas de segurança de todos os firewalls e funcionalidades solicitadas nesse tópico.
- Caso a solução possua licenças relacionadas a capacidade de log indexados e armazenamento, deve ser ofertado a maior capacidade suportada ou ilimitada.
- Caso a solução possua módulo de relatórios estendida, deve ser também entregue junto com a solução.
- Deve possuir solução de gerenciamento e administração centralizado, funcionando ON PREMISES e em nuvem pública, e também possibilitando o gerenciamento dos diversos equipamentos licitados neste termo de referência.
- Suportar validação de regras antes da aplicação.
- Suportar validação das políticas, avisando quando houver regras que ofusquem ou conflitem com outras (shadowing); O gerenciamento da solução deve possibilitar a coleta de estatísticas de todo o tráfego que passar pelos equipamentos da plataforma de segurança.
- O Software de Gestão Centralizada deverá ser homologada e totalmente compatível com os itens 01 e 03.
- Deve permitir a exportação de logs via SCP ou FTP assim como permitir a exportação para soluções de gerenciamento de logs compatível com Syslog.).
- Centralizar a administração de regras e políticas dos Firewalls, usando uma única interface de gerenciamento. O gerenciamento deve permitir/possuir monitoração de logs, ferramentas de investigação de logs e acesso concorrente de administradores.
- Deve permitir controle global de políticas para todos os equipamentos que compõe a plataforma de segurança.
- Deve suportar organizar os dispositivos administrados em grupos: os sistemas virtuais devem ser administrados como dispositivos individuais, os grupos podem ser geográficos, por funcionalidade (por exemplo, IPS), e distribuição física /lógica ou topologia de rede.
- Deve implementar sistema de hierarquia entre os firewalls gerenciados, onde seja possível aplicar configurações de forma granular em grupos de firewalls.
- Deve implementar a criação de perfis de usuários com acesso a plataforma de gerenciamento com definição exata de quais informações e de quais firewalls e grupos de firewalls o usuário terá acesso referente a logs e relatórios.

- Deve permitir que a configuração dos firewalls seja importada de forma automática na plataforma de gerenciamento centralizado e que possa ser usada em outros firewalls e grupos de firewalls.
- Deve mostrar os status dos firewalls em alta disponibilidade a partir da plataforma de gerenciamento centralizado; Através da análise de tráfego de rede, web e DNS, deve suportar a verificação de máquinas potencialmente comprometidas ou usuários com uso de rede suspeito.
- Deve possuir um painel com as informações de máquinas comprometidas indicando informações de endereço IP dos usuários, veredito, número de incidentes, etc....
- O relatório deve apresentar eventos em um único portal (dashboard) e geração de relatório de todas as funcionalidades de segurança que estão ativadas nos firewalls, sendo que deve possuir relatório e telas de apresentação onde consta todo os principais eventos das funcionalidades de controle de aplicação web, filtro URL, prevenção de ameaças (IPS, Antivírus, Anti-Malware e Sandboxing).
- A solução deve permitir o login de múltiplos usuários administradores simultâneos com perfil de escrita, possibilitando agilidade e rapidez no gerenciamento pelo grupo de administradores da solução.
- Deve ser possível exportar os logs em CSV ou TXT.
- Deve possibilitar a geração de relatórios de eventos no formato PDF ou HTML.
- Simular o impacto de segurança das alterações de configuração antes da instalação de acordo com a aderência aos padrões regulatórios apresentados no item anterior.
- Permitir notificação instantânea sobre mudanças de política de segurança que impactam negativamente a segurança. Monitorar constantemente o status de conformidade da solução aos padrões regulatórios informados.
- Destacar potenciais violações de segurança e conformidade, reduzindo o tempo necessário e os erros associados a gestão de conformidade manual.
- Gerar alertas de conformidade notificando os usuários sobre o impacto de suas decisões de segurança trazendo as considerações regulatórias na gestão de segurança.
- Permitir o gerenciamento eficaz das ações e recomendações, facilitando a priorização e programação de itens de ação. Possuir alertas de políticas e os potenciais violações de conformidade.
- Possuir recomendações de segurança acionáveis e orientações sobre como melhorar a segurança.
- Gerar relatórios regulamentares com base nas configurações de segurança em tempo real.
- Permitir que os relatórios possam ser salvos, enviados e impressos.
- Deve permitir a criação de filtros com base em qualquer característica do evento, tais como a origem e o IP destino, serviço, tipo de evento, severidade do evento, nome do ataque, o país de origem e destino etc..
- A solução deve prover, no mínimo, as seguintes funcionalidades para análise avançada dos incidentes:
- Visualizar quantidade de tráfego utilizado de aplicações e navegação.
- Gráficos com principais eventos de segurança de acordo com a funcionalidade selecionada.
- A solução de correlação deve possuir mecanismo para detectar login de administradores em horários irregulares. A solução deve ser capaz de detectar ataques de tentativa de login e senha utilizando tipos diferentes de credencias. Deve suportar a geração de relatório gerencial para apresentar aos executivos os eventos de ataque de forma completamente visual, utilizando gráficos referentes a consumo de banda, ataques sofridos e quantidade de eventos gerados e protegidos.
- Deve permitir a integração com servidores de autenticação LDAP Microsoft Active Directory via Radius.
- Caso a solução possua licenciamento relacionado a capacidade de criação de certificados, deve ser contemplado a sua maior capacidade ou ilimitada.
- Permitir criações de políticas de acesso de usuários autenticada no Active Directory, de forma que reconheça os usuários de forma transparente.
- Geração de painel e relatórios contendo mapas geográficos gerados em tempo real para a visualização das principais ameaças através de origens e destinos do tráfego gerado na Instituição.
- A plataforma de gerência centralizada e monitoração deve possibilitar a visualização dos logs de Firewall, navegação web, conteúdo de arquivos, prevenção de ameaças e Sandbox, todos a partir de um único local centralizado possibilitando a procura correlacionada de logs em uma única tela, como por exemplo pesquisar logs de Antivirus e navegação web simultaneamente na mesma query de pesquisa.
- O relatório das emulações (sandboxing) deve conter, pelo menos, o print screen dos arquivos emulados, assim como todo detalhamento das atividades executadas em filesystem, registros, uso de rede e manipulação de processos e o relatório das emulações deverá ser individualizado para cada SO emulado.
- A plataforma de gerência centralizada e monitoração deve possibilitar a procura por endereços IP e redes, sendo que os resultados mostrem estas informações nos campos de origem e destino dos logs na mesma tela de pesquisa.
- Possuir mecanismo para que logs antigos sejam removidos automaticamente. Possuir a capacidade de personalização de gráficos como barra, linha e tabela.
- Deve permitir a criação de dashboards customizados para visibilidades do tráfego de aplicativos, categorias de URL, ameaças, serviços, países, origem e destino.
- Deve possuir a capacidade de visualizar na interface gráfica da solução, informações do sistema como licenças, memória, disco e uso de CPU.
- A solução deve ser capaz de correlacionar eventos de todas as fontes de log em tempo real. A solução deve fornecer conteúdo de correlação pré-definido organizado por categoria. A solução deve ser capaz de personalizar e criar regras de correlação.

- A solução deve fornecer uma interface gráfica para criação das regras citadas no item anterior.
- A solução deve possuir painéis de eventos em tempo real com possibilidade de configuração das atualizações e frequências.

6.5 - REQUISITOS REFERENTE AO ITEM 07

- Suporte, garantia e manutenção, compreendendo a atualização do software com o objetivo de obter novas funcionalidades e correções de bugs. No que couber e sempre que necessário, os demais de suporte, garantia e manutenção deste item, serão os mesmos que estão especificados no tópico 4.5.2 e seus subitens (Requisitos de suporte /garantia/manutenção).

6.6 - REQUISITOS REFERENTE AO ITEM 08

- Treinamento oficial sobre a solução de Firewall NGFW oferecida, a ser ministrada aos colaboradores do MAPA(no mínimo 03 pessoas) que atuarão diretamente na administração e operação da solução após sua implementação, com carga horária mínima de 30 horas ou carga horária oficial. Obrigatoriamente, é necessário emitir certificado de participante para 03 pessoas e outros colaboradores poderão participar como ouvintes.
- O treinamento deve iniciar em no máximo 10 dias úteis após a instalação e configuração da solução contratada ou a depender da disponibilidade do pessoal do MAPA.
- Os dias e horários para capacitação serão definidos pelo MAPA, conforme demanda do mesmo, podendo optar por utilizar apenas meio período do dia(ou até menos, se necessário) até completar a carga total prevista, e serão acordados com a contratada com uma antecedência mínima de 15 dias corridos antes do início do treinamento.
- O treinamento deverá abranger tanto teoria quanto exercícios práticos, voltados para conhecimento da arquitetura da solução, sua implantação, configuração/operação e gerenciamento, administração e monitoramento da solução, contemplando todos os aspectos essenciais de funcionamento, além de tratamento de problemas típicos envolvendo a operação da solução. Ademais, deve cobrir os seguintes tópicos: Arquitetura da solução; Configurações iniciais básicas; Alta disponibilidade; Controle de acesso dos administradores da solução; Configuração de Interfaces; Criação e gerenciamento de Zonas de Segurança, Políticas de Segurança e Endereçamento NAT; Controle por Identificação de Aplicações; Controle por Identificação de Usuários, com conexão a fontes externas de autenticação; Criação e gerenciamento de Filtro URL; Descriptografia de tráfego; Configurações de VPN (SSL e IPSec); Monitoramento e Relatórios; Log e Auditoria.
- Deverá ser fornecido certificado a cada um dos servidores públicos participantes do treinamento. A apresentação destes certificados é requisito obrigatório para a comprovação da execução do serviço, sendo o principal artefato a ser utilizado pela equipe de fiscalização contratual para validação do serviço e emissão do Termo de Recebimento Definitivo da solução.
- Todo material didático a ser utilizado deverá ser fornecido pela contratada ou pelo fabricante, devendo esse ser uma documentação oficial do próprio fabricante, impresso ou em PDF com todos os tópicos abordados no treinamento, inclusive com exemplos práticos e ilustrações.
- O instrutor deve ser profissional certificado pelo fabricante dos produtos e com experiência comprovada nos produtos fornecidos.

A critério do MAPA, o treinamento poderá ocorrer em:

- Nas instalações do MAPA. Neste caso, a contratada arcará com todas as despesas relativas e necessárias, tais como transporte, hospedagem e diárias do(s) instrutor(es); infraestrutura complementar da sala e instalações; material didático e coffee break, e demais gastos para a execução do treinamento;
- Em Brasília-DF. A contratada arcará com todas as despesas relativas e necessárias, tais como transporte, hospedagem e diárias do(s) instrutor(es); infraestrutura da sala, das instalações e equipamentos; material didático e coffee break, e demais gastos para a execução do treinamento.

6.7 - REQUISITOS REFERENTE AO ITEM 09

Deverá ter a característica de Zero Trust Network Access e funcionalidades para no mínimo 500 usuários simultâneos com os seguintes aspectos:

- Deve ser composta pelos agentes a serem instalados nas máquinas dos usuários finais, bem como por um proxy de acesso, o qual concentrará as requisições dos agentes para acesso às aplicações corporativas.
- Deve controlar o acesso por sessão, validando o usuário e dispositivo, bem como estabelecendo um túnel criptografado de modo automático para cada sessão.
- Deve prover um método para controlar o acesso, identificando o dispositivo do usuário, autenticação e postura com base em tags de Zero Trust.
- A solução de proxy de acesso deve prover suporte a um método de publicação de aplicações corporativas sem necessidade de agente, tal como mediante um portal web SSL a ser acessado por cada usuário.

- Deve permitir o gerenciamento dos agentes remotamente, a partir de uma console central do próprio fabricante a ser disponibilizada em nuvem.
- Deve ser escalável até 3.000 agentes.
- O licenciamento deve se basear no número de agentes registrados na console de gerenciamento central do mesmo fabricante.
- Deve ser compatível com pelo menos os seguintes sistemas operacionais: Microsoft Windows: 7 (32 e 64 bits), 8.1 (32 e 64 bits), 10 (32 e 64 bits) e 11 (64 bits); Microsoft Windows Server: 2008 R2, 2012, 2012 R2, 2016, 2019 e 2022; Mac OS X: versões 13, 12, 11 e 10.15; Linux: Ubuntu 18.04 e posterior, Debian 11 e posterior, CentOS Stream 8, CentOS 7.4 e posterior, RedHat 7.4 e posterior, Fedora 36 e posterior.
- Deve dispor de mecanismos para analisar a requisição TLS Client hello e o cabeçalho HTTP User-Agent para determinar e controlar se a requisição está partindo de um dispositivo não passível de gerenciamento pela console central, tal como um dispositivo móvel.
- A comunicação de controle entre os agentes e a console central deve ser criptografada e acontecer através de TCP e TLS 1.2 e 1.3.
- Tanto mediante agente ou sem agente deve ser possível habilitar MFA (autenticação multifator) no processo de autenticação dos usuários.
- A console central deve emitir, assinar e instalar automaticamente um certificado para os agentes contendo ID único de cada agente, número de série do certificado e número de série da console central. O certificado emitido deverá ser único por agente e deverá ainda ser compartilhado com o proxy de acesso.
- Deve ser possível revogar o certificado de um agente por meio da console central.
- O certificado emitido deve ser utilizado no processo de autenticação via ZTNA para identificar o dispositivo do usuário final junto ao proxy de acesso.
- No passo de identificação do dispositivo mediante certificado deve ser possível averiguar se o identificador único do agente e número do certificado coincidem com o que o proxy de acesso conhece. Caso algum desses dados esteja diferente, o acesso deverá ser bloqueado por padrão.
- Deve ser possível configurar o idioma que o agente utiliza para, pelo menos, inglês, português, espanhol ou ainda usar o idioma do sistema operacional.
- A solução deve prover backup automático diariamente, permitindo que em um evento crítico seja possível restaurar os dados de até 05 dias anteriores ao ocorrido.
- Deve existir a possibilidade de restringir o usuário de realizar backup da configuração do agente.
- Deve ser possível enviar os logs para uma ferramenta de consolidação de logs do mesmo fabricante, visando consolidar os logs do proxy de acesso ZTNA em conjunto com os logs dos agentes.
- A solução deve suportar casos de uso utilizando IPv6 puro, bem como IPv6 em conjunto com IPv4.
- Deve ser possível agrupar agentes em grupos e atribuir grupos de agentes a perfis de políticas específicas.
- Deve ser possível exigir uma senha para desconectar o agente da console central.
- Deve ser possível evitar que o usuário realize shutdown do agente após estar registrado na console central. A console central deve apresentar um resumo das informações de cada endpoint, tais como nome do dispositivo, sistema operacional, IP privado, endereço mac, IP público, estado da conexão com a console central, zero trust tags associadas, detalhes da conexão de rede cabeada e WiFi, detalhes do hardware como modelo do dispositivo, fabricante, CPU, RAM, número de série e capacidade de armazenamento. Deve permitir ainda facilmente ver detalhes de qual política está associada com cada agente, qual versão de agente está em uso em um respectivo endpoint, número de série do agente, identificador único e número de série do certificado emitido para o processo de ZTNA.
- Deve permitir criação de regras de conformidade que avaliem à postura do dispositivo e auxiliem oadministrador no controle de acesso à recursos da infraestrutura, impedindo que um cliente não conforme possa se conectar a redes críticas.
- A console central deve permitir mapear as regras de destinos de ZTNA a serem sincronizadas com os endpoints e permitir ainda definir para qual tráfego deve ser aplicada criptografia, tal como para tráfego HTTP sem criptografia nativa.
- Deve possibilitar definir funções administrativas relacionadas às permissões dos endpoints, de políticas e de configurações gerais.
- Deve permitir criação de regras de conformidade que avaliem à postura do dispositivo e auxiliem o administrador no controle de acesso à recursos da infraestrutura, impedindo que um cliente que não esteja em conformidade possa se conectar a redes críticas.
- Deve ser possível aplicar um patch automático com base no nível de criticidade definido, tal como atualizar automaticamente patches considerados críticos.
- A console central deve possuir funcionalidade de rastreamento de vulnerabilidades a nível de endpoint, permitindo ainda definir o rastreamento no momento do registro, quando ocorrer uma atualização de uma assinatura vulnerável, bem como patches e atualizações de segurança a nível de sistema operacional. Além disso, deve ser possível agendar quando o rastreamento deve ocorrer ou vinculá-lo em conjunto com a janela de manutenção automática do Windows.
- Deve ser possível configurar o filtro de URL com base em caracteres curingas ou expressões regulares (regex) com as opções de permitir, bloquear ou monitorar.

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

7.1 - REQUISITOS SOCIAIS, METODOLOGIA DO TRABALHO, AMBIENTAIS E CULTURAIS

- Durante a execução de tarefas no ambiente do MAPA, os funcionários da empresa contratada deverão observar, no trato com os servidores públicos em geral, a urbanidade e os bons costumes de comportamento, tais como: asseio, pontualidade, cooperação, respeito mútuo, discrição e zelo com o patrimônio público.
- A documentação e os manuais de operação da solução deverão ser apresentados preferencialmente no idioma Português (Brasil – PT-BR) e, em sua ausência, deverão ser apresentados em idioma Inglês;
- A abertura de chamados técnicos e encaminhamentos de demandas deverão ser realizados, preferencialmente, sob a forma eletrônica, evitandose a impressão de papel. Além disso, as configurações de hardware e software deverão ser realizadas visando alto desempenho com a utilização racional de energia.
- Em conformidade com a IN SLTI/MPOG n. 01/2010, a CONTRATADA deverá cumprir com os seguintes requisitos de sustentabilidade ambiental, quando aplicável:
    - Que os bens sejam constituídos, no todo ou em parte, por material reciclado, atóxico, biodegradável, conforme ABNT NBR – 15448-1 e 15448-2;
    - Que sejam observados os requisitos ambientais para a obtenção de certificação do Instituto Nacional de Metrologia, Normalização e Qualidade Industrial – INMETRO como produtos sustentáveis ou de menor impacto ambiental em relação aos seus similares;
    - Que os bens devam ser, preferencialmente, acondicionados em embalagem individual adequada, com o menor volume possível, que utilize materiais recicláveis, de forma a garantir a máxima proteção durante o transporte e o armazenamento;
    - Que os bens não contenham substâncias perigosas em concentração acima da recomendada na diretiva RoHS (Restriction of Certain HazardousSubstances), tais como mercúrio (Hg), chumbo (Pb), cromo hexavalente (Cr (VI)), cádmio (Cd), bifenilpolibromados (PBBs), éteres difenil-polibromados (PBDEs).
- É dever da Contratada observar entre outras: o menor impacto sobre recursos naturais como flora, fauna, ar, solo e água; preferência para materiais, tecnologias e matériasprimas de origem local; maior eficiência na utilização de recursos naturais; maior geração de empregos; maior vida útil e menor custo de manutenção do bem; uso de inovações que reduzam a pressão sobre recursos naturais; e origem ambientalmente regular dos recursos naturais utilizados nos bens e serviços.
- O MAPA será a responsável pela verificação da aderência aos padrões de qualidade exigidos dos produtos entregues. A Contratada será responsável pelo fornecimento do software e gestão dos recursos humanos e materiais necessários para a prestação da garantia.

7.2 - REQUISITOS DE EXPERIÊNCIA PROFISSIONAL/ FORMAÇÃO DA EQUIPE

- Os profissionais que irão implantar a solução de TIC (Itens 01,03,05 e 06) devem ter experiência mínima de 03 anos em implantações/configurações da solução adquirida ou similar. Os atestados que comprovem essa experiência precisam ser apresentados formalmente. Os profissionais envolvidos deverão possuir certificado/certificação ou curso oficial fornecido pelo fabricante que o credencie na implantação da solução contratada ou similar.
- Para os itens 02,04,05,07 e 09 da contratação é solicitado o mesmo tempo de experiência em soluções correlatas ou de maior complexidade. A contratada deve ter profissional(is), pelo menos 01(um) profissional, com certificação, certificado ou curso oficial do fabricante que comprove o conhecimento prático nos respectivos itens da contratação.
- Já para o item 08 (treinamento) , o instrutor deve ter formação comprovada através de certificação/certificado ou curso oficial do fabricante e experiência em treinamentos de no mínimo 02 anos, devendo ser comprovado formalmente com documentos oficiais.

7.3 - REQUISITOS DE SEGURANÇA DA INFORMAÇÃO E PRIVACIDADE

Na execução dos serviços contratados, a CONTRATADA deverá zelar, no que for de sua competência, pela garantia da disponibilidade, integridade, confidencialidade e autenticidade das informações custodiadas no ambiente gerenciado. Além disso, deve adotar e se responsabilizar por medidas efetivas quanto ao seguinte:

- A contratada deverá submeter-se à Política de Segurança da Informação e Comunicações e demais normas de segurança vigentes no MAPA. (Portaria MAPA Nº 136, de 25 de Maio de 2021).
- Abster-se, qualquer que seja a hipótese, de veicular publicidade ou qualquer outra informação acerca dos serviços, sem prévia autorização. Ademais, observar, rigorosamente, todas as normas e procedimentos de segurança implementados no ambiente de Tecnologia da Informação - TI do MAPA.
- Normas e instruções normativas do GSI/PR no que se aplicar à respectiva contratação.
- Assegurar o adequado tratamento de dados pessoais e informações classificadas dos quais venha a ter conhecimento ou manusear em razão da execução do objeto do contrato, nos termos da Lei Federal n° 13.709/2018 e em aderência aos requisitos de segurança da informação vigentes no ambiente do MAPA.
- Evitar vazamento de dados e fraudes digitais nos ambientes gerenciados sob sua responsabilidade técnica.

- A contratada deverá assinar o termo de compromisso de manutenção de sigilo para fins de segurança de dados e da prestação do serviço, conforme o modelo de Termo de compromisso de Manutenção de Sigilo (https://www.gov. br /governodigital/pt-br/contratacoes/templates-e-listas-de-verificacao).
- Os colaboradores da contratada que atuarem nos serviços iniciais e durante toda a vigência do contrato e do prazo de suporte e garantia, deverão assinar o termo de ciência, conforme o modelo no Anexo-Termo de Ciência (https://www. gov.br/governodigital/pt-br/contratacoes/templates-e-listas-de-verificacao).
- A contratada deverá obedecer, quando aplicável, as normas de segurança da família ISO/IEC 27000.
- A contratada deverá manter sigilo, sob pena de responsabilidade civil, penal e administrativa, no que diz respeito a todo e qualquer assunto de interesse do MAPA ou de terceiros de que tomar conhecimento em razão da execução do objeto deste documento, devendo orientar seus empregados nesse sentido.
- A contratada deverá manter em caráter confidencial, mesmo após o término do prazo de vigência ou rescisão do contrato, as informações de que vier ter acesso durante a execução do contrato.
- A contratada deverá implementar processo de gestão de capacidade e recursos para redundância de forma que a utilização dos recursos seja monitorada, ajustada e as projeções das necessidades de capacidade futura sejam avaliadas para garantir o desempenho dos ativos relacionados ao objeto do contrato, assegurando também a disponibilidade e recuperação de dados e informações, em conformidade com um plano de continuidade relacionado ao objeto contratado, que garanta o nível requerido de continuidade para a segurança da informação durante uma situação adversa.
- A contratada deverá manter controles e procedimentos específicos para assegurar o nível adequado de segurança da informação às redes corporativas da Contratante e da Contratada, de forma a reduzir o nível de risco ao qual a Solução de TIC e a contratante estão expostos, considerando os critérios de aceitabilidade de riscos definidos pela contratante;
- A contratada deverá implementar e manter controles específicos para registro de eventos e rastreabilidade de forma a manter trilha de auditoria de segurança da informação e privacidade, aderente a disposto em dispositivo legal correlato publicado pelo GSI/PR, de forma a assegurar a rastreabilidade do tráfego por meio de logs de transações e acessos, conforme especificação de requisitos, e gerá-los e disponibilizá-los à contratante para fins de auditorias e inspeções.
- A contratada deverá utilizar recursos de segurança da informação e de tecnologia da informação de qualidade, eficiência e eficácia reconhecidas e em versões comprovadamente seguras e atualizadas, de forma reduzir o nível de risco ao qual o objeto do contrato e/ou a contratante está exposta, considerando os critérios de aceitabilidade de riscos definidos pela contratante.
- A contratada deverá implementar e manter controles e procedimentos específicos para assegurar completo e absoluto sigilo quanto a todos os dados e informações de que o preposto ou os demais empregados da contratada venham a tomar conhecimento em razão da execução do contrato, de forma a assegurar que seus empregados e outros profissionais sob sua direção e/ou controle respeitem o uso dos dados somente para as finalidades previstas em contrato e as restrições de uso dos ativos utilizado para desenvolvimento e/ou operação da Solução de TIC, cumprindo e fazendo cumprir o disposto nos Termo de Compromisso e Termo(s) de Ciência firmados respectivamente, pelo representante legal e pelo(s) empregado(s) da contratada.
- Todas as informações, documentos e especificações técnicas as quais a contratada tiver acesso em função da execução contratual deverão ser tratadas como confidenciais, sendo vedada sua reprodução, utilização ou divulgação à terceiros, devendo essa zelar pela manutenção do sigilo absoluto do conhecimento adquirido.

7.4 - REQUISITOS DE VISTORIA TÉCNICA

- A avaliação prévia do local de execução dos serviços é imprescindível para o conhecimento pleno das condições e peculiaridades do objeto a ser contratado, sendo assegurado ao interessado o direito de realização de vistoria prévia, acompanhado por servidor designado para esse fim, de segunda à sexta-feira, das 09:00 às 12:00 / 14:00 às 17:00 horas.
- Embora opcional, é recomendável a realização de visita técnica, e esta deve ser realizada até 03 (três) dias antes da data fixada para a sessão pública, mediante agendamento prévio de acordo com os contatos da Subsecretaria de Tecnologia da Informação do MAPA através dos e-mails: coseg@agro.gov.br e/ou cginfra.sti@agro.gov.br. (Telefone 3218-2208). A realização da visita técnica não se consubstancia em condição para a participação na licitação, ficando, contudo, as licitantes cientes de que após a apresentação das propostas não serão admitidas, em hipótese alguma, alegações no sentido da inviabilidade de cumprir com as obrigações, em face do desconhecimento dos serviços e de dificuldades técnicas não previstas.
- Para vistoria, o representante legal da empresa ou responsável técnico deverá estar devidamente identificado, apresentando documento de identidade civil e documento expedido pela empresa comprando sua habilitação para a realização da vistoria.
- O MAPA emitirá "Declaração de Realização de Vistoria Técnica", ao qual deverá ser apresentado junto a proposta de preços, conforme Anexo-Vistoria, deste Termo de Referência para os licitantes que fizerem a vistoria.
- Caso o licitante opte por não realizar a vistoria, deverá prestar declaração formal assinada pelo responsável técnico do licitante acerca do conhecimento pleno das condições e peculiaridades da contratação (Conforme anexo-Vistoria). A

não realização da vistoria não poderá embasar posteriores alegações de desconhecimento das instalações, dúvidas ou esquecimentos de quaisquer detalhes dos locais da prestação dos serviços, devendo o contratado assumir os ônus dos serviços decorrentes.

7.5 . FORMA DE PAGAMENTO

7.5.1. O artigo 40, inciso I, da Lei 14.133 de 2021, estabelece que as compras públicas, sempre que possível, devem pautar-se pelas condições de aquisição e pagamento semelhantes às do setor privado, confirmado pelo Acórdão 1177/2014 – Plenário, sendo juridicamente viável aquisição de bens de informática, com a prestação de garantia por determinado período, mediante pagamento integral no momento da entrega e aceitação dos equipamentos.

> *“Art. 15. As compras, sempre que possível, deverão: (...)*
> *III - submeter-se às condições de aquisição e pagamento semelhantes às do setor privado;” Lei 8.666/1993 (GRIFO NOSSO) e "Jurisprudência - Número 196*
> *É juridicamente viável a aquisição de bens de informática, com a prestação de garantia por determinado período, mediante o pagamento integral no momento da entrega e aceitação dos equipamentos.*
> *Consulta apresentada pelo Presidente do Tribunal Superior do Trabalho indagou ao Tribunal a possibilidade de aquisição de bens de informática, com a prestação de garantia (assistência técnica de preços e serviços) por determinado período, mediante o pagamento integral do valor contratado no momento da entrega e aceitação dos equipamentos. O relator, de início, mencionou que o objeto da Consulta não trata de pagamento antecipado “típico”, em que a entrega do numerário ao fornecedor é feita antes do recebimento do bem ou serviço pela Administração. Na espécie, trata-se de contratação de equipamentos de informática, em que está embutida a prestação de um serviço (assistência técnica durante o período de garantia), distinção que, na ótica do relator, tem relevância, pois no pagamento antecipado o risco para a Administração configura-se bem maior, já que efetuado antes de qualquer contraprestação por parte do fornecedor. Na situação em tese, o pagamento só seria realizado após o recebimento do bem, objeto principal da contratação. A prestação futura referiria-se apenas ao serviço de suporte técnico durante o período de garanti a, espécie de acessório em relação ao objeto principal. Depois de estabelecer tal distinção, o relator concluiu que é possível a contratação de bens de informática, com a prestação de garanti a, realizando-se o pagamento integral do valor contratado quando do recebimento dos bens." (GRIFO NOSSO)*

7.5.2 . O pagamento antecipado da garantia no momento da entrega e aceitação dos equipamentos é, em tese, considerado, por vezes em diversos órgãos da APF uma prática comum e aceitável. Entende-se que isto se dê pela mitigação de riscos inerentes às variações econômicas, crises e volatilidades, enfrentados em um cenário de 5 (cinco) anos de prestação de serviço.

7.5.3 . Esse entendimento é explicitado no Acórdão TCU 2569/2018 que tratou da auditoria operacional, práticas comerciais adotadas por grandes fabricantes de tecnologia da informação (TI) na relação com a administração pública, por ocasião da contratação de licenciamento de software e seus serviços agregados, em que os serviços agregados são normalmente comercializados junto com as licenças na primeira aquisição, quando têm a conotação de “garantia”, remetendo-se ao Código de Defesa do Consumidor, sendo a renovação opcional após o fim da vigência do primeiro período contratado. Nesse contexto, costuma-se, inclusive, exigir o pagamento à vista:

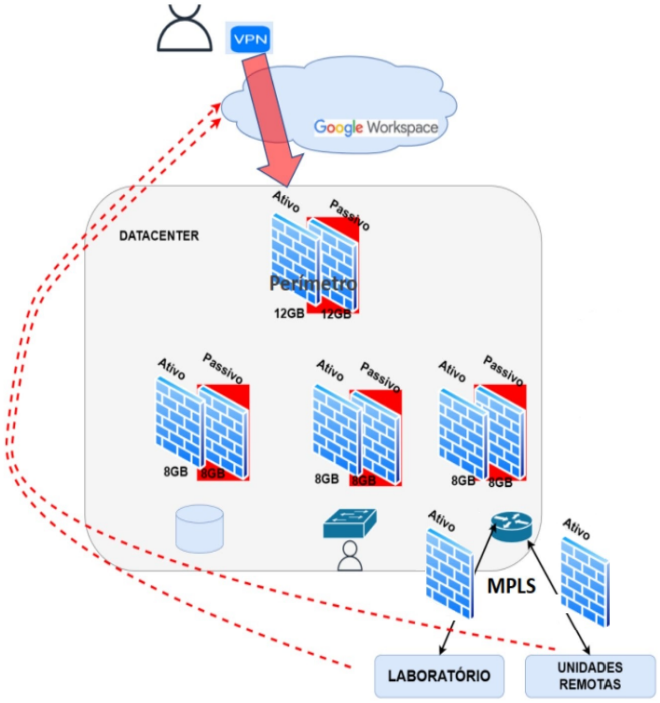
> *"156. Os fabricantes costumam exigir o pagamento à vista para o fornecimento de licenças e de serviços agregados, o que pode resultar na não utilização dos itens adquiridos devido à demora para viabilizar a utilização do software ou à interrupção de projetos. Por outro lado, o pagamento parcelado costuma incluir um custo financeiro da operação no preço final obtido pelas organizações públicas." (GRIFO NOSSO)*
> *"157. Os grandes fabricantes de soluções de TI costumam adotar, no país e também no exterior, a venda de licenças e de serviços agregados mediante recebimento de quantia à vista, seja quando a venda é direta, seja por intermédio de um representante (peça 69, p. 4, questão 6.b; peça 92, p. 4, questões 6.2 e 6.3; peça 95, p. 3, questão 6.2; peça 100, p. 2). Tanto as licenças quanto os serviços agregados possuem peculiaridades que devem ser consideradas pelos gestores na decisão de optar-se pelo pagamento à vista ou parcelado durante o processo da contratação. Além disso, a compra de licenças e de serviços agregados deve ocorrer em momento oportuno dos projetos para evitar que haja dispêndio de recursos em período no qual não há utilização desses itens." (GRIFO NOSSO)*
> *"172. O modelo de pagamento à vista é adotado pela maioria dos fabricantes tanto para licenças como para serviços agregados (parágrafo 157)." (GRIFO NOSSO)*

7.5.4 . Diante do exposto, o posicionamento pelo pagamento à vista dos itens 01 ao 09 referente à prestação de serviços agregados de garantia e suporte será analisado com maior detalhes durante a pesquisa completa de preços. Ademais, justificativas adicionais podem ser descritas no termo de referência ou a forma de pagamento/vigência contratual pode ser alterada de acordo com a consolidação da pesquisa de preços.

8. Estimativa da demanda - quantidade de bens e serviços

8.1 - CONTEXTUALIZAÇÃO DA DEMANDA

Atualmente o parque computacional de perímetro do MAPA conta com a seguinte arquitetura:



Nota-se que é de posse do MAPA os seguintes equipamentos de Firewall, distribuídos da seguinte forma:

- 12 Gbps Throughput para perímetro. Sendo 1 equipamento de 12Gbps como ativo e outro equipamento de 12Gbps como passivo.
- 9 Gbps Throughput para aplicações e banco de dados. Sendo 1 equipamento de 9 Gbps como ativo e outro equipamento de 9Gbps como passivo.
- 9 Gbps Throughput para intranet. Sendo 1 equipamento de 9 Gbps como ativo e outro equipamento de 9 Gbps como passivo.
- 9 Gbps Throughput para rede MPLS ligada a localidades remotas. Sendo 1 equipamento de 9 Gbps como ativo e outro equipamento de 9 Gbps como passivo.
- 27 (SFA- Superintendências Federais de Agricultura) 4 Gbps Throughput para rede MPLS ligada a Sede do MAPA. Sendo 1 equipamento ativo.
- 6 (LFDA - Laboratórios Federais de Defesa Agropecuária) 4 Gbps Throughput para rede MPLS ligada a Sede do MAPA. Sendo 1 equipamento ativo.

Tais equipamentos encontram-se em operação constante e com sua capacidade computacional sendo consumida pelo MAPA. Para o estudo em questão, estima-se uma arquitetura similar com a mesma quantidade de equipamentos, com interesses de trafégos diferentes , de modo a prover flexibilidade e redundância ao MAPA. Além disso, trazendo os outros benefícios que a solução atual não proporciona ao MAPA.

Recentemente, com o novo contrato de prestação de serviços de Internet para o MAPA, de abrangência nacional, os Firewalls que atualmente estavam em uso nas SFAs e LFDAs tiveram que ser desativados pois, além de estarem obsoletos, não eram capazes de prestar o serviço de SDWAN, modalidade de conectividade contratada no contrato 03/2023. Diante desse cenário, todo o papel de filtragem de conteúdo e proteção por regras de ACL será encaminhado para os equipamentos da SEDE. Desta forma, os firewalls da SEDE passarão a fazer o papel de Web Filter, IPS/IDS e Firewall por ACL para a SEDE, as 27 unidades regionais, Laboratórios Federais de Agricultura e demais unidades descentralizadas do Mapa, do MDA e do MPA, que totalizam 81 pontos de acesso, assumindo o papel de 33 firewalls regionais e mais 8 firewalls que atualmente atendem a SEDE.

Fora as mudanças de arquitetura do ministério, temos também o crescimento orgânico do tráfego que devemos a diversos fatores, como:

- **Recursos mais ricos:** Novas aplicações geralmente têm recursos mais avançados, como streaming de vídeo em alta definição, realidade virtual ou aumentada, o que exige mais conexões e trafego para funcionar de forma eficiente.

- **Integração de serviços:** Muitas aplicações modernas se conectam a diversos serviços, onde mais trafego e conexões são necessárias para acessar esses recursos.
- **Compartilhamento de dados em tempo real:** Aplicações mais recentes frequentemente dependem de trocas de dados em tempo real, como mensagens instantâneas, videoconferências e colaboração em tempo real.
- **Segurança:** Novas aplicações também tendem a ser mais preocupadas com a segurança, o que pode envolver o uso de várias conexões para autenticação, criptografia e proteção contra ameaças cibernéticas.

As taxas de crescimento específicas de data centers podem variar dependendo de estudos individuais, fontes de dados e metodologias de análise. No entanto, algumas organizações e empresas de pesquisa frequentemente publicam relatórios e estudos sobre o crescimento do tráfego de data centers e da internet em geral. Alguns desses estudos são:
1. Cisco Global Cloud Index (GCI): A Cisco publica periodicamente o Cisco GCI, que oferece insights sobre as tendências de tráfego de data centers, uso de nuvem e previsões para o futuro. Este relatório é uma referência na área. (https://www.cisco.com/c/dam/m/en_us/service-provider/ciscoknowledgenetwork/files/622_11_15-16-Cisco_GCI_CKN_2015-2020_AMER_EMEAR_NOV2016.pdf)
2. Relatórios da empresa de análise de mercado IDC: A IDC (International Data Corporation) publica pesquisas e relatórios que incluem previsões sobre o crescimento do tráfego de data centers, bem como tendências em tecnologia da informação e comunicações. (https://www.idc.com/getdoc.jsp?containerId=US49018922).

Com isso, podemos estimar que, no mínimo, os novos equipamentos terão que lidar com um volume de 3 a 4 vezes maior no que diz respeito a filtragem de conteúdo, detecção e bloqueio de intrusão, e controle de conectividade por endereços IP e portas de comunicação.
Cabe ressaltar também que, atualmente, o papel de prevenção e bloqueio de intrusões (IPS/IDS) é feito por equipamentos específicos, que também estão obsoletos, e cujo contrato, que vence no final do ano corrente, não se pretende renovar. Os equipamentos objeto do processo de contratação em tela assumirão as funções de detecção e prevenção e intrusão em substituição aos atuais.
Outro aspecto relativo ao dimensionamento dos equipamentos que se pretende adquirir é que eles dispõem de diversos outros recursos de segurança que os atuais, por sua característica de obsolescência, não dispõem, como ZTNA (Zero Trust Network Access), VPN (Virtual Private Network) por SSL (Secure Socket Layer - mais moderna, leve segura e estável que a provida pelos firewalls atuais, que usa IPSec), inspeção de tráfego criptografado (para tentar identificar ameaças em conteúdo criptografado que passe pelos firewalls, em tempo real) e prevenção contra malwares.
Especialmente no que diz respeito à VPN, temos uma séria limitação para oferecer esse tipo de serviço devido à capacidade dos equipamentos atuais, que limitam o número de conexões simultâneas a 200 (duzentas). Com a institucionalização do trabalho remoto por meio dos Programas de Gestão, nos vemos incapazes de atender a toda a demanda por acesso aos recursos hospedados na nossa infraestrutura local, que não podem ser publicados na Internet, por VPN. Pretende-se, com a aquisição dos novos equipamentos, prover o serviço com maior segurança e escalabilidade, e ampliar em ao menos 5 (cinco) vezes a quantidade de conexões simultâneas ao serviço de VPN.

Contudo, há que se pensar que o MAPA possui uma perspectiva de crescimento em seu ambiente computacional, devendo incluir esse ponto nesta contratação. A estimativa da demanda relacionada aos bens e serviços de TIC inclusos nesta contratação consta especificada na tabela abaixo:

ESTIMATIVA DA DEMANDA DA CONTRATAÇÃO

LOTE	ITEM	DESCRIÇÃO	QUANTIDADE
ÚNICO	1	Appliance físicos - Firewall - Solução de plataforma de segurança denominada Next Generation Firewall(NGFW), com licenciamento incluso.	01
	2	Suporte,garantia e manutenção do item 01.	01
	3	Appliance físicos - Firewall - Solução de plataforma de segurança denominada Next Generation Firewall(NGFW), com licenciamento incluso.	03
	4	Suporte, garantia e manutenção do item 03.	01
	5	Serviço de instalação e configuração dos firewalls NGFW dos itens 01 e 03.	01
	6	Appliance - Plataforma de gestão e monitoramento centralizado, com licenciamento, instalação e configuração.	01
	7	Suporte, garantia e manutenção do item 06.	01
	8	Treinamento ministrado por profissional certificado pelo fabricante.	01
	9	Plataforma de ZTNA - Zero Trust Network Access.	01

9. Levantamento de soluções

Este estudo técnico preliminar identificou como solução para a aquisição de equipamentos Firewall do tipo "Next Generation Firewall(NGFW)" contemplando serviço de instalação, licenciamento, suporte, garantia e treinamento para o ambiente do MAPA, possíveis soluções para a terceirização desse tipo de serviço, conforme pode ser observado no quadro abaixo:

LEVANTAMENTO DE SOLUÇÕES (CENÁRIOS)

ID	DESCRIÇÃO DA SOLUÇÃO (CENÁRIO)
01	Utilização de software livre.
02	Solução de Firewall UTM.
03	Composição de soluções de segurança.
04	Solução de Firewall "*Next Generation Firewall*" (NGFW).

A seguir, iremos demonstrar em detalhes cada cenário, levantando suas vantagens e desvantagens, entre outros aspectos:

9.1 - SOLUÇÃO 01 (UTILIZAÇÃO DE SOFTWARE LIVRE)

Não há disponibilidade de solução de software livre capaz de atender aos requisitos técnicos dessa contratação. Os *firewalls* baseados em código aberto ou livre possuem limitações em funcionalidades essenciais, por exemplo, controle e identificação de aplicações. Ademais, o volume de tráfego vem crescendo a cada ano, desta forma, exigindo hardwares dedicados para essa função. Segue abaixo outras limitações da utilização dessa solução:

- **Suporte limitado:** Embora muitos firewalls de software livre possam ser usados com sucesso em ambientes corporativos, o suporte pode ser limitado, especialmente no Administração Pública. Isso pode resultar em problemas de desempenho ou segurança que podem ser difíceis de resolver sem o suporte adequado.

- **Falta de recursos avançados:** Muitas soluções de firewall de software livre oferecem apenas recursos básicos de segurança e gerenciamento de rede. Isso pode ser suficiente para pequenas empresas ou redes domésticas, mas pode não ser adequado para ambientes maiores ou redes complexas que exigem recursos avançados de segurança, por exemplo, O Ministério da Agricultura e Pecuária.

- P**ossíveis vulnerabilidades de segurança:** Como qualquer software, os firewalls de software livre podem ter vulnerabilidades de segurança que podem ser exploradas por hackers e outros invasores. Embora as comunidades de software livre geralmente sejam rápidas em corrigir vulnerabilidades conhecidas, pode haver um risco maior de exposição a ataques se as atualizações de segurança não forem aplicadas imediatamente.

Um exemplo de solução seria a utilização do software livre (PFSENSE). O PFSense é uma distribuição customizada, livre e open source (de código aberto) do projeto FreeBSD. O fato de se ter uma solução *open source* realizando a proteção de perímetro pode trazer grande preocupação, tendo em vista que não há suporte 24x7 para tal solução, não há um centro de descoberta de ameaças cibernéticas sendo utilizado, e principalmente, não há diversas funcionalidades de segurança de última geração, já amplamente em uso nos dias de hoje. Ainda podemos citas outras desvantagens de uma solução baseada em software livre caso fosse adotada como solução no MAPA, são elas:

1. **Dependência de hardware:** Embora o pfSense possa ser instalado em um hardware existente, o desempenho do firewall pode depender da qualidade do hardware usado. Isso pode ser um problema para organizações que desejam implementar firewalls em larga escala por exemplo, o Ministério da Agricultura e Pecuária e seus Ministérios demandantes.
2. **Gerenciamento de patches:** O pfSense pode exigir atualizações regulares de segurança para manter-se protegido contra ameaças atuais, o que pode ser um desafio para algumas organizações que têm dificuldade em gerenciar patches e atualizações em seus sistemas.
3. **Integração com outros sistemas:** O pfSense pode não ser tão compatível com outros sistemas e aplicativos de segurança, o que pode ser um problema para organizações que desejam integrá-lo com outros produtos e serviços de segurança.

9.2 - SOLUÇÃO 02 (CONTRATAÇÃO DE FIREWALL UTM)

O Firewall UTM é uma solução de segurança de rede que oferece várias funcionalidades de segurança, como firewall de rede. Esse tipo de firewall é adequado para pequenas e médias empresas que precisam de proteção básica contra ameaças

cibernéticas. A solução atual está ultrapassada e não comporta o crescimento dos próximos anos. Há que se dizer ainda que tal contrato não possui a possibilidade de utilização de acesso remoto seguro no modelo ZTNA, e que tal fato, caracteriza grande problema de segurança ao ambiente do MAPA.

O firewall UTM não é a melhor opção para esta aquisição, uma vez que o mesmo possui conhecidos problemas de performance quando todas as inspeções são habilitadas, podendo prejudicar o bom funcionamento dos sistemas, gerando lentidão nos acessos e inclusive ocasionar em parada total.

9.3 - SOLUÇÃO 03 (COMPOSIÇÃO DE SOLUÇÕES DE SEGURANÇA)

A proposta dessa solução é composta de equipamentos e softwares de diversos fabricantes, cada um atuando em uma funcionalidade específica. Por se tratar de diferentes tipos de soluções, muitas vezes são necessários diversos treinamentos para operação dos equipamentos e softwares, que apesar de similares trabalham com sintaxes distintas, sendo necessário treinamento para cada fabricante. Num eventual incidente, a correlação das informações contidas nos equipamentos de diferentes fabricantes poderia levar horas ou dias, comprometendo a disponibilidade e segurança das informações.
Manter e gerenciar uma solução totalmente redundante com diversos equipamentos e de diferentes fabricantes acarreta custo operacional elevado, bem como alto custo de renovação de contrato, visto que para cada solução será necessária uma licença. Esse tipo de solução dificulta ainda o estabelecimento de processos de gerência de redes, inviabilizando a especialização da equipe para operação dos equipamentos e suas funcionalidades, visto que serão necessários diversos treinamentos para as funcionalidades distintas que nem sempre irão garantir sua interoperabilidade.

9.4 - SOLUÇÃO 04 (SOLUÇÃO DE FIREWALL "NEXT GENERATION FIREWALL")

O tema de proteção de perímetro com solução de Next Generation Firewall é amplamente conhecido no mercado de Cybersegurança. O que pode diferenciar um fabricante de outro é a capacidade de responder rapidamente a uma ameaça. Para que se tenha esta resposta rápida, se faz necessário o emprego de diversos profissionais e tecnologias.

A titulo de exemplo, imagine que uma vulnerabilidade foi descoberta, fabricantes de NGFW diferente levarão tempos diferentes para defesa de tal vulnerabilidade. Dessa forma quanto mais rápido o fabricante puder defender o seu cliente maior será sua eficiência.

É uma plataforma de rede integrada, baseada em inspeção profunda (deep packet inspection), provendo múltiplos mecanismos de proteção em um único equipamento, tais como Intrusion Prevention System (IPS), Antivírus, Inspeção a nível de aplicação e usuários, Inspeção de SSL/SSH, Filtro de Websites e Gerenciamento de banda (QoS). O firewall de próxima geração nasceu em 2009 e é a evolução do firewall UTM, que além de prover a centralização das inspeções e correlação de logs ainda entrega performance para redes de grande porte.

O Firewall de Próxima Geração permite: Instalação on-line sem perda de performance; Capacidades de firewall de primeira geração (Ex. NAT, Stateful Inspection Protocol, ZTNA, etc.); IPS; Visibilidade de Aplicativos de forma granular e Decriptografia SSL para permitir a identificação de aplicações criptografadas indesejadas. Além disso, diversas vantagens de segurança são encontradas nesse cenário de contratação, tais como: Detecção de ameaças avançadas do dia zero, Inspeção de tráfego criptografado, Filtragem de URL, Antimalware, Anti-Phishing, Anti-bot, Políticas de segurança mais granulares, Análise de comportamento de rede, gerencia única e simplificada, configuração facilitada entre outros.

Outro ponto a ser levado em consideração é que os fabricantes de firewall (NGFW) não participam diretamente das licitações, quem disputa são os revendedores parceiros e distribuidores das respectivas soluções.

10. Análise comparativa de soluções

Dentre as soluções identificadas, a tabela a seguir foi preenchida com o objetivo de identificar quais soluções se encaixam nos requisitos exigidos pelo órgão central do SISP:

REQUISITO	SOLUÇÃO	SIM	NÃO	NÃO SE APLICA
A Solução encontra-se implantada em outro órgão ou entidade da Administração Pública?	Solução 01	X		
	Solução 02	X		
	Solução 03		X	
	Solução 04	X		
	Solução 01		X	

A Solução está disponível no Portal do Software Público Brasileiro? (quando se tratar de software)	Solução 02			X
	Solução 03			X
	Solução 04			X
A Solução é composta por software livre ou software público? (quando se tratar de software)	Solução 01	X		
	Solução 02		X	
	Solução 03		X	
	Solução 04		X	
A Solução é aderente às políticas, premissas e especificações técnicas definidas pelos Padrões de governo ePing, eMag, ePWG?	Solução 01			X
	Solução 02			X
	Solução 03			X
	Solução 04			X
A Solução é aderente às regulamentações da ICP-Brasil? (quando houver necessidade de certificação digital)	Solução 01			X
	Solução 02			X
	Solução 03			X
	Solução 04			X
A Solução é aderente às orientações, premissas e especificações técnicas e funcionais do e-ARQ Brasil? (quando o objetivo da solução abranger documentos arquivísticos)	Solução 01			X
	Solução 02			X
	Solução 03			X
	Solução 04			X

A equipe de planejamento da contratação entende que os requisitos mínimos definidos pelo órgão central do SISP não é suficiente para fazer uma comparação das soluções, desta forma, definimos abaixo outras características para comparação:

REQUISITO	**SOLUÇÃO**	**SIM**	**NÃO**	**NÃO SE APLICA**
Gerenciamento simplificado centralizado com funções básicas de relatórios e histórico.	Solução 01		X	
	Solução 02	X		
	Solução 03		X	
	Solução 04	X		
Interface WEB de gerência e configuração de toda solução.	Solução 01		X	
	Solução 02	X		
	Solução 03		X	
	Solução 04	X		
Compatibilidade com software de gerência e análise de logs.	Solução 01		X	
	Solução 02	X		
	Solução 03		X	
	Solução 04	X		
Suporte oficial do fabricante.	Solução 01		X	
	Solução 02	X		
	Solução 03		X	
	Solução 04	X		
Garantia de funcionamento.	Solução 01		X	
	Solução 02	X		
	Solução 03		X	
	Solução 04	X		
A solução é ou está defasada tecnologicamente ou não é adequada para a Administração Pública Federal.	Solução 01	X		
	Solução 02	X		
	Solução 03	X		

	Solução 04		X	
Treinamento e implantação oficial da solução.	Solução 01		X	
	Solução 02	X		
	Solução 03		X	
	Solução 04	X		
Laboratório de segurança para descobertas de ameaças / Inspeção de trafego criptografado / Filtragem de URL avançada.	Solução 01		X	
	Solução 02		X	
	Solução 03		X	
	Solução 04	X		
Detecção de ameaças avançadas zero-day ; Análise de comportamento de rede.	Solução 01		X	
	Solução 02		X	
	Solução 03		X	
	Solução 04	X		

11. Registro de soluções consideradas inviáveis

11.1 - JUSTIFICATIVA DAS SOLUÇÕES INVIÁVEIS

Diante do exposto abaixo, considerando as diferenças de tecnologia, primando pela segurança cibernética do MAPA, entendemos que as soluções 01,02 e 03 são consideradas inviáveis.

ID	DESCRIÇÃO DA SOLUÇÃO(CENÁRIO)	JUSTIFICATIVA DA INVIABILIDADE DA SOLUÇÃO
01	Utilização de software livre.	Não existe um único produto baseado em software livre que seja capaz de oferecer todas as funcionalidades oferecidas por outras soluções proprietárias reunidas em um único produto. Para implementação da solução por meio de software livre, **seria necessário utilizar várias soluções diferentes e não integradas**, tais como Firewall Iptables, Web Filter Squid, OpenVPN e IPS Snort, entre outras, aumentando exponencialmente **o esforço de implementação e sustentação**, falta de garantia em caso de falhas no software e **ausência de suporte**. Além disso, deve ser considerada a curva de aprendizagem, com capacitação e especialização do corpo técnico existente nas diversas soluções *open sources* citadas e o **possível custo de contratação de mão de obra especializada**, tempo para implementação e custos indiretos. Além disso, podemos citar outras **desvantagens** dessa solução: • Configuração e gerenciamento: O firewall de software livre pode exigir mais **conhecimento técnico para configurá-lo e gerenciá-lo em comparação com os firewalls proprietários**. Isso pode ser um desafio para os profissionais de TI que não estão acostumados a trabalhar com software livre. • Suporte: Embora existam comunidades de usuários e desenvolvedores de software livre que podem oferecer suporte, pode ser **difícil encontrar uma empresa especializada em software livre** para fornecer suporte técnico, **especialmente em caso de falhas críticas**. • Hardware e compatibilidade: A escolha de hardware pode ser mais limitada em relação aos firewalls proprietários, e pode haver **problemas de compatibilidade** com outros softwares e dispositivos de rede • Personalização: Enquanto o software livre oferece mais flexibilidade para personalização, pode haver um custo mais alto para adaptar esta solução às necessidades específicas do MAPA em comparação às soluções proprietárias. • Interoperabilidade: Pode haver **dificuldades em garantir a interoperabilidade** entre um firewall de software livre e outros sistemas de rede e segurança. • Segurança: Pode haver p**reocupações sobre a segurança de dados confidenciais** e sistemas críticos quando se trata desse tipo de firewall.

		• Conformidade: pode ser necessário garantir que o firewall de software livre atenda a regulamentos e normas de segurança específicas, o que pode ser um desafio para a equipe de TI.
	Solução de Firewall UTM.	Para atender as necessidades da MAPA, o UTM deveria ser composto com uma solução de Ameaça Persistente Avançada, o que implica na necessidade de pelo menos dois diferentes fabricantes. Com dois fabricantes distintos perde-se o gerenciamento centralizado e a correlação dos eventos da solução. Com o intuito de adquirir uma solução que comporte a rede atual, mas também o crescimento dos próximos anos, o firewall UTM não será a melhor opção para esta aquisição, uma vez que o mesmo possui conhecidos **problemas de performance quando todas as inspeções são habilitadas** e ocorre o **compartilhamento do hardware entre vários serviços**, podendo prejudicar o bom funcionamento dos sistemas, **gerando lentidão nos acessos e inclusive ocasionar em parada total.**
03	Composição de soluções de segurança.	A proposta dessa solução é composta de equipamentos de diversos fabricantes, cada um atuando em uma área de inspeção. Nesse tipo de solução, **não existe nenhuma integração de gerenciamento entre esses servidores e seus respectivos serviços**. Dessa forma, em determinadas situações, por exemplo, obter informações sobre um incidente de acesso indevido, é necessário realizar diversas consultas, em diversos sistemas de armazenamento de logs. Assim, a correlação das informações contidas nos equipamentos de diferentes fabricantes poderia levar horas ou dias, **comprometendo a disponibilidade e segurança das informações.** A necessidade da aquisição de diferentes licenças e de diferentes fabricantes poderia fazer com os preços fossem maiores quando comparados a aquisição de uma solução que atenda a todas as necessidades. Além disso, seria necessário que **diferentes treinamentos fossem realizados**, visto que essas soluções, apesar de similares, trabalham com sintaxes distintas em seus hardwares e softwares, sendo necessários diferentes treinamentos para cada solução implantada. Isso iria demandar mais tempo dos analistas de TI da UFSM para realizar os treinamentos e possivelmente, se tornaria mais caro que realizar o treinamento de uma única solução. Outro aspecto que deve ser considerado é a **dificuldade de se estabelecer processos de gerenciamento**, pois quando se tem diversos tipos de soluções, fica mais difícil implementar um gerenciamento centralizado, pois muitos equipamentos não permitem integração, conforme já citado anteriormente.

12. Análise comparativa de custos (TCO)

12.1 - ANÁLISE COMPARATIVA DE CUSTOS (SOLUÇÃO 04)

Uma vez detalhado o escopo, cenário ideal e requisitos técnicos mínimos para a solução de TIC em questão, foi realizada uma rápida pesquisa de contratações similares para os itens desta contratação. Bem, a IN SGD/ME nº 94, de 23 de Dezembro de 2022 indica, em seu artigo 20, que as pesquisas de preços devem seguir o método prescrito na antiga Instrução Normativa SEGES/ME no 65, de 7 de julho de 2021, da Secretaria de Gestão da Secretaria Especial de Desburocratização, Gestão e Governo Digital do Ministério da Economia, que inclui:

> 1. Composição de custos unitários menores ou iguais à mediana do item correspondente nos sistemas oficiais de governo, como Painel de Preços ou banco de preços, observado o índice de atualização de preços correspondente;
> 2. Contratações similares feitas pela Administração Pública, em execução ou concluídas no período de 1 (um) ano anterior à data da pesquisa de preços, inclusive mediante sistema de registro de preços, observado o índice de atualização de preços correspondente;
> 3. Dados de pesquisa publicada em mídia especializada, de tabela de referência formalmente aprovada pelo Poder Executivo federal e de sítios eletrônicos especializados ou de domínio amplo, desde que atualizados no momento da pesquisa e compreendidos no intervalo de até 6 (seis) meses de antecedência da data de divulgação do edital, contendo a data e a hora de acesso;
> 4. Pesquisa direta com, no mínimo, 3 (três) fornecedores, mediante solicitação formal de cotação, por meio de ofício ou e-mail, desde que seja apresentada justificativa da escolha desses fornecedores e que não tenham sido obtidos os orçamentos com mais de 6 (seis) meses de antecedência da data de divulgação do edital; ou

5. Pesquisa na base nacional de notas fiscais eletrônicas, desde que a data das notas fiscais esteja compreendida no período de até 1 (um) ano anterior à data de divulgação do edital, conforme disposto no Caderno de Logística, elaborado pela Secretaria de Gestão da Secretaria Especial de Desburocratização, Gestão e Governo Digital do Ministério da Economia.

Vale destacar que esta IN dispõe que devem ser priorizados os dois primeiros mecanismos, conforme definido no seu artigo 5º, §1. Lembremos, porém, **que neste momento estamos, em princípio, realizando estudo preliminares,** de forma que podemos utilizar quaisquer desses parâmetros, ou uma combinação deles, zelando sempre para que as estimativas estejam próximas à realidade do mercado. Independentemente, um**a pesquisa de preços completa será formalizada, de acordo com a** Instrução Normativa SEGES/ME no 65, de 7 de julho de 2021, **nos autos do processo quando da estimativa do preço final da contratação.**

Abaixo, segue a tabela com a **estimativa de preços preliminar** através de contratos similares:

- Ministério das Comunicações-MCOM (Documento SEI Nº 27909400)
- INEP - Instituto Nacional de Estudos e Pesquisas Educacionais Anísio Teixeira (Documento SEI Nº27909355)
- PREVIC - Superintendência Nacional de Previdência Complementar (Documento SEI Nº27909466)
- IFB-DF - Instituto Federal de Educação, Ciência e Tecnologia de Brasília (Documento SEI Nº 27909585)
- EBSERH - Hospital Universitário de Santa Maria da Universidade Federal de Santa Maria (Documento SEI Nº 28068591)

Diante de tais contratações, a característica principal (throughput) dos equipamentos ofertados foram analisadas conforme abaixo:

Contratação	**Fabricante**	**Throughput**	**Valor**	**Vigência**
Contratação MCOM	Fortinet	3Gbps	R$ 560.000,00	Vigência do contrato de 12 meses e garantia de 60 meses.
Contratação INEP	N/A	10Gbps	R$ 2.214.800,00	Vigência do contrato de 36 e garantia de 36 meses.
Contratação PREVIC	N/A	4,4Gbps	R$ 550.000,00	Vigência do contrato de 12 meses e garantia de 48 meses.
Contratação IFB-DF	Checkpoint	5Gbps	R$ 729.300,02	Vigência do contrato de Garantia de 60 meses.
Contratação EBSERH	Palo Alto	1Gbps	R$ 386.000,00	Garantia de 36 meses.

Logo após, obteve-se o valor estimado por 1 Gb, com licenciamento para o período de 12 meses.

Contratação	**Valor Gb**	**Valor Gb / mês**	**Valor Gb/ano**	**Média de Gb /ano**
Contratação MCOM	R$ 186.666,66	R$ 3.111,11	R$ 37.333,32	
Contratação INEP	R$ 221.480,00	R$ 6.152,22	R$ 73.826,66	

Contratação PREVIC	R$ 125.000,00	R$ 2.604,16	R$ 31.249,92	R$ 60.049,71
Contratação IFB-DF	R$ 145.860,00	R$ 2.431,00	R$ 29.172,00	
Contratação EBSERH	R$ 386.000,00	R$ 10.722,22	R$ 128.666,67	

Em seguida, estimamos com base na quantidade de throughput desejada (23Gbps e 11Gbps) para os itens 01 e 03, aos quais foram calculados abaixo.

Estimativa para o item 01 e 03

Valor Média Gb ano	**Throughput estimado**	**Estimativa Média do item 01 (Unitário)**	**Throughput estimado**	**Estimativa do item 02 (Unitário)**
R$ 60.049,71	23Gbps	R$ 1.381.143,42	11Gbps	R$ 660.546,85
Estimativa média para o item 01 **R$ 1.381.143,42**			Estimativa média para o item 03 **R$ 660.544,83**	

Consolidando todos os valores chegamos aos valores médios por item, conforme explicitado abaixo:

LOTE	**ITEM**	**DESCRIÇÃO**	**QUANTIDADE**	**VALOR UNITÁRIO**	**VALOR TOTAL**
ÚNICO	1	Appliance físicos - Firewall - Solução de plataforma de segurança denominada Next Generation Firewall(NGFW), com licenciamento incluso.	01	R$ 1.381.143,42	R$ 1.381.143,42
	2	Suporte, garantia e manutenção do item 01.	01	R$ 1.472.136,55	R$ 1.472.136,55
	3	Appliance físicos - Firewall - Solução de plataforma de segurança denominada Next Generation Firewall(NGFW), com licenciamento incluso.	03	R$ 660.544,83	R$1.981.634,49
	4	Suporte, garantia e manutenção do item 03.	01	R$ 2.070.923,69	R$ 2.070.923,69
	5	Serviço de instalação e configuração dos firewalls NGFW dos itens 01 e 03.	01	R$ 223.237,26	R$ 63.562,50
	6	Appliance - Plataforma de gestão e monitoramento centralizado, com licenciamento, instalação e configuração.	01	R$ 118.072,29	R$ 118.072,29
	7	Suporte, garantia e manutenção do item 06.	01	R$ 50.040,16	R$ 50.040,16
	8	Treinamento ministrado por profissional certificado pelo fabricante.	01	R$ 62.896,12	R$ 62.896,12
	9	Plataforma de ZTNA - Zero Trust Network Access.	01	R$ 208.674,70	R$ 208.674,70
Desta forma, a estimativa preliminar para a contratação é de R$ 7.409.083,92					

Observações: É importante ressaltar que no mercado existem diversos modelos e soluções de firewall próximas/diferentes, resultando em uma quantidade de combinações e características relativamente amplas (capacidade de throughput de diversos tipos, quantidade de sessões novas e simultâneas, quantidade de interface, usuários simultâneos, quantidade de políticas de firewall, entre vários outros fatores.), desta forma, não foi possível observar nenhuma que pudesse trazer o mesmo escopo da contratação ora pretendia. Diante disso, após a elaboração do termo de referência será feita uma pesquisa de preços completa conforme a legislação em vigor, conforme dito anteriormente acima, com o objetivo de refletir a realidade do mercado e preços atualizados de acordo especificamente com o detalhado no termo de referência.

12.2 - MAPA COMPARATIVO DOS CÁLCULOS TOTAIS DE PROPRIEDADE(TCO)

Conforme o § 1º do inciso V do artigo 11 da Instrução Normativa SGD/ME Nº94, de 23 de Dezembro de 2022, a equipe de planejamento da contratação está dispensando a realização dos respectivos cálculos de custo total de propriedade das soluções consideradas inviáveis. Portanto, conforme apresentado no presente estudo, apenas a solução 04 foi classificada como viável.

ESTIMATIVA de TCO ao longo da contratação - Considerando um reajuste estimado de 6% ao ano.

ANO 1	ANO 2	ANO 3	ANO 4	ANO 5	TOTAL
R$ 7.409.083,92	R$ 4.029.881,61	R$ 4.271.674,50	R$ 4.527.974,97	R$ 4.799.653,47	**R$ 25.038.268,47**

A depender a pesquisa de preços completa ao longo do processo de contratação, esse valor pode ser alterado.

13. Descrição da solução de TIC a ser contratada

A solução de TIC a ser contratada será através do item 04 Solução de Firewall "*Next Generation Firewall*" (NGFW).

13.1 - PARCELAMENTO DA SOLUÇÃO

O objeto do certame não será parcelado, uma vez que os bens e serviços que compõem o objeto formam um conjunto indissociável, composto pela interligação dos serviços que funcionam harmonicamente. As melhores práticas de gestão em TI se baseiam na integração dos serviços, que são indissociáveis e apresentam inter-relação entre si, de forma que assegurem o alinhamento e a coerência em termos de qualidade técnica, resultando assim, no perfeito atendimento dos princípios da celeridade, economicidade e eficiência.
Somente a execução de forma integrada dos serviços garante a disponibilidade, segurança e a preservação dos dados de execução, evitando transferência de responsabilidades, nos casos de eventuais problemas causados por serviços prestados por mais de uma empresa CONTRATADA.

O fornecimento de itens por meio de CONTRATADAS distintas traria enormes riscos ao projeto. Um grande risco viria da necessidade contínua de comunicação entre os diferentes fornecedores, o que, historicamente, não ocorre com fluidez nem de forma satisfatória, sendo a parte mais lesada o MAPA. Além disso, há necessidade de ocorrer perfeita integração técnica entre os itens do objeto. Dessa forma, o fornecimento parcial dos itens por diferentes fornecedores traria não apenas maior complexidade, como maiores custos de integração e riscos de não execução adequada.

A licitação por item poderia causar prejuízo para o conjunto da licitação (questões técnicas) ou para a economia de escala (questões econômicas), e tornaria inviável e prejudicial o bom desempenho da solução, por se tratar de serviços complementares.

Ademais, por se tratar de uma solução de serviços integrados, é fundamental para a garantia da qualidade do serviço, que sejam executados por um mesmo fornecedor, dada a impossibilidade de segregação do objeto sem que haja prejuízo ao conjunto, objetivando alcançar produtividade, economicidade e eficiência na realização dos serviços.

Desta forma, o agrupamento de elementos que compõem a mesma solução compõe a melhor estratégia da Administração, quando a adjudicação de itens isolados onera o “o trabalho da administração pública, sob o ponto de vista do emprego de recursos humanos e da dificuldade de controle, colocando em risco a economia de escala e a celeridade processual”, vide o ACÓRDÃO Nº 5301/2013 – TCU – 2ª Câmara.

É importante também, se observar o posicionamento do Egrégio Tribunal de Contas da União, nos autos do Acórdão nº 1916 /2009 – Plenário, sob a matéria:

> *"15. Acerca da alegada possibilidade de fragmentação do objeto, vale notar que nos termos do art. 23, § 1º, da Lei n. 8.666/1993, exige-se o parcelamento do objeto licitado sempre que isso se mostre técnica e economicamente viável. A respeito da matéria, esta Corte de Contas já editou a Súmula n. 247/2004, in verbis: "É obrigatória a admissão da adjudicação por item e não por preço global, nos editais das licitações para a contratação de obras, serviços, compras e alienações, cujo objeto seja divisível, desde que não haja prejuízo para o conjunto ou complexo ou perda de economia de escala, tendo em vista o objetivo de propiciar a ampla participação de licitantes..." (grifou-se).*

Depreende-se, portanto, que a divisão do objeto deverá ser implementada sempre que houver viabilidade técnica e econômica para a sua adoção.
Nesse ponto, calha trazer à baila o escólio de Marçal Justen Filho: "O fracionamento em lotes deve respeitar a integridade qualitativa do objeto a ser executado. Não é possível desnaturar um certo objeto, fragmentando-o em contratações diversas e que importam o risco de impossibilidade de execução satisfatória." (Comentários à Lei de Licitações e Contratos Administrativos. 10. ed. São Paulo: Dialética, 2004. p. 209)."
Adicionalmente, em virtude da especificidade do objeto, pode-se afirmar ser tecnicamente inadequado o seu desmembramento, sob pena de não se atender o objetivo buscado, no sentido de fortalecer a disponibilidade, segurança, a preservação dos dados e ativos de TI do MAPA na manutenção da operabilidade do ambiente de TI.
Ainda, sob o ponto de vista econômico, não há elementos nos autos que permitam concluir que a adoção do parcelamento do objeto, seria, no caso concreto, mais vantajosa para o MAPA.

Por fim, o objeto não será parcelado, pois constitui-se em uma única solução de TIC e os serviços que compõem o objeto licitado são serviços de mesma natureza, dependentes entre si, e sua divisão impactaria na execução do projeto e tornaria a contratação menos econômica, eficaz e eficiente para a Administração. Assim, considerando-se a inviabilidade técnica e econômica para o parcelamento do objeto da presente contratação, bem como consideradas as suas respectivas peculiaridades, interdependência e natureza acessória entre os serviços que compõem o objeto, a contratação pretendida deverá ser realizada em um único grupo.

14. Estimativa de custo total da contratação

Valor (R$): 7.409.083,92

A metodologia usada para estimativa de valores da contratação foi o valor médio das contratações similares encontradas nos últimos 02 anos. A estimativa de custo total para esta aquisição , de acordo com as necessidade do Ministério da Agricultura e Pecuária-MAPA, é de **R$ 7.409.083,92,** pelo período de 12 meses.

LOTE	ITEM	DESCRIÇÃO	QUANTIDADE	VALOR UNITÁRIO	VALOR TOTAL
ÚNICO	1	Appliance físicos - Firewall - Solução de plataforma de segurança denominada Next Generation Firewall(NGFW), com licenciamento incluso.	01	R$ 1.381.143,42	R$ 1.381.143,42
	2	Suporte,garantia e manutenção do item 01.	01	R$ 1.472.136,55	R$ 1.472.136,55
	3	Appliance físicos - Firewall - Solução de plataforma de segurança denominada Next Generation Firewall(NGFW), com licenciamento incluso.	03	R$ 660.544,83	R$ 1.981.634,49
	4	Suporte,garantia e manutenção do item 03.	01	R$ 2.070.923,69	R$ 2.070.923,69
	5	Serviço de instalação e configuração dos firewalls NGFW dos itens 01 e 03.	01	R$ 223.237,26	R$ 63.562,50
	6	Appliance - Plataforma de gestão e monitoramento centralizado, com licenciamento, instalação e configuração.	01	R$ 118.072,29	R$ 118.072,29

	7	Suporte, garantia e manutenção do item 06.	01	R$ 50.040,16	R$ 50.040,16
	8	Treinamento ministrado por profissional certificado pelo fabricante.	01	R$ 62.896,12	R$ 62.896,12
	9	Plataforma de ZTNA - Zero Trust Network Access.	01	R$ 208.674,70	R$ 208.674,70
Desta forma, a estimativa preliminar para a contratação é de R$ 7.409.083,92					

15. Justificativa técnica da escolha da solução

Considera-se tecnicamente viável a Solução 04 pela necessidade de um equipamento para atender as demandas de segurança e gestão da rede do MAPA e seus Ministérios demandantes, tendo em vista a não renovação do contrato atual de firewall. Além de oferecer um nível maior de segurança à rede, um firewall de próxima geração, com uma maior capacidade de processamento, possibilita a implementação de novos serviços, por exemplo, análise do tráfego, ZTNA, entre outros. Com isso, será possível ter uma visualização detalhada da utilização da rede e das aplicações utilizadas. Adicionalmente, o processo de identificação de ameaças é facilitado e permite a aplicação de políticas de segurança mais eficientes.

Do ponto de vista da solução de Acesso Remoto Seguro, há que se dizer que o MAPA possui atualmente cerca de 200 licenças de VPN, aos quais funcionam em modelo flutuante, ou seja, podem ter apenas 200 conexões ao mesmo tempo. Tal modelo de acesso remoto deverá ser substituído por um modelo de acesso seguro, em modelo de confiança zero. Adicionalmente, a solução atual de firewall tem difícil integração com outras soluções de segurança do mercado.

Outra funcionalidade importante que pode ser implementada é a identificação de usuários que utilizam a rede e o registro de conexões, permitindo um melhor inventário dos ativos de TI do MAPA e seus Ministérios demandantes. Com o aumento no número de usuários trabalhando de casa, a quantidade de conexões externas para trabalho fora das instalações dos Ministério (trabalho remoto) aumentou consideravelmente durante o período de pandemia, aumentando a necessidade de conexões VPN suportadas pelo equipamento antigo. O aumento na quantidade de ataques às empresas, precipuamente na tentativa de sequestro de dados em troca de resgate, fez com que a necessidade de um firewall que pudesse mitigar melhor ataques de negação de serviço, bloquear infecções maliciosas, ter uma maior e mais rápida análise do tráfego de dados na rede institucional, principalmente em casos de ataques de ransomware, ficasse evidente para o setor de tecnologia da informação do MAPA.

15.1 . DO PARCELAMENTO DA CONTRATAÇÃO DECORRENTE DE ASPECTOS TÉCNICOS

Não se aplica.

16. Justificativa econômica da escolha da solução

Deve-se atentar não somente os custos de cada solução possível, mas também aos diversos benefícios que elas proporcionam, pois o objetivo não é apenas gastar menos recursos públicos, mas qualificar o gasto, isto é, atender satisfatoriamente às necessidades sem esquecer da razoabilidade. Outras justificativas econômicas estão pormenorizadas ao longo dos itens 09 ao 12.

Deste modo, tivemos apenas uma solução viável e não há como fazer comparação econômica em relação às demais soluções levantadas.

16.1 . DO PARCELAMENTO DA CONTRATAÇÃO DECORRENTE DE ASPECTOS ECONÔMICOS

Não se aplica.

17. Contratações Correlatas

Atualmente o MAPA possui o contrato Nº 19/2021 com a empresa OGASEC CONSULTORIA E INFORMÁTICA S.A cujo objeto é prestação de serviço de atualização da solução de segurança integrada AKER de firewall e analisador de conteúdo web existente no Ministério da Agricultura e Pecuária. Além desse, é importante citar o contrato 33/2022, em que temos perfis profissionais de segurança da informação que podem executar os serviços de Gerenciamento de acessos, Administração de IPS, ZTNA, Administração/Configuração de Firewall, Configuração de regras de firewall, configuração de filtro de URL, entre outros.

Portanto, este respectivo estudo visa a substituição e aprimoramento da contratação com diversos novos recursos.

18. Benefícios a serem alcançados com a contratação

Os **resultados pretendidos** com essa contratação são:

1. Aumento da capacidade de resposta aos incidentes cibernéticos.
2. Melhorar o acesso remoto de maneira estável aos colaboradores de forma segura.
3. Aprimorar a segurança de TIC do Ministério da Agricultura ,e demais órgãos atrelados, frente às recentes ameaças.
4. Contribuir para a garantia de um nível adequado de Confidencialidade, Integridade e Disponibilidade.
5. Maior visibilidade do trafego das informações e da rede, possibilitando a detecção e proteção em tempo real contra as ameaças. Com isso, será possível corrigir comportamentos inadequados; direcionar recursos para demandas mais relevantes; controlar serviços e aplicações suspeitas ou que interferem diretamente na produtividade.
6. Permitir a criação de políticas de proteção da rede contra eventuais ataques de usuários mal-intencionados, através do bloqueio de portas não utilizadas e controle mais refinado de uso de banda de internet, a fim de evitar abusos em sua utilização;
7. Maior rapidez na detecção - Priorização de alertas de segurança e avisos constantes sobre normas de cibersegurança dentro de uma organização, evitando que erros humanos sejam cometidos na hora de acessar links duvidosos e outras páginas maliciosas.
8. Aprimorar a detecção e bloqueio de ameaças avançadas, como malware, ataques de negação de serviço distribuídos (DDoS) e tentativas de invasão de rede.
9. Melhoria na geração de relatórios diversos para rápida análise de informações sobre tráfego, aplicações, ameaças, usuários, etc.
10. Melhoria na filtragem de conteúdo web, implementando uma filtragem mais abrangente, com criação de regras de uso de aplicações web, que permitam a limitação de acesso a certas categorias de serviços, por meio de análise de tráfego.

19. Providências a serem Adotadas

Não se aplica.

20. Declaração de Viabilidade

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

20.1. Justificativa da Viabilidade

O presente estudo técnico preliminar, elaborado pelos integrantes técnico e requisitante em harmonia com o disposto no artigo 11 da Instrução Normativa Nº 94/2022 SGD, considerando a análise das alternativas de atendimento das necessidades elencadas pela área requisitante e os demais aspectos normativos, conclui pela viabilidade da contratação, uma vez considerados os benefícios em termos de eficácia, eficiência, efetividade e economicidade, detalhados ao longo deste documento. Em complemento, os requisitos listados atendem adequadamente às demandas formuladas, os custos são compatíveis e os riscos identificados são administráveis, pelo que recomendamos o prosseguimento da pretensa contratação.

21. Responsáveis

Todas as assinaturas eletrônicas seguem o horário oficial de Brasília e fundamentam-se no §3º do Art. 4º do Decreto nº 10.543, de 13 de novembro de 2020.

THIAGO PEREIRA DA COSTA

Membro da comissão de contratação

Assinou eletronicamente em 18/09/2023 às 15:12:05.

MARCO ANTONIO BITTENCOURT SUCUPIRA

Membro da comissão de contratação

Assinou eletronicamente em 19/09/2023 às 10:28:13.

CAMILO MUSSI

Membro da comissão de contratação

Assinou eletronicamente em 19/09/2023 às 15:22:17.

MINISTÉRIO DA AGRICULTURA E PECUÁRIA

MINUTA DE CONTRATO

* MINUTA DE DOCUMENTO

CONTRATO ADMINISTRATIVO Nº ...../...., QUE FAZEM ENTRE SI A UNIÃO, POR INTERMÉDIO DO MINISTÉRIO DA AGRICULTURA E PECUÁRIA, E A EMPRESA .....

Modelo Contrato - TIC - Serviços - Lei 14.133 (Atualização: maio/2023)
Modelo Contrato - TIC - Compras - Lei 14.133 (Atualização: maio/2023)

A União, por intermédio do **MINISTÉRIO DA AGRICULTURA E PECUÁRIA**, com sede na Esplanada dos Ministérios, Bloco D, na cidade de Brasília/DF, inscrito no CNPJ/MF sob o nº 00.396.895/0011-05, neste ato representado pelo(a) ..... (nome e cargo), nomeado(a) pela Portaria nº ....., de ..... de ..... de 20..., publicada no DOU de ..... de ..... de ....., portador(a) da Matrícula Funcional nº ....., doravante denominado **CONTRATANTE**, e o(a) ..... inscrito(a) no CNPJ/MF sob o nº ....., sediado(a) na ....., em ....., doravante designado **CONTRATADO**, neste ato representado(a) por ....., conforme atos constitutivos da empresa OU procuração apresentada nos autos, tendo em vista o que consta no Processo nº 21000.020025/2023-02 e em observância às disposições da Lei nº 14.133, de 1º de abril de 2021, e demais legislação aplicável, resolvem celebrar o presente Termo de Contrato, decorrente do Pregão Eletrônico n. ...../20...., mediante as cláusulas e condições a seguir enunciadas.

1. CLÁUSULA PRIMEIRA – OBJETO (ART. 92, I E II)

1.1. O objeto do presente instrumento é a contratação de solução de proteção de rede com características de Next Generation Firewall (NGFW), contemplando os hardwares com licenciamento, suporte e garantia, instalação e configuração, treinamento, plataforma de gestão, treinamento e Plataforma de ZTNA pelo período de 05 anos, para atender a demanda do Ministério da Agricultura e Pecuária e órgãos demandantes (Ministério da Pesca e Aquicultura / Ministério do Desenvolvimento Agrário e Agricultura Familiar), nas condições estabelecidas no Termo de Referência.

1.2. Objeto da contratação:

ITEM	ESPECIFICAÇÃO	CATSER/CATMAT	UNIDADE DE MEDIDA	QUANTIDADE	VALOR UNITÁRIO	VALOR TOTAL
1	Appliances físicos - Firewall - Solução de plataforma de segurança, denominada Next Generation Firewall (NGFW), com licenciamento incluso	481646	UNIDADE	01		
2	Suporte, garantia e manutenção do item 01	27740	SERVIÇO	01		
3	Appliances físicos - Firewall - Solução de plataforma de segurança, denominada Next Generation Firewall (NGFW).	481646	UNIDADE	03		
4	Suporte, garantia e manutenção do item 03.	27740	SERVIÇO	01		
5	Serviço de instalação e configuração dos firewalls NGFW dos itens 01 e 03	26972	SERVIÇO	01		
6	Appliance - Plataforma de gestão e monitoramento centralizado, com licenciamento, instalação e configuração.	481646/481647	UNIDADE	01		
7	Suporte, garantia e Manutenção do item 06.	27740	SERVIÇO	01		
8	Treinamento ministrado por profissional certificado pelo fabricante	16837/20052	CAPACITAÇÃO	01		
9	Plataforma de ZTNA - Zero Trust Network Access	27742	SERVIÇO	01		

1.3. Vinculam esta contratação, independentemente de transcrição:

1.3.1. O Termo de Referência;

1.3.2. O Edital da Licitação;

1.3.3. A Proposta do **CONTRATADO**;

1.3.4. Eventuais anexos dos documentos supracitados.

2. CLÁUSULA SEGUNDA – VIGÊNCIA E PRORROGAÇÃO

2.1. O prazo de vigência da contratação é de 2 (dois) anos contados a partir da data de assinatura, prorrogável para até 5 (cinco) anos, na forma dos artigos 106 e 107 da Lei nº 14.133, de 2021.

2.2. A prorrogação de que trata esse item é condicionada à avaliação, por parte do Gestor do Contrato, da vantajosidade da prorrogação, a qual deverá ser realizada motivadamente, com base no Histórico de Gestão do Contrato, nos princípios da manutenção da necessidade, economicidade e oportunidade da contratação, e nos demais aspectos que forem julgados relevantes.

2.3. O **CONTRATADO** não tem direito subjetivo à prorrogação contratual.

2.4. A prorrogação de contrato deverá ser promovida mediante celebração de termo aditivo.

2.5. O contrato não poderá ser prorrogado quando o **CONTRATADO** tiver sido penalizado nas sanções de declaração de inidoneidade ou impedimento de licitar e contratar com poder público, observadas as abrangências de aplicação.

3. CLÁUSULA TERCEIRA – MODELOS DE EXECUÇÃO E GESTÃO CONTRATUAIS (ART. 92, IV, VII E XVIII)

3.1. O regime de execução contratual, os modelos de gestão e de execução, assim como os prazos e condições de conclusão, entrega, observação e recebimento do objeto constam no Termo de Referência, anexo a este Contrato.

4. CLÁUSULA QUARTA – SUBCONTRATAÇÃO

4.1. Não será admitida a subcontratação do objeto contratual.

5. CLÁUSULA QUINTA – PREÇO

5.1. O valor total da contratação é de R$ ..... (.....).

5.2. 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.

5.3. O valor acima é meramente estimativo, de forma que os pagamentos devidos ao contratado dependerão dos quantitativos efetivamente fornecidos.

6. CLÁUSULA SEXTA – PAGAMENTO (ART. 92, V E VI)

6.1. O prazo para pagamento ao contratado e demais condições a ele referentes encontram-se definidos no Termo de Referência, anexo a este Contrato.

7. CLÁUSULA SÉTIMA – REAJUSTE (ART. 92, V)

7.1. Os preços inicialmente contratados são fixos e irreajustáveis no prazo de um ano contado da data do orçamento estimado, em 30/06/2023.

7.2. Após o interregno de um ano, e independentemente de pedido do contratado, os preços iniciais serão reajustados, mediante a aplicação, do índice de Custos de Tecnologia da Informação - ICTI, mantido pela Fundação Instituto de Pesquisa Econômica Aplicada - IPEA, exclusivamente para as obrigações iniciadas e concluídas após a ocorrência da anualidade.

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

7.4. No caso de atraso ou não divulgação do(s) índice (s) de reajustamento, o contratante pagará ao contratado a importância calculada pela última variação conhecida, liquidando a diferença correspondente tão logo seja(m) divulgado(s) o(s) índice(s) definitivo(s).

7.5. Nas aferições finais, o(s) índice(s) utilizado(s) para reajuste será(ão), obrigatoriamente, o(s) definitivo(s).

7.6. Caso o(s) índice(s) estabelecido(s) para reajustamento venha(m) a ser extinto(s) ou de qualquer forma não possa(m) mais ser utilizado(s), será(ão) adotado(s), em substituição, o(s) que vier(em) a ser determinado(s) pela legislação então em vigor.

7.7. 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.

7.8. O reajuste será realizado por apostilamento.

8. CLÁUSULA OITAVA – OBRIGAÇÕES DO CONTRATANTE (ART. 92, X, XI E XIV)

8.1. São obrigações do **CONTRATANTE**, além das previstas no Termo de Referência:

8.1.1. Exigir o cumprimento de todas as obrigações assumidas pelo **CONTRATADO**, de acordo com o contrato e seus anexos;

8.1.2. Receber o objeto no prazo e condições estabelecidas no Termo de Referência;

8.1.3. Notificar o **CONTRATADO**, por escrito, sobre vícios, defeitos ou incorreções verificadas no objeto fornecido, para que seja por ele substituído, reparado ou corrigido, no total ou em parte, às suas expensas;

8.1.4. Acompanhar e fiscalizar a execução do contrato e o cumprimento das obrigações pelo **CONTRATADO**;

8.1.5. Comunicar a empresa para emissão de Nota Fiscal relativa à parcela incontroversa da execução do objeto, para efeito de liquidação e pagamento, quando houver controvérsia sobre a execução do objeto, quanto à dimensão, qualidade e quantidade, conforme o art. 143 da Lei nº 14.133, de 2021;

8.1.6. Efetuar o pagamento ao **CONTRATADO** do valor correspondente à execução do objeto, no prazo, forma e condições estabelecidos no presente Contrato e no Termo de Referência;

8.1.7. Aplicar ao **CONTRATADO** as sanções previstas na lei e neste Contrato;

8.1.8. Cientificar o órgão de representação judicial da Advocacia-Geral da União para adoção das medidas cabíveis quando do descumprimento de obrigações pelo **CONTRATADO**;

8.1.9. Explicitamente emitir decisão sobre todas as solicitações e reclamações relacionadas à execução do presente Contrato, ressalvados os requerimentos manifestamente impertinentes, meramente protelatórios ou de nenhum interesse para a boa execução do ajuste.

8.1.9.1. A Administração terá o prazo de 45 (quarenta e cinco) dias, a contar da data do protocolo do requerimento para decidir, admitida a prorrogação motivada, por igual período.

8.1.10. Responder eventuais pedidos de reestabelecimento do equilíbrio econômico-financeiro feitos pelo **CONTRATADO** no prazo máximo de 45 (quarenta e cinco) dias.

8.1.11. Notificar os emitentes das garantias quanto ao início de processo administrativo para apuração de descumprimento de cláusulas contratuais.

8.1.12. Comunicar o **CONTRATADO** na hipótese de posterior alteração do projeto pelo **CONTRATANTE**, no caso do art. 93, §2º, da Lei nº 14.133, de 2021.

8.2. A Administração não responderá por quaisquer compromissos assumidos pelo **CONTRATADO** com terceiros, ainda que vinculados à execução do contrato, bem como por qualquer dano causado a terceiros em decorrência de ato do **CONTRATADO**, de seus empregados, prepostos ou subordinados.

9. CLÁUSULA NONA – OBRIGAÇÕES DO CONTRATADO (ART. 92, XIV, XVI E XVII)

9.1. O **CONTRATADO** deve cumprir todas as obrigações constantes deste Contrato e de seus anexos, assumindo como exclusivamente seus os riscos e as despesas decorrentes da boa e perfeita execução do objeto, observando, ainda, as obrigações a seguir dispostas, além das previstas no Termo de Referência:

9.1.1. Manter preposto aceito pela Administração no local da obra ou do serviço para representá-lo na execução do contrato.

9.1.1.1. A indicação ou a manutenção do preposto da empresa poderá ser recusada pelo órgão ou entidade, desde que devidamente justificada, devendo a empresa designar outro para o exercício da atividade.

9.1.2. Atender às determinações regulares emitidas pelo fiscal do contrato ou autoridade superior (art. 137, II) e prestar todo esclarecimento ou informação por eles solicitados;

9.1.3. Alocar os empregados necessários ao perfeito cumprimento das cláusulas deste contrato, com habilitação e conhecimento adequados, fornecendo os materiais, equipamentos, ferramentas e utensílios demandados, cuja quantidade, qualidade e tecnologia deverão atender às recomendações de boa técnica e a legislação de regência;

9.1.4. Reparar, corrigir, remover, reconstruir ou substituir. às suas expensas, no total ou em parte, no prazo fixado pelo fiscal do contrato, os serviços nos quais verificarem vícios, defeitos ou incorreções resultantes da execução ou dos materiais empregados.

9.1.5. Responsabilizar-se pelos vícios e danos decorrentes da execução do objeto, de acordo com o Código de Defesa do Consumidor (Lei nº 8.078, de 1990), bem como por todo e qualquer dano causado à Administração ou terceiros, não reduzindo essa responsabilidade a fiscalização ou o acompanhamento da execução contratual pelo Contratante, que ficará autorizado a descontar dos pagamentos devidos ou da garantia, caso exigida no edital, o valor correspondente aos danos sofridos;

9.1.6. Não contratar, durante a vigência do contrato, cônjuge, companheiro ou parente em linha reta, colateral ou por afinidade, até o terceiro grau, de dirigente do contratante ou do fiscal ou gestor do contrato, nos termos do artigo 48, parágrafo único, da Lei nº 14.133, de 2021;

9.1.7. Quando não for possível a verificação da regularidade no Sistema de Cadastro de Fornecedores – SICAF, o **CONTRATADO** deverá entregar ao setor responsável pela fiscalização do contrato, até o dia trinta do mês seguinte ao da prestação dos serviços, os seguintes documentos: 1) prova de regularidade relativa à Seguridade Social; 2) certidão conjunta relativa aos tributos federais e à Dívida Ativa da União; 3) certidões que comprovem a regularidade perante a Fazenda Municipal ou Distrital do domicílio ou sede do **CONTRATADO**; 4) Certidão de Regularidade do FGTS – CRF; e 5) Certidão Negativa de Débitos Trabalhistas – CNDT;

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

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

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

9.1.11. Paralisar, por determinação do **CONTRATANTE**, qualquer atividade que não esteja sendo executada de acordo com a boa técnica ou que ponha em risco a segurança de pessoas ou bens de terceiros.

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

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

9.1.14. Submeter previamente, por escrito, ao **CONTRATANTE**, para análise e aprovação, quaisquer mudanças nos métodos executivos que fujam às especificações do memorial descritivo ou instrumento congênere.

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

9.1.16. Manter durante toda a vigência do contrato, em compatibilidade com as obrigações assumidas, todas as condições exigidas para habilitação na licitação;

9.1.17. Cumprir, durante todo o período de execução do contrato, a reserva de cargos prevista em lei para pessoa com deficiência, para reabilitado da Previdência Social ou para aprendiz, bem como as reservas de cargos previstas na legislação (art. 116);

9.1.18. Comprovar a reserva de cargos a que se refere a cláusula acima, no prazo fixado pelo fiscal do contrato, com a indicação dos empregados que preencheram as referidas vagas (art. 116, parágrafo único);

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

9.1.20. 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, devendo complementá-los, caso o previsto inicialmente em sua proposta não seja satisfatório para o atendimento do objeto da contratação, exceto quando ocorrer algum dos eventos arrolados no art. 124, II, d, da Lei nº 14.133, de 2021;

9.1.21. Cumprir, além dos postulados legais vigentes de âmbito federal, estadual ou municipal, as normas de segurança do **CONTRATANTE**;

9.1.22. Realizar os serviços de manutenção e assistência técnica no(s) seguinte(s) local(is):

a) Ministério da Agricultura e Pecuária - MAPA. Esplanada dos Ministérios - Bloco D e Anexos - Brasília/DF - CEP: 70.043-900; e

b) Remotamente, de acordo com o especificado no Termo de Referência.

9.1.22.1. O técnico deverá se deslocar ao local da repartição sempre que necessário e sem custos, de acordo com o Termo de Referência.

9.1.23. Alocar os empregados necessários, com habilitação e conhecimento adequados, ao perfeito cumprimento das cláusulas deste contrato, fornecendo os materiais, equipamentos, ferramentas e utensílios demandados, cuja quantidade, qualidade e tecnologia deverão atender às recomendações de boa técnica e a legislação de regência;

9.1.24. Orientar e treinar seus empregados sobre os deveres previstos na Lei nº 13.709, de 14 de agosto de 2018, adotando medidas eficazes para proteção de dados pessoais a que tenha acesso por força da execução deste contrato;

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

9.1.26. Submeter previamente, por escrito, ao contratante, para análise e aprovação, quaisquer mudanças nos métodos executivos que fujam às especificações do memorial descritivo ou instrumento congênere.

9.1.27. 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.

9.1.28. Observar a Política de Segurança da Informação do MAPA e os seus atos normativos complementares.

10. CLÁUSULA DÉCIMA – GARANTIA DE EXECUÇÃO (ART. 92, XII E XIII)

10.1. A contratação conta com garantia de execução, nos moldes do art. 96 da Lei nº 14.133, de 2021, na modalidade XXXXXX, em valor correspondente a 6,5% (seis e meio por cento) do valor anual do contrato.

OU

O **CONTRATADO** apresentará, no prazo máximo de 10 (dez) dias úteis, prorrogáveis por igual período, a critério do contratante, contado da assinatura do contrato, comprovante de prestação de garantia, podendo optar por caução em dinheiro ou títulos da dívida pública ou, ainda, pela fiança bancária, em valor correspondente a 6,5% (seis e meio por cento) do valor anual do contrato.

10.2. Caso utilizada a modalidade de seguro-garantia, a apólice deverá ter validade durante a vigência do contrato e por 90 (noventa) dias após término deste prazo de vigência, permanecendo em vigor mesmo que o **CONTRATADO** não pague o prêmio nas datas convencionadas.

10.3. A apólice do seguro garantia deverá acompanhar as modificações referentes à vigência do contrato principal mediante a emissão do respectivo endosso pela seguradora.

10.4. Será permitida a substituição da apólice de seguro-garantia na data de renovação ou de aniversário, desde que mantidas as condições e coberturas da apólice vigente e nenhum período fique descoberto, ressalvado o disposto no item 10.5 deste contrato.

10.5. Na hipótese de suspensão do contrato por ordem ou inadimplemento da Administração, o **CONTRATADO** ficará desobrigado de renovar a garantia ou de endossar a apólice de seguro até a ordem de reinício da execução ou o adimplemento pela Administração.

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

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

10.6.2. multas moratórias e punitivas aplicadas pela Administração ao **CONTRATADO**; e

10.6.3. obrigações trabalhistas e previdenciárias de qualquer natureza e para com o FGTS, não adimplidas pelo contratado, quando couber.

10.7. A modalidade seguro-garantia somente será aceita se contemplar todos os eventos indicados no item 10.6, observada a legislação que rege a matéria.

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

10.9. 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 Economia.

10.10. No caso de garantia na modalidade de fiança bancária, deverá ser emitida por banco ou instituição financeira devidamente autorizada a operar no País pelo Banco Central do Brasil, e deverá constar expressa renúncia do fiador aos benefícios do artigo 827 do Código Civil.

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

10.12. Se o valor da garantia for utilizado total ou parcialmente em pagamento de qualquer obrigação, o **CONTRATADO** obriga-se a fazer a respectiva reposição no prazo máximo de 05 (cinco) dias úteis, contados da data em que for notificada.

10.13. O **CONTRATANTE** executará a garantia na forma prevista na legislação que rege a matéria.

10.13.1. O emitente da garantia ofertada pelo **CONTRATADO** deverá ser notificado pelo **CONTRATANTE** quanto ao início de processo administrativo para apuração de descumprimento de cláusulas contratuais (art. 137, § 4º, da Lei nº 14.133, de 2021).

10.13.2. Caso se trate da modalidade seguro-garantia, ocorrido o sinistro durante a vigência da apólice, sua caracterização e comunicação poderão ocorrer fora desta vigência, não caracterizando fato que justifique a negativa do sinistro, desde que respeitados os prazos prescricionais aplicados ao contrato de seguro, nos termos do art. 20 da Circular Susep nº 662, de 11 de abril de 2022.

10.14. Extinguir-se-á a garantia com a restituição da apólice, carta fiança ou autorização para a liberação de importâncias depositadas em dinheiro a título de garantia, acompanhada de declaração do **CONTRATANTE**, mediante termo circunstanciado, de que o **CONTRATADO** cumpriu todas as cláusulas do contrato;

10.15. A garantia somente será liberada ou restituída após a fiel execução do contrato ou após a sua extinção por culpa exclusiva da Administração e, quando em dinheiro, será atualizada monetariamente.

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

10.17. O **CONTRATADO** autoriza o **CONTRATANTE** a reter, a qualquer tempo, a garantia, na forma prevista no Edital e neste Contrato.

10.18. A garantia de execução é independente de eventual garantia do produto ou serviço prevista especificamente no Termo de Referência.

11. CLÁUSULA DÉCIMA PRIMEIRA – INFRAÇÕES E SANÇÕES ADMINISTRATIVAS (ART. 92, XIV)

11.1. Comete infração administrativa, nos termos da Lei nº 14.133, de 2021, o **CONTRATADO** que:

a) der causa à inexecução parcial do contrato;

b) der causa à inexecução parcial do contrato que cause grave dano à Administração ou ao funcionamento dos serviços públicos ou ao interesse coletivo;

c) der causa à inexecução total do contrato;

d) ensejar o retardamento da execução ou da entrega do objeto da contratação sem motivo justificado;

e) apresentar documentação falsa ou prestar declaração falsa durante a execução do contrato;

f) praticar ato fraudulento na execução do contrato;

g) comportar-se de modo inidôneo ou cometer fraude de qualquer natureza;

h) praticar ato lesivo previsto no art. 5º da Lei nº 12.846, de 1º de agosto de 2013.

11.2. Serão aplicadas ao **CONTRATADO** que incorrer nas infrações acima descritas as seguintes sanções:

I - **Advertência**, quando o **CONTRATADO** der causa à inexecução parcial do contrato, sempre que não se justificar a imposição de penalidade mais grave (art. 156, §2º, da Lei nº 14.133, de 2021);

II - **Impedimento de licitar e contratar**, quando praticadas as condutas descritas nas alíneas "b", "c" e "d" do subitem acima deste Contrato, sempre que não se justificar a imposição de penalidade mais grave (art. 156, § 4º, da Lei nº 14.133, de 2021);

III - **Declaração de inidoneidade para licitar e contratar**, quando praticadas as condutas descritas nas alíneas "e", "f", "g" e "h" do subitem acima deste Contrato, bem como nas alíneas "b", "c" e "d", que justifiquem a imposição de penalidade mais grave (art. 156, §5º, da Lei nº 14.133, de 2021).

IV - **Multa:**

1. moratória de 0,25% (vinte e cinco centésimos por cento) por dia de atraso injustificado sobre o valor da parcela inadimplida, até o limite de 60 (sessenta) dias;

2. moratória de 0,07% (sete centésimos por cento) por dia de atraso injustificado sobre o valor total do contrato, até o máximo de 2% (dois por cento), pela inobservância do prazo fixado para apresentação, suplementação ou reposição da garantia.

a) O atraso superior a 25 (vinte e cinco) dias autoriza a Administração a promover a extinção do contrato por descumprimento ou cumprimento irregular de suas cláusulas, conforme dispõe o inciso I do art. 137 da Lei n. 14.133, de 2021.

3. Compensatória, para as infrações descritas nas alíneas "e" a "h" do subitem 11.1, de 3,5% (três vírgula cinco por cento) do valor do Contrato.

4. Compensatória, para a inexecução total do contrato prevista na alínea "c" do subitem 11.1, de 3,5% (três vírgula cinco por cento) do valor do Contrato.

5. Para infração descrita na alínea "b" do subitem 11.1, a multa será de 2,5% (dois vírgula cinco por cento) do valor do Contrato.

6. Para infrações descritas na alínea "d" do subitem 11.1, a multa será de 2,5% (dois vírgula cinco por cento) do valor do Contrato.

7. Para a infração descrita na alínea "a" do subitem 11.1, a multa será de 1% (um por cento) do valor do Contrato, ressalvadas as seguintes infrações:

- Ausência de atualizações de segurança dos softwares envolvidos de toda a solução de TIC;

- Desempenho insatisfatório com determinados tipos de tráfego; e

- Ausência de funcionalidades prometidas.

11.3. A aplicação das sanções previstas neste Contrato não exclui, em hipótese alguma, a obrigação de reparação integral do dano causado ao **CONTRATANTE** (art. 156, §9º, da Lei nº 14.133, de 2021).

11.4. Todas as sanções previstas neste Contrato poderão ser aplicadas cumulativamente com a multa (art. 156, §7º, da Lei nº 14.133, de 2021).

11.4.1. Antes da aplicação da multa será facultada a defesa do interessado no prazo de 15 (quinze) dias úteis, contado da data de sua intimação (art. 157, da Lei nº 14.133, de 2021).

11.4.2. Se a multa aplicada e as indenizações cabíveis forem superiores ao valor do pagamento eventualmente devido pelo **CONTRATANTE** ao **CONTRATANTE**, além da perda desse valor, a diferença será descontada da garantia prestada ou será cobrada judicialmente (art. 156, §8º, da Lei nº 14.133, de 2021).

11.4.3. Previamente ao encaminhamento à cobrança judicial, a multa poderá ser recolhida administrativamente no prazo máximo de 30 (trinta) dias, a contar da data do recebimento da comunicação enviada pela autoridade competente.

11.5. A aplicação das sanções realizar-se-á em processo administrativo que assegure o contraditório e a ampla defesa ao **CONTRATADO**, observando-se o procedimento previsto no caput e parágrafos do art. 158 da Lei nº 14.133, de 2021, para as penalidades de impedimento de licitar e contratar e de declaração de inidoneidade para licitar ou contratar.

11.6. Na aplicação das sanções serão considerados (art. 156, §1º, da Lei nº 14.133, de 2021):

a) a natureza e a gravidade da infração cometida;

b) as peculiaridades do caso concreto;

c) as circunstâncias agravantes ou atenuantes;

d) os danos que dela provierem para o **CONTRATANTE**;

e) a implantação ou o aperfeiçoamento de programa de integridade, conforme normas e orientações dos órgãos de controle.

11.7. Os atos previstos como infrações administrativas na Lei nº 14.133, de 2021, ou em outras leis de licitações e contratos da Administração Pública que também sejam tipificados como atos lesivos na Lei nº 12.846, de 2013, serão apurados e julgados conjuntamente, nos mesmos autos, observados o rito procedimental e autoridade competente definidos na referida Lei (art. 159).

11.8. A personalidade jurídica do **CONTRATADO** poderá ser desconsiderada sempre que utilizada com abuso do direito para facilitar, encobrir ou dissimular a prática dos atos ilícitos previstos neste Contrato ou para provocar confusão patrimonial, e, nesse caso, todos os efeitos das sanções aplicadas à pessoa jurídica serão estendidos aos seus administradores e sócios com poderes de administração, à pessoa jurídica sucessora ou à empresa do mesmo ramo com relação de coligação ou controle, de fato ou de direito, com o **CONTRATADO**, observados, em todos os casos, o contraditório, a ampla defesa e a obrigatoriedade de análise jurídica prévia (art. 160, da Lei nº 14.133, de 2021).

11.9. O **CONTRATANTE** deverá, no prazo máximo 15 (quinze) dias úteis, contado da data de aplicação da sanção, informar e manter atualizados os dados relativos às sanções por ela aplicadas, para fins de publicidade no Cadastro Nacional de Empresas Inidôneas e Suspensas (Ceis) e no Cadastro Nacional de Empresas Punidas (Cnep), instituídos no âmbito do Poder Executivo Federal. (Art. 161, da Lei nº 14.133, de 2021).

11.10. As sanções de impedimento de licitar e contratar e declaração de inidoneidade para licitar ou contratar são passíveis de reabilitação na forma do art. 163 da Lei nº 14.133/21.

11.11. Os débitos do **CONTRATADO** para com a Administração contratante, resultantes de multa administrativa e/ou indenizações, não inscritos em dívida ativa, poderão ser compensados, total ou parcialmente, com os créditos devidos pelo referido órgão decorrentes deste mesmo contrato ou de outros contratos administrativos que o **CONTRATADO** possua com o mesmo órgão ora contratante, na forma da Instrução Normativa SEGES/ME nº 26, de 13 de abril de 2022.

12. CLÁUSULA DÉCIMA SEGUNDA – DA EXTINÇÃO CONTRATUAL (ART. 92, XIX)

12.1. O contrato será extinto quando vencido o prazo nele estipulado, independentemente de terem sido cumpridas ou não as obrigações de ambas as partes contraentes.

12.2. O contrato poderá ser extinto antes do prazo nele fixado, sem ônus para o **CONTRATANTE**, quando esta não dispuser de créditos orçamentários para sua continuidade ou quando entender que o contrato não mais lhe oferece vantagem.

12.3. A extinção nesta hipótese ocorrerá na próxima data de aniversário do contrato, desde que haja a notificação do **CONTRATADO** pelo **CONTRATANTE** nesse sentido com pelo menos 2 (dois) meses de antecedência desse dia.

12.4. Caso a notificação da não-continuidade do contrato de que trata este subitem ocorra com menos de 2 (dois) meses da data de aniversário, a extinção contratual ocorrerá após 2 (dois) meses da data da comunicação.

12.5. O contrato poderá ser extinto antes de cumpridas as obrigações nele estipuladas, ou antes do prazo nele fixado, por algum dos motivos previstos no artigo 137 da Lei nº 14.133/21, bem como amigavelmente, assegurados o contraditório e a ampla defesa.

12.5.1. Nesta hipótese, aplicam-se também os artigos 138 e 139 da mesma Lei.

12.5.2. A alteração social ou a modificação da finalidade ou da estrutura da empresa não ensejará a extinção se não restringir sua capacidade de concluir o contrato.

12.5.2.1. Se a operação implicar mudança da pessoa jurídica contratada, deverá ser formalizado termo aditivo para alteração subjetiva.

12.6. O termo de extinção, sempre que possível, será precedido:

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

12.6.2. Relação dos pagamentos já efetuados e ainda devidos;

12.6.3. Indenizações e multas.

12.7. A extinção do contrato não configura óbice para o reconhecimento do desequilíbrio econômico-financeiro, hipótese em que será concedida indenização por meio de termo indenizatório (art. 131, *caput*, da Lei n.º 14.133, de 2021).

12.8. O contrato poderá ser extinto caso se constate que o **CONTRATADO** mantém vínculo de natureza técnica, comercial, econômica, financeira, trabalhista ou civil com dirigente do órgão ou entidade contratante ou com agente público que tenha desempenhado função na licitação ou atue na fiscalização ou na gestão do contrato, ou que deles seja cônjuge, companheiro ou parente em linha reta, colateral ou por afinidade, até o terceiro grau (art. 14, inciso IV, da Lei n.º 14.133, de 2021).

13. CLÁUSULA DÉCIMA TERCEIRA – DOTAÇÃO ORÇAMENTÁRIA (ART. 92, VIII)

13.1. As despesas decorrentes da presente contratação correrão à conta de recursos específicos consignados no Orçamento Geral da União deste exercício, na dotação abaixo discriminada:

Gestão/Unidade: 00001/130005

Fonte de Recursos: 100

Programa de Trabalho:

Elemento de Despesa: 339040 e 449052

Plano Interno: PROGESTÃO

Nota de Empenho:

13.2. A dotação relativa aos exercícios financeiros subsequentes será indicada após aprovação da Lei Orçamentária respectiva e liberação dos créditos correspondentes, mediante apostilamento.

14. CLÁUSULA DÉCIMA QUARTA – DOS CASOS OMISSOS (ART. 92, III)

14.1. Os casos omissos serão decididos pelo **CONTRATANTE**, segundo as disposições contidas na Lei nº Lei nº 14.133, de 2021 e demais normas federais aplicáveis e, subsidiariamente, segundo as disposições contidas na Lei nº 8.078, de 1990 – Código de Defesa do Consumidor - normas e princípios gerais dos contratos.

15. CLÁUSULA DÉCIMA QUINTA – ALTERAÇÕES

15.1. Eventuais alterações contratuais reger-se-ão pela disciplina dos arts. 124 e seguintes da Lei nº 14.133, de 2021.

15.2. O **CONTRATADO** é obrigado 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.

15.3. As alterações contratuais deverão ser promovidas mediante celebração de termo aditivo, submetido à prévia aprovação da consultoria jurídica do **CONTRATANTE**, salvo nos casos de justificada necessidade de antecipação de seus efeitos, hipótese em que a formalização do aditivo deverá ocorrer no prazo máximo de 1 (um) mês (art. 132 da Lei nº 14.133, de 2021).

15.4. Registros que não caracterizam alteração do contrato podem ser realizados por simples apostila, dispensada a celebração de termo aditivo, na forma do art. 136 da Lei nº 14.133, de 2021.

16. CLÁUSULA DÉCIMA SEXTA – PUBLICAÇÃO

16.1. Incumbirá ao **CONTRATANTE** divulgar o presente instrumento no Portal Nacional de Contratações Públicas (PNCP), na forma prevista no art. 94 da Lei 14.133, de 2021, bem como no respectivo sítio oficial na Internet, em atenção ao art. 91, *caput*, da Lei nº 14.133, de 2021, e ao art. 8º, §2º, da Lei n. 12.527, de 2011, c/c art. 7º, §3º, inciso V, do Decreto n. 7.724, de 2012.

17. CLÁUSULA DÉCIMA SÉTIMA – FORO (ART. 92, §1º)

17.1. Fica eleito o Foro da Justiça Federal - Seção Judiciária do Distrito Federal para dirimir os litígios que decorrerem da execução deste Termo de Contrato que não puderem ser compostos pela conciliação, conforme art. 92, §1º, da Lei nº 14.133/21.

_____

Responsável legal do **CONTRATANTE**

_____

Responsável legal do **CONTRATADO**

TESTEMUNHAS:

1 -

2 -

Documento assinado eletronicamente por **Larissa Timo Almeida**, **Coordenador (a)**, em 21/09/2023, às 16:09, conforme horário oficial de Brasília, com fundamento no art. 4º,§ 3º, do Decreto nº 10.543, de 13 de novembro de 2020.

A autenticidade deste documento pode ser conferida no site: https://sei.agro.gov.br/sei/controlador_externo.php?acao=documento_conferir&id_orgao_acesso_externo=0 , informando o código verificador **30802542** e o código CRC **E8C9EBE9**.

MINISTÉRIO DA AGRICULTURA E PECUÁRIA
SERVIÇO DE ELABORAÇÃO DE EDITAIS

MODELO DE PROPOSTA DE PREÇOS
(em papel personalizado da empresa)

Processo nº 21000.020025/2023-02

Pregão Eletrônico nº ...../.....

Razão Social: ..... CNPJ: .....

Endereço: ..... Tel./Fax: .....

CEP: ..... Cidade: .....

Banco: ..... Agência: ..... Conta: .....

Apresentamos a nossa proposta para a licitação visando a contratação de empresa para o fornecimento de solução de proteção de rede com características de *Next Generation Firewall* (NGFW), contemplando os hardwares com licenciamento, suporte e garantia, instalação e configuração, treinamento, plataforma de gestão, treinamento e Plataforma de ZTNA pelo período de dois anos, para atender a demanda do Ministério da Agricultura e Pecuária e órgãos demandantes (Ministério da Pesca e Aquicultura/Ministério do Desenvolvimento Agrário e Agricultura Familiar), conforme condições, quantidades e exigências estabelecidas no Edital e seus anexos.

Grupo	Item	Descrição/Especificação	CATSER	Unidade de Medida	Quantidade	Valor Unitário	Valor Total Mensal	Valor Total Anual	Valor Total Global (para dois anos)
Único	1	Appliances físicos - Firewall - Solução de plataforma de segurança, denominada Next Generation Firewall (NGFW), com licenciamento incluso.	481646	Unidade	01				
	2	Suporte, garantia e manutenção do item 01.	27740	Serviço	01				
	3	Appliances físicos - Firewall - Solução de plataforma de segurança, denominada Next Generation Firewall (NGFW).	481646	Unidade	03				
	4	Suporte, garantia e manutenção do item 03.	27740	Serviço	01				
	5	Serviço de instalação e configuração dos firewalls NGFW dos itens 01 e 03.	26972	Serviço	01				
	6	Appliance - Plataforma de gestão e monitoramento centralizado, com licenciamento, instalação e configuração.	481646 / 481647	Unidade	01				
	7	Suporte, garantia e Manutenção do item 06.	27740	Serviço	01				
	8	Treinamento ministrado por profissional certificado pelo fabricante.	16837 / 20052	Capacitação	01				
	9	Plataforma de ZTNA - Zero Trust Network Access.	27742	Serviço	01				
								Valor Total do Grupo (R$)	

Observação: Validade da proposta: 60 (sessenta) dias.

Declaramos que:

1. O preço cotado inclui todas as despesas, tributos e encargos de qualquer natureza incidentes sobre o objeto deste pregão;

2. Quaisquer tributos, custos e despesas omitidas da proposta ou incorretamente cotadas serão considerados como inclusos nos preços, e não serão solicitados acréscimos, a qualquer título, sendo os serviços prestados sem ônus adicional;

3. Caso nos seja adjudicado o objeto da licitação, comprometemo-nos a assinar o contrato dela advindo;

4. Estamos de acordo com as condições estabelecidas no Edital e seus anexos e que tomamos conhecimento de todas as informações e das condições para o cumprimento das obrigações.

Dados do representante legal da empresa para assinatura do contrato:

Nome: .....

Endereço: .....

CEP: ..... Cidade: .....

CPF:..... Cargo/Função: .....

RG: ..... Órgão Expedido: .....

Naturalidade: ..... Nacionalidade: .....

Local e data

.....

Assinatura e carimbo (representante da empresa)

Documento assinado eletronicamente por **LUCAS BEZERRA CAMPOS**, **Agente Administrativo**, em 26/09/2023, às 15:47, conforme horário oficial de Brasília, com fundamento no art. 4º,§ 3º, do Decreto nº 10.543, de 13 de novembro de 2020.

A autenticidade deste documento pode ser conferida no site: https://sei.agro.gov.br/sei/controlador_externo.php?acao=documento_conferir&id_orgao_acesso_externo=0 , informando o código verificador **31209666** e o código CRC **9576EBA7**.