Ministério da Justiça e Segurança Pública
Divisão de Licitações

PREGÃO ELETRÔNICO Nº 09/2023

PROCESSO Nº 08006.000158/2023-36

Torna-se público que o Ministério da Justiça e Segurança Pública (UASG 200005), realizará licitação, na modalidade PREGÃO, na forma ELETRÔNICA, sob a forma de execução indireta, nos termos da Lei nº 10.520, de 17 de julho de 2002, do Decreto nº 10.024, de 20 de setembro de 2019, do Decreto 9.507, de 21 de setembro de 2018, do Decreto nº 7.746, de 05 de junho de 2012, das Instruções Normativas SEGES/MP nº 05, de 26 de maio de 2017 e nº 03, de 26 de abril de 2018 e da Instrução Normativa SLTI/MP nº 01, de 19 de janeiro de 2010, da Lei Complementar n° 123, de 14 de dezembro de 2006, da Lei nº 11.488, de 15 de junho de 2007, do Decreto n° 8.538, de 06 de outubro de 2015, aplicando-se, subsidiariamente, a Lei nº 8.666, de 21 de junho de 1993 e as exigências estabelecidas neste Edital.

Data da sessão: 18/09/2023

Horário: 10h00

Local: Portal de Compras do Governo Federal – **https://www.gov.br/compras/pt-br**

Critério de Julgamento: Menor Preço por Grupo

Regime de Execução: Empreitada por Preço Unitário

1. DO OBJETO

1.1. O objeto da presente licitação é a escolha da proposta mais vantajosa para a contratação de solução de firewall contemplando serviços de instalação e suporte técnico com garantia pelo período de 60 meses, com vistas a atender às necessidades do Ministério da Justiça e Segurança Pública - MJSP.**,** conforme condições, quantidades e exigências estabelecidas neste Edital e seus anexos.

1.2. A licitação será realizada em grupo único, formados por 04 itens, conforme tabela constante no Termo de Referência, devendo o licitante oferecer proposta para todos os itens que o compõem.

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

2. DOS RECURSOS ORÇAMENTÁRIOS

2.1. As despesas para atender a esta licitação estão programadas em dotação orçamentária

própria, prevista no orçamento da União para o exercício de 2023, na classificação abaixo:

2.1.1. Programa de Trabalho: 04122003220000000001

2.1.2. Plano de Trabalho Resumido (PTRES): 172184

2.1.3. Fonte: 1000

2.1.4. Ação: 2000

2.1.5. Plano Orçamentário (PO): 000C

2.1.6. Plano Interno (PI): GL67OTCGLTI

2.1.7. As Naturezas de despesas serão detalhadas da tabela abaixo:

Grupo	Item	Descrição do Bem ou Serviço	Natureza de Despesa
1	1	FIREWALL TIPO I - APPLIANCE FÍSICO	449052
	2	FIREWALL TIPO II - APPLIANCE FÍSICO	449052
	3	APPLIANCE FÍSICO PARA ANÁLISE DO TRÁFEGO DE DADOS	449052
	4	APPLIANCE VIRTUAL DE GERENCIAMENTO CENTRALIZADO	449040

Tabela 11 - Natureza de despesa dos bens

3. DO CREDENCIAMENTO

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

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

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

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

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

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

4. DA PARTICIPAÇÃO NO PREGÃO

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

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

4.1.2. Será concedido tratamento favorecido para as microempresas e empresas de pequeno porte, para as sociedades cooperativas mencionadas no artigo 34 da Lei nº 11.488, de 2007, para o agricultor familiar, o produtor rural pessoa física e para o microempreendedor

individual - MEI, nos limites previstos da Lei Complementar nº 123, de 2006.

4.2. Não poderão participar desta licitação os interessados:

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

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

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

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

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

4.2.6. entidades empresariais que estejam reunidas em consórcio;

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

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

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

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

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

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

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

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

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

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

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

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

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

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

4.5.5. que não emprega menor de 18 anos em trabalho noturno, perigoso ou insalubre e não emprega menor de 16 anos, salvo menor, a partir de 14 anos, na condição de aprendiz, nos termos do artigo 7°, XXXIII, da Constituição;

4.5.6. que a proposta foi elaborada de forma independente;

4.5.7. que não possui, em sua cadeia produtiva, empregados executando trabalho degradante ou forçado, observando o disposto nos incisos III e IV do art. 1º e no inciso III do art. 5º da Constituição Federal;

4.5.8. que a solução é fornecida por empresas que comprovem cumprimento de reserva de cargos prevista em lei para pessoa com deficiência ou para reabilitado da Previdência Social e que atendam às regras de acessibilidade previstas na legislação, conforme disposto no art. 93 da Lei nº 8.213, de 24 de julho de 1991.

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

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

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

5. DA APRESENTAÇÃO DA PROPOSTA E DOS DOCUMENTOS DE HABILITAÇÃO

5.1. Os licitantes encaminharão, exclusivamente por meio do sistema, concomitantemente com os documentos de habilitação exigidos no edital, proposta com a descrição do objeto ofertado e o preço, até a data e o horário estabelecidos para abertura da sessão pública, quando, então, encerrar-se-á automaticamente a etapa de envio dessa documentação

5.2. O envio da proposta, acompanhada dos documentos de habilitação exigidos neste Edital, ocorrerá por meio de chave de acesso e senha.

5.3. Os licitantes poderão deixar de apresentar os documentos de habilitação que constem do SICAF, assegurado aos demais licitantes o direito de acesso aos dados constantes dos sistemas.

5.4. As Microempresas e Empresas de Pequeno Porte deverão encaminhar a documentação de habilitação, ainda que haja alguma restrição de regularidade fiscal e trabalhista, nos termos do art. 43, § 1º da LC nº 123, de 2006.

5.5. Incumbirá ao licitante acompanhar as operações no sistema eletrônico durante a sessão pública do Pregão, ficando responsável pelo ônus decorrente da perda de negócios, diante da inobservância de quaisquer mensagens emitidas pelo sistema ou de sua desconexão.

5.6. Até a abertura da sessão pública, os licitantes poderão retirar ou substituir a proposta e os documentos de habilitação anteriormente inseridos no sistema

5.7. Não será estabelecida, nessa etapa do certame, ordem de classificação entre as propostas apresentadas, o que somente ocorrerá após a realização dos procedimentos de negociação e julgamento da proposta.

5.8. Os documentos que compõem a proposta e a habilitação do licitante melhor classificado somente serão disponibilizados para avaliação do pregoeiro e para acesso público após o encerramento do envio de lances.

6. DO PREENCHIMENTO DA PROPOSTA

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

6.1.1. valor total do item*;*

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

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

6.3. Nos valores propostos estarão inclusos todos os custos operacionais, encargos previdenciários, trabalhistas, tributários, comerciais e quaisquer outros que incidam direta ou indiretamente na prestação dos serviços, apurados mediante o preenchimento do modelo de Planilha de Custos e Formação de Preços, conforme anexo deste Edital;

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

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

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

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

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

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

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

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

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

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

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

6.10.1. O descumprimento das regras supramencionadas pela Administração por parte dos contratados pode ensejar a responsabilização pelo Tribunal de Contas da União e, após o devido processo legal, gerar as seguintes consequências: assinatura de prazo para a adoção das medidas necessárias ao exato cumprimento da lei, nos termos do art. 71, inciso IX, da Constituição; ou condenação dos agentes públicos responsáveis e da empresa contratada ao pagamento dos prejuízos ao erário, caso verificada a ocorrência de superfaturamento por sobrepreço na execução do contrato

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

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

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

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

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

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

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

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

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

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

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

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

7.8. O intervalo mínimo de diferença de valores 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 1% (um por cento).

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

7.25.4. As licitantes qualificadas como microempresas ou empresas de pequeno porte que fizerem jus ao direito de preferência previsto no Decreto nº 7.174, de 2010, terão prioridade no exercício desse benefício em relação às médias e às grandes empresas na mesma situação.

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

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

7.27.1. por empresas brasileiras;

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

7.27.3. por empresas que comprovem cumprimento de reserva de cargos prevista em lei para pessoa com deficiência ou para reabilitado da Previdência Social e que atendam às regras de acessibilidade previstas na legislação.

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

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

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

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

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

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

8. DA ACEITABILIDADE DA PROPOSTA VENCEDORA.

8.1. Encerrada a etapa de negociação, o pregoeiro examinará a proposta classificada em primeiro lugar quanto à adequação ao objeto e à compatibilidade do preço em relação ao máximo

estipulado para contratação neste Edital e em seus anexos, observado o disposto no parágrafo único do art. 7º e no § 9º do art. 26 do Decreto n.º 10.024/2019.

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

8.3. A Planilha de Custos e Formação de Preços deverá ser encaminhada pelo licitante exclusivamente via sistema, no prazo de 02 (duas) horas, contado da solicitação do Pregoeiro, com os respectivos valores adequados ao lance vencedor e será analisada pelo Pregoeiro no momento da aceitação do lance vencedor.

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

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

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

8.5.2. contenha vício insanável ou ilegalidade;

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

8.5.4. apresentar preço final superior ao preço máximo fixado (Acórdão nº 1455/2018 - TCU - Plenário), percentual de desconto inferior ao mínimo exigido, ou que apresentar preço manifestamente inexequível;.

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

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

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

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

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

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

8.8.1. Na hipótese de necessidade de suspensão da sessão pública para a realização de diligências, com vistas ao saneamento das propostas, a sessão pública somente poderá ser

reiniciada mediante aviso prévio no sistema com, no mínimo, vinte e quatro horas de antecedência, e a ocorrência será registrada em ata

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

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

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

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

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

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

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

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

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

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

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

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

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

9. DA HABILITAÇÃO

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

a) SICAF;

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

c) Cadastro Nacional de Condenações Cíveis por Atos de Improbidade Administrativa,

mantido pelo Conselho Nacional de Justiça (www.cnj.jus.br/improbidade_adm/consultar_requerido.php).

d) Lista de Inidôneos mantida pelo Tribunal de Contas da União - TCU (https://contas.tcu.gov.br/ords/f?p=INABILITADO:CERTIDAO:0:);

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

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

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

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

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

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

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

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

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

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

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

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

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

integridade do documento digital.

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

9.6. Se o licitante for a matriz, todos os documentos deverão estar em nome da matriz, e se o licitante for a filial, todos os documentos deverão estar em nome da filial, exceto para atestados de capacidade técnica, e no caso daqueles documentos que, pela própria natureza, comprovadamente, forem emitidos somente em nome da matriz.

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

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

9.8. **Habilitação jurídica:**

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

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

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

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

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

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

9.9. **Regularidade fiscal e trabalhista:**

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

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

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

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

9.9.5. prova de inscrição no cadastro de contribuintes Estadual/Distrital **OU** Municipal, relativo ao domicílio ou sede do licitante, pertinente ao seu ramo de atividade e compatível com o objeto contratual;

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

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

9.10. **Qualificação Econômico-Financeira:**

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

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

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

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

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

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

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

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

9.10.4. As empresas que apresentarem resultado inferior ou igual a 1(um) em qualquer dos índices de Liquidez Geral (LG), Solvência Geral (SG) e Liquidez Corrente (LC), deverão comprovar patrimônio líquido de 10% (dez por cento) do valor total estimado da contratação ou do item pertinente.

9.11. **Qualificação Técnica:**

9.11.1. **Da vistoria técnica**

9.11.1.1. Para o correto dimensionamento e elaboração de sua proposta, o licitante *poderá* realizar vistoria nas instalações do local onde serão instalados os firewalls, acompanhado por servidor designado para esse fim, de segunda à sexta-feira, das 08:00 horas às 18:00 horas, agendada com antecedência mínima de 12 (doze) horas através do e-mail (correio eletrônico): **citic@mj.gov.br**.

9.11.1.1.1. O prazo para vistoria iniciar-se-á no dia útil seguinte ao da publicação do Edital, estendendo-se até o dia útil anterior à data prevista para a abertura da sessão pública.

9.11.1.2. Para a vistoria o licitante, ou o seu representante legal, deverá estar devidamente identificado, apresentando documento de identidade civil e documento expedido pela empresa comprovando sua habilitação para a realização da vistoria.

9.11.1.3. Por ocasião da vistoria, ao licitante, ou ao seu representante legal, poderá ser entregue CD-ROM, "pen-drive" ou outra forma compatível de reprodução, contendo as informações relativas ao objeto da licitação, para que a empresa tenha condições de bem elaborar sua proposta.

9.11.1.4. A não realização da vistoria, quando facultativa, não poderá embasar posteriores alegações de desconhecimento das instalações, dúvidas ou esquecimentos de quaisquer detalhes dos locais da prestação dos serviços, devendo a licitante vencedora assumir os ônus dos serviços decorrentes.

9.11.1.5. A licitante deverá declarar que tomou conhecimento de todas as informações e das condições locais para o cumprimento das obrigações objeto da licitação.

9.11.2. **Qualificação técnica**

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

9.11.2.2. Para efeito de aferição da qualificação técnica do fornecedor, o(s) licitante(s) deverá(ão) apresentar atestado(s) de capacidade técnica em seu(s) nome(s), fornecido por pessoa jurídica de direito público ou privado, comprovando:

9.11.2.3. **Grupo I:**

9.11.2.3.1. No mínimo o fornecimento de 50% do quantitativo do item 1 e 50% do item 2 com características compatíveis com as especificadas nesse Termo de Referência.

9.11.2.3.2. O quantitativo previsto para o item 2 é de 5 (cinco) equipamentos, o que resultará em número fracionado. Sendo assim, considera-se o mínimo exigido de 2 (dois) equipamentos.

9.11.2.4. Poderá ser apresentado mais de um atestado para fim de comprovação da qualificação técnica.

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

9.11.2.5. Caso não haja menção explícita no atestado quanto às funcionalidades solicitadas, deve ser apresentada documentação oficial do fabricante que comprove tal suporte nos modelos constantes no atestado.

9.11.2.5.1. É vetada a indicação de entidade certificadora, exceto nos casos previamente dispostos em normas da Administração Pública.

9.11.2.5.2. É vetada a exigência, para fins de qualificação técnica na fase de habilitação, de atestado, declaração, carta de solidariedade, comprovação de parceria ou credenciamento emitidos por fabricantes.

9.11.2.6. O licitante disponibilizará todas as informações necessárias à comprovação da legitimidade dos atestados apresentados, apresentando, dentre outros documentos,

cópia do contrato que deu suporte à contratação, endereço atual da contratante e local em que foram prestados os serviços, consoante o disposto no item 10.10 do Anexo VII-A da IN SEGES/MPDG n. 5/2017.

9.11.2.7. As competências exigidas correspondem às quantidades relevantes dos itens mais críticos para assegurar que a LICITANTE tenha efetiva capacidade de prestar os serviços considerando a complexidade da infraestrutura de TI que a CONTRATANTE deseja implementar. Além disso, conforme exposto na justificativa da contratação, pretende-se realizar melhorias na topologia de firewall do MJSP, o que torna essencial, para garantir a correta implementação do projeto, que configurações adequadas, desempenho, qualidade, além da disponibilidade, confiabilidade e integridade das informações, sejam garantidas pela LICITANTE, sendo isso exposto pelas qualificações técnicas solicitadas.

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

9.11.4. A s empresas, cadastradas ou não no SICAF, deverão apresentar atestado de vistoria assinado pelo servidor responsável, caso exigida no Termo de Referência.

9.11.5. O atestado de vistoria poderá ser substituído por declaração emitida pelo licitante em que conste, alternativamente, ou que conhece as condições locais para execução do objeto; ou que tem pleno conhecimento das condições e peculiaridades inerentes à natureza do trabalho, assume total responsabilidade por este fato e não utilizará deste para quaisquer questionamentos futuros que ensejem desavenças técnicas ou financeiras com a contratante.

9.12. O licitante enquadrado como microempreendedor individual que pretenda auferir os benefícios do tratamento diferenciado previstos na Lei Complementar n. 123, de 2006, estará dispensado da prova de inscrição nos cadastros de contribuintes estadual e municipal

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

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

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

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

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

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

9.18. Nos itens não exclusivos a microempresas e empresas de pequeno porte, em havendo inabilitação, haverá nova verificação, pelo sistema, da eventual ocorrência do empate ficto, previsto

nos artigos 44 e 45 da LC nº 123, de 2006, seguindo-se a disciplina antes estabelecida para aceitação da proposta subsequente.

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

10. DO ENCAMINHAMENTO DA PROPOSTA VENCEDORA

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

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

10.1.2. apresentar a proposta de custos e formação de preços, devidamente ajustada ao lance vencedor, em conformidade com o modelo anexo a este Edital;

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

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

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

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

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

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

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

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

11. DOS RECURSOS

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

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

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

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

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

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

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

12. DA REABERTURA DA SESSÃO PÚBLICA

12.1. A sessão pública poderá ser reaberta:

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

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

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

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

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

13. DA ADJUDICAÇÃO E HOMOLOGAÇÃO

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

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

14. DA GARANTIA DE EXECUÇÃO

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

15. DO TERMO DE CONTRATO OU INSTRUMENTO EQUIVALENTE

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

15.2. O adjudicatário terá o prazo de 05 (cinco) dias úteis, contados a partir da data de sua convocação, para assinar o Termo de Contrato, sob pena de decair do direito à contratação, sem prejuízo das sanções previstas neste Edital.

15.2.1. O presente instrumento será firmado através de assinatura eletrônica e/ou digital, certificada pelo Sistema Eletrônico de Informações do Ministério da Justiça e Segurança Pública, garantida a eficácia das Cláusulas, nos termos do Decreto nº 8.539, de 08 de outubro de 2015.

15.2.2. O prazo previsto no subitem 15.2 poderá ser prorrogado, por igual período, por solicitação justificada do adjudicatário e aceita pela Administração.

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

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

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

15.4. Na assinatura do contrato, será exigida a comprovação das condições de habilitação consignadas no edital, que deverão ser mantidas pelo licitante durante a vigência do contrato.

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

15.6. O prazo de vigência da contratação é o estabelecido no Termo de Referência.

16. DO REAJUSTAMENTO EM SENTIDO GERAL

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

17. DO RECEBIMENTO DO OBJETO E DA FISCALIZAÇÃO

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

18. DAS OBRIGAÇÕES DA CONTRATANTE E DA CONTRATADA

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

19. DO PAGAMENTO

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

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

20. DAS SANÇÕES ADMINISTRATIVAS.

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

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

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

20.1.3. apresentar documentação falsa;

20.1.4. deixar de entregar os documentos exigidos no certame;

20.1.5. ensejar o retardamento da execução do objeto;

20.1.6. não mantiver a proposta;

20.1.7. cometer fraude fiscal;

20.1.8. comportar-se de modo inidôneo;

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

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

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

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

20.4.2. Multa de 2% (dois por cento) sobre o valor estimado do(s) item(s) prejudicado(s) pela conduta do licitante;

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

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

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

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

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

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

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

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

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

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

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

20.14. As penalidades serão obrigatoriamente registradas no SICAF.

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

21. DA IMPUGNAÇÃO AO EDITAL E DO PEDIDO DE ESCLARECIMENTO

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

21.2. A impugnação poderá ser realizada por forma eletrônica, pelo e-mail licitacao@mj.gov.br, ou por petição dirigida ou protocolada no endereço à Coordenação de Procedimentos Licitatórios/COPLI – MJ, situada à Esplanada dos Ministérios, Bloco “T”, Anexo II, sala 612, em Brasília – DF, CEP 70064-900.

21.3. Caberá ao Pregoeiro, auxiliado pelos responsáveis pela elaboração deste Edital e seus anexos, decidir sobre a impugnação no prazo de até 2 (dois) dias úteis contados da data de recebimento da impugnação.

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

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

21.6. O Pregoeiro responderá aos pedidos de esclarecimentos no prazo de 2 (dois) dias úteis, contado da data de recebimento do pedido, e poderá requisitar subsídios formais aos responsáveis pela elaboração do Edital e dos anexos.

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

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

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

22. DAS DISPOSIÇÕES GERAIS

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

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

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

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

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

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

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

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

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

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

22.11. O Edital está disponibilizado, na íntegra, no endereço eletrônico https://www.gov.br/compras/pt-br/ e https://www.gov.br/mj/pt-br, e também poderá ser solicitado o acesso eletrônico externo por meio do endereço eletrônico licitacao@mj.gov.br.

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

22.12.1. ANEXO I - Termo de Referência (25023326);

22.12.1.1. ANEXO I - A - ESPECIFICAÇÕES TÉCNICAS

22.12.1.2. ANEXO I - B - PROPOSTA DE PREÇOS

22.12.1.3. ANEXO I - C - MODELO DE ORDEM DE SERVIÇO – O.S.

22.12.1.4. ANEXO I - D - MODELO DE DECLARAÇÃO DE VISTORIA

22.12.1.5. ANEXO I - E - TERMO DE CIÊNCIA

22.12.1.6. ANEXO I - F - TERMO DE COMPROMISSO

22.12.1.7. ANEXO I - G - MODELO DE DECLARAÇÃO DE RENÚNCIA À VISTORIA

22.12.1.8. ANEXO I - H - MODELO DE PLANO DE INSERÇÃO

22.12.1.9. ANEXO I - I - MODELO DE PLANO DE FISCALIZAÇÃO

22.12.1.10. ANEXO I - J - MODELO DE DECLARAÇÃO DE SUSTENTABILIDADE AMBIENTAL

22.12.2. ANEXO II - Estudo Técnico Preliminar (24328235);

22.12.3. ANEXO III – Minuta de Termo de Contrato (24740533);

22.12.4. ANEXO IV - Valores Máximos Admissíveis (25110173)

assinatura eletrônica novembro de 2020.

A autenticidade do documento pode ser conferida no site http://sei.autentica.mj.gov.br informando o código verificador **25359252** e o código CRC **546D1E71**
O trâmite deste documento pode ser acompanhado pelo site http://www.justica.gov.br/acesso-a-sistemas/protocolo e tem validade de prova de registro de protocolo no Ministério da Justiça e Segurança Pública.

Referência: Processo nº 08006.000158/2023-36 SEI nº 25359252

Ministério da Justiça e Segurança Pública
Secretaria-Executiva
Coordenação de Infraestrutura de TIC

HISTÓRICO DE REVISÕES

Data	Versão	Descrição	Autor
11/05/2023	1.0	Finalização da primeira versão do documento	Equipe de Planejamento da Contratação
23/05/2023	2.0	Após revisão da Coordenação - Geral de Licitações e Contratos	Equipe de Planejamento da Contratação
04/08/2023	3.0	Após revisão da Consultoria Jurídica - CONJUR	Equipe de Planejamento da Contratação

TERMO DE REFERÊNCIA OU PROJETO BÁSICO
PROCESSO Nº 08006.000158/2023-36

Referência: Arts. 12 a 24 IN SGD/ME Nº 01/2019

1. OBJETO DA CONTRATAÇÃO

1.1. Contratação de solução de firewall contemplando serviços de instalação e suporte técnico com garantia pelo período de 60 meses, com vistas a atender às necessidades do Ministério da Justiça e Segurança Pública - MJSP.

2. DESCRIÇÃO DA SOLUÇÃO DE TIC

2.1. **Bens e serviços que compõem a solução**

Grupo	Item	Descrição do Bem ou Serviço	Código CATMAT/CATSER	Quantidade	Métrica ou Unidade
1	1	FIREWALL TIPO I - APPLIANCE FÍSICO	484747	04	Unidade
	2	FIREWALL TIPO II - APPLIANCE FÍSICO	484747	05	Unidade
	3	APPLIANCE FÍSICO PARA ANÁLISE DO TRÁFEGO DE DADOS	481647	01	Unidade
	4	APPLIANCE VIRTUAL DE GERENCIAMENTO CENTRALIZADO	27472	01	Unidade

Tabela 1 - Relação de itens

2.2. A presente contratação é formada por um único grupo (Grupo 1) com 4 (quatro) itens.

2.3. O Grupo 1 terá contrato de 12 (doze) meses, tendo garantia de 60 meses contados a partir do **aceite definitivo da solução (Termo de Recebimento Definitivo (TRD))** e com pagamento único.

2.4. As especificações técnicas serão detalhadas no ANEXO I - A - ESPECIFICAÇÕES TÉCNICAS.

3. FUNDAMENTAÇÃO LEGAL

3.1. A presente contratação está fundamentada nas seguintes normas e leis, dentre outras fontes:

3.1.1. Lei nº 8.666/93 e suas alterações posteriores - Licitações e Contratos da Administração Pública.

3.1.2. Lei nº 10.520/2002: Institui, no âmbito da União, Estados, Distrito Federal e Municípios, nos termos do art. 37, inciso XXI, da Constituição Federal, modalidade de licitação denominada pregão, para aquisição de bens e serviços comuns, e dá outras providências.

3.1.3. Decreto-Lei nº. 200/1967: Dispõe sobre a organização da Administração Federal, estabelece diretrizes para a Reforma Administrativa e dá outras providências.

3.1.4. 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.

3.1.5. 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.

3.1.6. 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.

3.1.7. Instrução Normativa SEGES/ME nº 73, de 5 de agosto de 2020: Dispõe sobre o procedimento administrativo para a realização de pesquisa de preços para a aquisição de bens e contratação de serviços em geral, no âmbito da administração pública federal direta, autárquica e fundacional.

3.1.8. Instrução normativa SGD/ME nº 01, de 4 de abril de 2019 e seus Anexos: 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.

3.1.9. Instrução Normativa nº 03/2018 - Regras de funcionamento do SICAF.

3.1.10. Instrução Normativa SLTI/MP nº 01/2010: 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.

3.1.11. Guias, manuais e modelos publicados pelo Órgão Central do SISP (art. 8º, §2, da IN SGD/ME nº 01/2019).

4. JUSTIFICATIVA PARA A CONTRATAÇÃO

4.1. *Contextualização e Justificativa da Contratação*

4.1.1. A Subsecretaria de Tecnologia da Informação e Comunicação do Ministério da Justiça e Segurança Pública (STIC/MJSP) passou por mudanças estruturais e regimentais importantes de 2019 a 2023, ocasionando um crescimento nas demandas das áreas de negócio por soluções de tecnologia da informação e comunicação, tornando-se necessária a busca por soluções que proporcionem uma infraestrutura tecnológica escalável e atualizada com o mercado.

4.1.2. A busca por evolução dos serviços de informática vem resultando em mudanças no perfil de tráfego de suas aplicações internas e externas, exigindo uma revisão da arquitetura de ativos de segurança atualmente em funcionamento, requerendo dos equipamentos maiores taxas de transmissão e maior poder de processamento.

4.1.3. Tal implementação requer uma maior interatividade da parte de procedimentos de configuração, desempenho e qualidade, bem como a total interoperabilidade, visando uniformização dos recursos como um todo.

4.1.4. Nesse sentido, a adoção de tecnologias modernas e inovadoras, como solução de Firewall de alto desempenho, deixaram de ser uma tendência e passaram a ser uma realidade na Administração Pública Federal – APF, que deve estar alinhada às modernas e eficientes práticas do mercado.

4.1.5. Os Firewalls possuem funções fundamentais em uma rede de TIC, podendo evitar que pacotes indesejados e prejudiciais tenham acesso à rede interna e, portanto, às informações e recursos em posse da mesma. Assim também, os "filtros" implementados por esses equipamentos evitam que *hosts* internos tenham acesso a domínios e informações que não condizem com a política de segurança da rede.

4.1.6. Além disso, é um dos mecanismo de segurança utilizados para proteger a rede computacional contra acessos indevidos, através da identificação, análise, bloqueio, isolamento e tratamento das rotas de rede utilizadas pelo usuários e pelos sistemas computacionais sob responsabilidade do MJSP, além do gerenciamento das atividades que envolvam ameaças relacionadas à configuração de rotas. Com isso, diminui-se o risco de acessos indevidos aos sistemas do MJSP enquanto o desempenho geral da rede é otimizado através do gerenciamento mais eficaz do roteamento dos ativos de TI do órgão.

4.1.7. Existem muitas vantagens em manter uma solução de *Firewall* com poder de processamento robusto, com altas taxas de transmissão e em um ambiente de TIC totalmente coberto com suporte e garantia, cabendo destaque para os listados abaixo:

a) Manutenção da integridade dos dados;

b) Maior controle do acesso às informações;

c) Manutenção da integridade da rede;

d) Melhora a segurança da rede;

e) Proteção contra malwares;

4.1.8. Além dessas vantagens consideradas essenciais, deve-se observar os riscos que o MJSP correrá caso opte em não utilizar uma solução de *Firewall*:

a) **Comprometimento dos dados** - trata-se de um incidente de segurança em que dados pessoais e/ou informações privadas e sigilosas podem ser expostos publicamente ou a terceiros sem autorização.

b) **Sujeição aos ataques dos cibercriminosos** - atualmente, com o alto fluxo de informação, gera-se um aumento significativo de ataques, espionagem e roubo de dados cibernéticos. Ou seja, a maior conectividade trouxe com ela a maior exposição a risco e Malwares diversos, completamente dispersos pela rede ou tecnicamente planejados para atacar órgãos específicos.

c) **Comprometimento da integridade da rede** - acessos indevidos à rede podem ocorrer, afetando assim a garantia da integridade dos dados e informações essenciais.

d) **Descontrole da autorização de acesso às informações** - As políticas de segurança coincidem com as regras aplicadas no firewall, ditam as regras de permissões e proibições de acesso que um *firewall* deve implementar.

4.1.9. Em virtude dos aspectos abordados, é de fundamental importância a abordagem e entendimento da arquitetura atual da solução de firewall e sua topologia aplicada à rede do MJSP, assim como o entendimento do escopo dos projetos de segurança em infraestrutura realizados ao longo dos anos.

4.2. **Atual arquitetura da solução de firewall na topologia de redes**

4.2.1. Na atual conjuntura, a estrutura de Tecnologia da Informação do Ministério vem passando por mudanças de disposição física em suas unidades, o que tem provocado a necessidade de aquisição de equipamentos, processos de automatização e alta disponibilidade que suportem este dinamismo.

4.2.2. A atual plataforma de ativos de rede do MJSP, formada pela rede do núcleo central, é composta por três camadas:

- Camada Central;
- Camada de Distribuição e
- Camada de Acesso.

4.2.3. A Camada Central abriga os switches do tipo core, que são equipamentos de alto desempenho, os quais devem ser robustos para suportarem grande tráfego de pacotes. A arquitetura desta camada deve proporcionar alto grau de disponibilidade, capacidade, redundância e resiliência.

4.2.4. A Camada de Distribuição é responsável pela interconexão entre a camada Central e de Acesso, sendo responsável pela concentração dos pacotes de dados oriundos da Camada de Acesso para encaminhamento à Camada Central. A Camada de Distribuição controla o fluxo do tráfego da rede usando políticas e determina domínios de broadcast, realizando funções de roteamento entre VLANs, além de conectar os pontos de acesso da rede sem fio (APs).

4.2.5. A Camada de Acesso é a camada de switches mais próxima das máquinas dos usuários, sendo que os equipamentos ativos desta camada captam os pacotes de dados oriundos das máquinas de usuários, impressoras, telefones VoIP e outros equipamentos da ponta, e os encaminham à Camada de Distribuição. O principal propósito da camada de acesso é fornecer um meio de conectar dispositivos à rede e controlar quais têm permissão de comunicação na rede.

4.2.6. Dentre os projetos de aquisição de equipamentos para essas camadas, o de reestruturação e modernização de ativos de rede da Camada Central (Core), se relaciona diretamente com funcionamento da solução de firewall, pois trouxe inovação para os Data Centers do MJSP (Primário e Secundário), e ainda teve por objetivo a inserção da estrutura *Spine-Leaf,* a qual consiste em uma espinha dorsal formada pelo SPINE e os LEAFs, que servem de entrada dos diversos subsistemas de rede. A arquitetura proposta forma um único *Fabric,* que funciona de forma redundante em camada 3 (três) e com a utilização de roteamento dinâmico interno ao Data Center.

4.2.7. A estrutura de firewall do Ministério é composta pelos equipamentos instalados nos 2 (dois) Data Centers do MJSP, além de equipamentos localizados nas 05 (cinco) Penitenciárias Federais (Catanduvas (PR), Campo Grande (MS), Mossoró (RN), Porto Velho (RO) e Brasília (DF)). Importante salientar, que, a topologia de redes difere das implantada no MJSP e CICCN, tendo em vista que a rede de uma Penitenciária federal é menos complexa, utilizando somente switches de distribuição para ligar os equipamentos de firewall. Então, em cada Penitenciária foi instalado um Appliance Físico, contemplando assim 5 "caixas" desses ativos no total.

4.2.8. A tabela abaixo apresenta o quantitativo atual de equipamentos que atende a todo o MJSP (Data Centers Primário, Secundário e Penitenciárias):

Solução de Firewall Atual		
Descrição	**Tipo**	**Quantidade**
Appliance de Firewall para uso nos Datacenters do MJSP	Unidade	04
Appliance de Firewall para uso nas Penitenciárias Federais	Unidade	05
Appliance para análise do tráfego de dados para uso nos Datacenters do MJSP	Unidade	01
Appliance de gerenciamento centralizado para uso nos Datacenters do MJSP	Unidade	01

Tabela 2 - Equipamentos atuais

4.2.9. Esses equipamentos de Firewall foram adquiridos por meio do

processo 08006.001190/2016-18, tendo o suporte e garantia prazos de expiração em 28/06/2023, o que requer atenção especial com a elaboração de pesquisas e análises de soluções voltadas ao atendimento da necessidade.

4.2.10. Nesse sentido, um fator importante em adquirir uma solução robusta e com alto desempenho, é a necessidade observada de utilizar links de internet redundantes em algumas unidades do MJSP, destacando-se as Penitenciárias Federais.

4.2.11. A interligação das Penitenciárias Federais à infraestrutura do Ministério é realizada pela tecnologia MPLS (Multiprotocol Label Switching, ou "Comutação de Rótulos Multiprotocolo") que é uma tecnologia de rede usada, em geral, para conectar suas unidades remotas, ou por provedores de internet para a segmentação de tráfego de layer 2 e layer 3. A empresa contratada para fornecimento do MPLS é a Telebrás, sendo que o contrato prevê dupla abordagem de links, ou seja, um por fibra óptica outro por meio sem fio. Apesar disso, diversos incidentes na rede foram registrados nos anos de 2022 e agora em 2023, ocasionando que sistemas importantes para a segurança pública ficassem indisponíveis.

4.2.12. Sendo assim, foram 480 (quatrocentos e oitenta) incidentes relacionados à solução de internet/MPLS da Telebrás, contando todas as unidades do MJSP. Esta situação de recorrentes indisponibilidades traz transtornos e perdas consideradas incalculáveis, levando em conta todos os sistemas e serviços que foram afetados e deixados de ser prestados à população. Cabe destacar que muitos dos incidentes ocorrem em decorrência da Telebrás terceirizar a última milha do link, tendo em vista a capilaridade da operadora não chegar em algumas localidades.

4.2.13. Dito isso, a equipe técnica está analisando a possibilidade de implementação, em um futuro próximo, da tecnologia SD-WAN (WAN definida por software), com o objetivo de aumentar a disponibilidade, a velocidade do link e diminuir os custos com links MPLS. Vários benefícios podem ser elencados da SD-WAN em comparação com o MPLS, como por exemplo:

a) As **SD-WANs não dependem de hardware especializado** As MPLS requerem a configuração de roteadores especializados para encaminhar pacotes corretamente. As SD-WANs podem ser executadas usando qualquer hardware de rede.

b) As **SD-WANs não têm limites de largura de banda inerentes** Como as conexões MPLS são mais ou menos definidas (a menos que sejam reconfiguradas), há um limite rígido sobre quanta capacidade pode ser provisionada em uma conexão MPLS de uma só vez . As conexões SD-WAN podem adicionar capacidade conforme necessário, combinando várias conexões e aproveitando a conectividade mais rápida disponível.

c) As **SD-WANs são independentes do provedor de serviços** As MPLS exigem que as organizações usem a mesma operadora em todos os sites conectados por WAN porque as conexões MPLS precisam ser configuradas em roteadores físicos na rede adjacente. As conexões SD-WAN são executadas pela internet comum; qualquer provedor pode ser compatível com uma conexão SD-WAN.

d) O **roteamento SD-WAN é mais flexível** A SD-WAN pode aproveitar várias opções de conectividade, incluindo conexões de internet de banda larga, linhas privadas e 5G. Ela pode direcionar o tráfego e o failover entre todas as opções de conectividade disponíveis. Os serviços de MPLS normalmente exigem conexões de linha privada dedicadas do provedor de serviços.

e) As **SD-WANs se integram mais facilmente com a nuvem** Conectar-se à nuvem via MPLS é um serviço especializado oferecido por alguns provedores de serviços MPLS para alguns provedores de nuvem. Com a MPLS, a conexão com a nuvem requer a construção de uma rota direta para a infraestrutura desse provedor de nuvem.

4.2.14. Diante dos motivos expostos e das necessidades apresentadas, se faz necessário a contratação de solução de firewall contemplando serviços de instalação e suporte técnico com garantia pelo período de 60 meses, com vistas a atender às necessidades do Ministério da Justiça e Segurança Pública - MJSP.

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

ALINHAMENTO AOS PLANOS ESTRATÉGICOS	
ID	**Objetivos Estratégicos**
OE11	Fortalecer e ampliar a estrutura e os serviços de TIC (Finalidade: Avaliar se os serviços de TIC considerados estratégicos estão em operação conforme acordado, quais sejam: 1) E-mail; 2) SEI; 3) mj.gov.br; 4) Rede Local; e 5) Acesso à Internet.);

ALINHAMENTO AO PDTIC 2021-2023			
ID	**Ação do PDTIC**	**ID**	**Meta do PDTIC associada**
A0454	Contratação de Expansão e Atualização Tecnológica de Ferramenta de Firewall.	N4343	Expansão e Atualização Tecnológica de

	[illegible]		Ferramenta de Firewall

ALINHAMENTO AO PCA 2023	
Item	**Descrição**
28	Contratação de suporte técnico e atualização tecnológica da ferramenta de Firewall

4.4. ***Estimativa da demanda***

4.4.1. Os quantitativos foram definidos considerando as necessidades atuais e a médio prazo do Datacenter MJSP (SEDE), CICCN-DF e das Penitenciárias Federais, levando em conta funcionalidades e características de escalabilidade e desempenho.

Item	Descrição	Quantidade Total	Quantidade por localidade	Local de Instalação
1	Appliance de Firewall para uso nos Datacenters do MJSP	04	02	Datacenter Primário - SEDE do MJSP
			02	Datacenter Secundário - CICCN
2	Appliance de Firewall para uso nas Penitenciárias Federais	05	01	Penitenciária Federal Catanduvas (PR)
			01	Penitenciária Federal Campo Grande (MS)
			01	Penitenciária Federal Mossoró (RN)
			01	Penitenciária Federal Porto Velho (RO)
			01	Penitenciária Federal Brasília (DF)
3	Appliance para análise do tráfego de dados	01	01	Datacenter Primário - SEDE do MJSP
4	Appliance de gerenciamento centralizado	01	01	Datacenter Primário - SEDE do MJSP

Tabela 3 - Equipamentos por localidade

4.4.2. A Figura 1 demonstra a topologia de firewall implementada junto aos equipamentos de redes presentes no Datacenter MJSP (SEDE) e CICCN-DF:

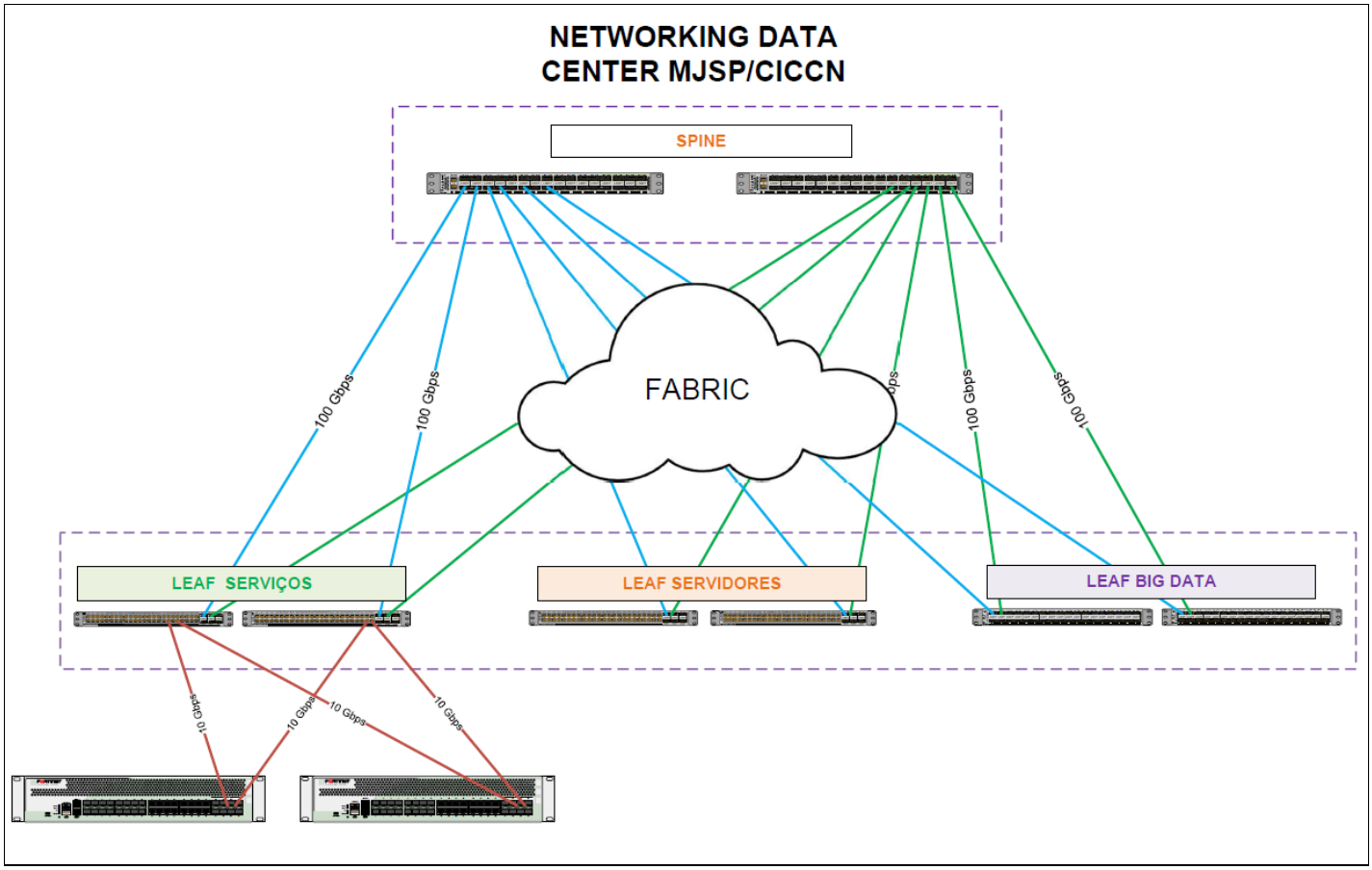

Figura 1 – Topologia MJSP e CICCN

4.4.3. De um modo geral, a topologia física não será alterada, permanecendo a nova solução também conectada aos switches Leafs de Serviços, proporcionando a padronização de topologia física, mitigando os riscos de uma parada da rede e obtendo a possibilidade de uma futura expansão tecnológica.

4.4.4. Destaca-se na nova solução, a importância em adquirir Firewalls considerados de Última Geração (Firewalls Next Generation - NGFW, que faz inspeção profunda de pacote que vai além da inspeção e do bloqueio de portas/protocolos para adicionar uma inspeção ao nível da aplicação, uma prevenção de intrusões e obter informações fora da firewall), com a implementação da tecnologia de SD-WAN, sendo listado abaixo as principais características e vantagens, como:

4.4.4.1. Os NGFWs são a evolução e ampliação das capacidades dos firewalls tradicionais. Inspeciona os dados em um nível mais profundo para identificar e bloquear ameaças que podem estar ocultas no tráfego normal.

4.4.4.2. Os NGFWs usam inspeção profunda de pacotes (DPI), ou seja, inspeciona o corpo de cada pacote, não apenas o cabeçalho, verificando os corpos dos pacotes em busca de assinaturas de malware e de outras ameaças em potencial. Durante essa inspeção, o conteúdo de cada pacote é comparado com o conteúdo de ataques maliciosos conhecidos.

4.4.4.3. Faz o controle do aplicativo e application awareness, isto é, bloqueiam ou autorizam pacotes com base em para qual aplicativo eles estão sendo encaminhados. Os NGFWs fazem isso analisando o tráfego na camada 7, a camada de aplicativos.

4.4.4.4. Maior capacidade em prevenção de intrusões (IPSs), utilizando métodos de detecção de assinaturas (verifica as informações dentro dos pacotes recebidos e as compara com ameaças conhecidas), detecção de anomalias estatísticas (verifica o tráfego para detectar mudanças incomuns de comportamento, em comparação com uma base de referência) e detecção de análise de protocolos stateful (semelhante à detecção de anomalias estatísticas, mas com foco nos protocolos de rede em uso, comparando-os com o uso normal dos protocolos).

4.4.4.5. Inteligência contra ameaças, ou seja, são capazes de receber e agir com base em informações de inteligência contra ameaças provenientes de fontes externas, mantendo a eficácia da detecção de assinaturas do provedor ao fornecer as assinaturas de malware mais recentes, também fornecendo informações sobre a reputação de IP. "A reputação de IP" identifica os endereços de IP de onde os ataques (especialmente ataques de bot).

4.4.4.6. Os NGFWs podem processar o tráfego em várias camadas no modelo OSI, não apenas nas camadas 3 (camada de rede) e 4 (a camada de transporte). Os NGFWs podem analisar o tráfego na camada 7 HTTP e identificar quais aplicativos estão sendo utilizados.

4.4.5. A Figura 2 demonstra a topologia de firewall implementada nas Penitenciárias junto aos principais equipamentos de redes presentes nas localidades:

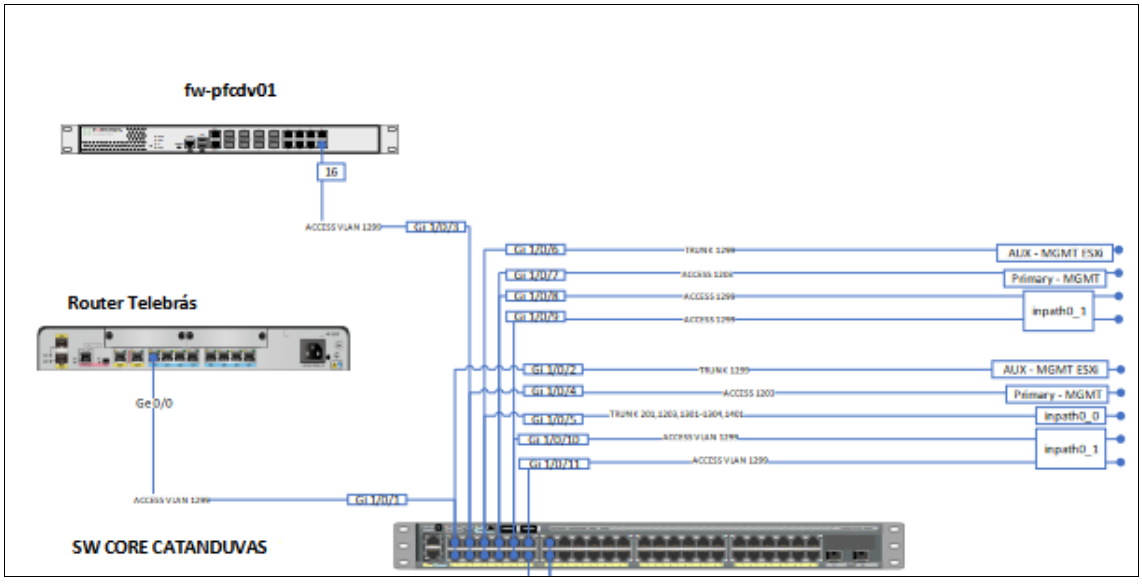

Figura 2 – Topologia de Firewall das Penitenciárias

4.4.6. A topologia de firewall implementada nas penitenciárias segue um padrão, utilizando-se de um appliance físico (de menor processamento e capacidade devido à quantidade de usuários na rede) ligado diretamente os Switch Core juntamente com outros serviços. Esta topologia física também será mantida, substituindo os atuais equipamentos por outros mais modernos, visando a utilização mais predominante da tecnologia de SD-WAN.

4.4.7. A SD-WAN pode ser entendida como uma WAN definida por software, ou seja, uma tecnologia de implantações de redes WAN baseadas em software via internet, oferecendo valor de utilidade significativo para os órgãos públicos e unidades distribuídas em termos de agilidade e capacidade de alavancar a economia da largura de banda da Internet.

4.4.8. A SD-WAN garante desempenho e resiliência consistentes de aplicativos, automatiza o direcionamento de tráfego de maneira orientada por aplicativos com base nos propósitos do MJSP, melhora a segurança da rede e simplifica a arquitetura WAN.

4.4.9. Além disso, a implantação rápida de serviços de WAN (como largura de banda e firewall) é menos complexa e muitas vezes sem a necessidade de enviar pessoal de TI no local, pois tem o gerenciamento centralizado (Centralizado no Datacenter Primário do MJSP). A largura de banda pode ser facilmente adicionada (com circuitos adicionais) ou reduzida à medida que os requisitos de negócios evoluem. A virtualização e a configuração automatizada de políticas de negócios e de segurança permitem serviços de direcionamento de tráfego automatizados, controlados centralmente com poucos cliques.

4.4.10. Sendo assim, adquirir uma nova solução de firewall (Firewall Next Generation (NGFW)), com implementação da solução de SD-WAN, vai otimizar implantações de links de dados e VPN nas unidades do MJSP, principalmente nas Penitenciárias Federais, e apresentam ainda outras funcionalidades, como:

4.4.10.1. Automatização do caminho das WANs e possibilidade de automação do controle do caminho baseado em políticas de negócios e aplicações;

4.4.10.2. Definição dinâmica de caminhos e métricas, baseadas na visibilidade em tempo real, sobre o destino desejado da aplicação, seu desempenho, a experiência do usuário final da aplicação e a qualidade das redes disponíveis no caminho;

4.4.10.3. Automação alinhada aos negócios e baseada em políticas para definir a qualidade do serviço e privilégios de acesso para todas as aplicações e todos os usuários, em combinação com a escolha automatizada do caminho;

4.4.10.4. Gerenciamento centralizado, com uma visualização integrada e topologia "full mesh" da estrutura de conectividade entre o datacenter e Unidades, tudo em uma plataforma de gerenciamento integrada e centralizada, que possibilite automatizar a implantação da VPN, com escolha do melhor link de dados e melhor caminho para a VPN, possibilitar múltiplas VPN's e continuidade do serviço de VPN em caso de falhas ou degradação de um dos links de dados, melhorando a conectividade entre redes das Unidades e a Sede;

4.4.10.5. Monitoramento de desempenho integrado de ponta a ponta e otimização da WAN de forma segura.

4.4.10.6. Suporte a VLANs, capacidade de segregar tráfego pelas WANs e entre redes LANs sem fio, e com fio e capacidade de segregar tráfego com base nas aplicações da camada 7;

4.4.10.7. Capacidade de aplicar regras de controle de acesso, desempenho e segurança com base na política definida no console de gerenciamento central;

4.4.10.8. Implantação sem configurações na unidade remota " zero-touch" via ativação automatizada e segura de todos os gateways de WAN.

4.4.11. Em virtude dos fatos mencionados, a solução de contratação de toda uma nova solução de firewall contemplando serviços de instalação e suporte técnico com garantia pelo período de 60 meses encontra-se detalhada com os devidos quantitativos.

4.5. ***Parcelamento da Solução de TIC***

4.5.1. A licitação será realizada na modalidade pregão eletrônico, com julgamento pelo critério de **MENOR PREÇO POR GRUPO** atendidas as especificações e características técnicas exigidas no presente Termo de Referência.

4.5.2. A presente contratação é formada por um único grupo (Grupo 1).

4.5.2.1. O Grupo 1 possui a quantidade de 4 (quatro) itens, sendo tecnicamente inviável o desmembramento do grupo em itens isolados em virtude da complexidade e riscos envolvidos na definição e integração de todos os ativos de firewall, serviços de instalação e manutenção necessários para prover, por completo, o perfeito funcionamento e compatibilidade dos equipamentos.

4.5.2.2. Para a presente contratação, devido à complexidade dos equipamentos e serviços envolvidos, está sendo considerado que o Grupo 1 deverá ser adjudicado por valor global, não sendo tecnicamente viável o desmembramento do Grupo 1 em itens isolados.

4.5.2.3. Devido à estrutura comum de integração das soluções ao contrato, os fabricantes da solução concedem condições diferenciadas devido ao quantitativo proposto e à estruturação do parque computacional considerados requisitos fundamentais e essenciais ao projeto. Com isso, a divisão vai de encontro ao que a Lei nº 8.666, de 1993, que descreve em seu art. 23 §1º, por não permitir a administração pública obter valores menores devido a economia de escala e à viabilidade técnica da solução:

> *"§ 1o As obras, serviços e compras efetuadas pela Administração serão divididas em tantas parcelas quantas se comprovarem técnica e economicamente viáveis, procedendo-se à licitação com vistas ao melhor aproveitamento dos recursos disponíveis no mercado e à ampliação da competitividade sem perda da economia de escala."*

4.5.2.4. A contratação da solução em itens isolados, apesar da hipótese de ampliação de

empresas participantes, não implicará em ganho para a administração pública pelo aproveitamento dos recursos disponíveis no mercado, haja vista que a forma de fornecimento dos equipamentos e licenciamento de garantia não atingem o mesmo nível de desconto quando adquiridos em pequena escala e não compõem uma solução adequada para atendimento das necessidades técnicas do Ministério.

4.5.2.5. Além dos benefícios elencados pela modalidade de contratação com 1 (um) Grupo, citam-se as seguintes vantagens:

a) Maior nível de controle pela Administração na execução dos serviços, pelo fato da existência de uma quantidade mínima de softwares de gerenciamento;

b) Maior interação entre as diferentes fases da implantação/implementação;

c) Redução de custos no que se refere ao Custo Total de Propriedade – TCO, considerando que não seria necessário adequação de hardwares e softwares dos sistemas de gerenciamento da solução para cada um dos itens licitados;

d) Maior facilidade no cumprimento do cronograma preestabelecido;

e) Diminuição da quantidade de servidores públicos a serem alocados para atividades de fiscalização e gestão do contrato, tendo em vista que cada equipe é composta por no mínimo 4 servidores (gestor, fiscal técnico, fiscal requisitante e fiscal administrativo), exigindo a alocação de recursos humanos para composição de equipes de gestão e fiscalização em função da celebração de inúmeros contratos para o mesmo objeto e, considerando o cenário atual do Ministério da Justiça e Segurança Pública, no qual há notória insuficiência de força trabalho, tal estratégia demonstra-se inviável, corroborando para a realização do certame em somente 1 (um) Grupo.

f) Na observância dos prazos, concentração da responsabilidade pela execução em uma equipe de gestão e fiscalização;

g) Concentração da garantia dos resultados.

4.5.2.6. Diante o exposto, devido à complexidade do objeto dessa licitação e suas peculiaridades técnicas (coesão e integração), é tecnicamente inviável o desmembramento por itens separados, além de fugir às melhores práticas das contratações analisadas no âmbito da Administração Pública.

4.6. Justificativa para Não Participação de Consórcios e Cooperativas

4.6.1. **Não será permitida a participação de empresas que estiverem reunidas em consórcio**, **assim como não será permitida a participação de cooperativas,** qualquer que seja sua forma de constituição, dadas as características específicas da contratação da solução a ser fornecida, uma vez que, dadas as características específicas da contratação, que não pressupõem multiplicidade de atividades empresariais distintas (heterogeneidade de atividades empresariais). Com vistas a subsidiar o entendimento a respeito da participação de consórcios em licitações públicas, transcrevemos, abaixo, comentário do Professor Marçal Justen Filho sobre o assunto:

> *...A complexidade dos objetos licitados determina a natureza do consórcio. Usualmente, há consórcios heterogêneos quando a execução do objeto pressupõe multiplicidade de atividades empresariais distintas. Isso se passa especialmente no tocante a concessões de serviço público. Nesses casos, a ausência de permissão de consórcios produziria enormes dificuldades para participação no certame. Configura-se hipótese em que admitir participação de consórcios é imprescindível, sob pena de inviabilizar a competição. (Justen Filho, Marçal, Comentários à lei de licitações e contratos administrativos. 11ª ed. São Paulo: Dialética,2005. p. 360).*

4.6.2. Desta forma, resta claro que a participação de consórcios em certames licitatórios somente se torna "obrigatória" quando o objeto a ser licitado pressuponha heterogeneidade de atividades empresariais, sendo que, sua não inclusão, resultaria em restrição da competitividade. Assim, a Administração Pública ao vedar a participação de consórcio procura manter a unidade do sistema, eis que o Termo de Referência, da forma como foi concebido demonstra a existência de uma unidade conceitual que perpassa todo o projeto. Tal integração de conceitos se verifica não só entre suas etapas, como também nos serviços previstos em cada etapa. Isto porque cada serviço solicitado representa uma preparação para que o serviço subsequente possa ser compreendido e elaborado. Vale dizer que somente a empresa que estiver envolvida e for responsável pela totalidade do objeto será conhecedora, de forma suficiente, de todas as questões pertinentes, estando apta a apresentar os serviços de forma encadeada. A opção pela participação ou não de empresas em consórcios encontra-se na esfera da discricionariedade administrativa, a qual contempla o exame da conveniência e oportunidade do ato administrativo. Se o ato é vinculado, é porque o legislador pré-estabeleceu o que não ocorreu no caso presente. No caso em questão, a lei não estabelece disposição expressa exigindo a admissão de consórcios, mas deixa ao administrador a possibilidade de verificar as hipóteses em que este seria admissível, o que se depreende do art. 33, caput, da Lei nº. 8.666/93: "Quando permitida na licitação a participação de empresas em consórcio (...)".

4.7. *Resultados e Benefícios a Serem Alcançados*

4.7.1. Reestruturar e modernizar a arquitetura de firewall do Ministério, provendo aquisição de equipamentos robustos e confiáveis.

4.7.2. Suportar o aumento no número de usuários e prestação de serviços a estes de maneira rápida, segura e eficaz.

4.7.3. Suportar a crescente demanda por conectividade de rede, internet e acesso a sistemas internos que estão hospedados em nuvem.

4.7.4. Garantir a continuidade dos negócios do MJSP por meio de melhorias, apoio técnico e manutenções da solução a ser adquirida.

4.7.5. Prover a mitigação de impactos para as áreas de negócios decorrentes de problemas no funcionamento dos equipamentos de segurança.

4.7.6. Aumentar a segurança por meio da ativação novas funcionalidade técnicas à nova solução.

4.7.7. Prover solução de firewall eficiente com a atualização dos ativos deste Ministério.

4.7.8. Manter a integridade da rede em conjunto com a integridade dos dados.

4.7.9. Permitir gestão centralizada de todos dos dispositivos de segurança e borda da rede das agilizando a recuperação de desastres (disaster recovery).

4.7.10. Assegurar estabilidade da rede e dos sistemas frente à ampliação da infraestrutura de rede existente nas Unidades do MJSP.

4.7.11. Manter a compatibilidade tecnológica do parque de ativos de segurança em funcionamento na rede do Ministério.

4.7.12. Prover maior proteção contra malwares;

4.7.13. Atender prontamente ao aumento de novos serviços online e em nuvem prestados pelo MJSP e na melhoria do acesso à Internet nas Unidades Penitenciárias.

4.7.14. Garantir a continuidade da conexão da VPN entre o MJSP e diversas localidades e serviços.

4.7.15. Assegurar disponibilidade entre links de internet em unidades do MJSP.

5. ESPECIFICAÇÃO DOS REQUISITOS DA CONTRATAÇÃO

5.1. Conforme previsto no Art. 11, Inciso I da IN 01/2019 SGD/ME, o Estudo Técnico Preliminar da Contratação definiu e especificou as necessidades de negócio e tecnológicas, e os requisitos necessários e suficientes à escolha da solução de TIC, contendo de forma detalhada, motivada e justificada, inclusive quanto à forma de cálculo, o quantitativo de bens e serviços necessários para a sua composição.

5.2. *Requisitos de Negócio*

5.2.1. Auxiliar de forma tecnológica na Redução de homicídios e outros crimes violentos.

5.2.2. Fortalecer o enfrentamento à criminalidade, com enfoque em organizações criminosas, corrupção, lavagem de dinheiro e atuação na faixa de fronteira.

5.2.3. Promover o acesso à justiça e proteger os direitos do cidadão.

5.2.4. Aperfeiçoar a coordenação estratégica e a integração dos órgãos de segurança pública.

5.2.5. Aperfeiçoar a gestão do sistema prisional.

5.2.6. Promover a gestão e a alienação do produto de crimes de tráfico de drogas.

5.2.7. Ampliar a escala e a efetividade das ações de defesa da concorrência e do consumidor.

5.2.8. Aprimorar mecanismos de gestão e de disseminação do conhecimento com foco no público externo.

5.2.9. Aprimorar e integrar a gestão e a governança institucional.

5.3. *Requisitos de Capacitação*

5.3.1. **Grupo 1**

5.3.1.1. Após a entrega da solução completa, deverá ser realizado treinamento para a equipe técnica da STIC, para até 5 (cinco) servidores.

5.3.1.2. O treinamento deve garantir que toda a informação gerada durante os processos de instalação e migração seja integral e formalmente apresentada à equipe da CONTRATADA, por meio de métodos expositivos, realização prática das atividades, apresentação de resumos, esquemas, relatórios ou qualquer outro documento que viabilize ou facilite a absorção da tecnologia do novo ambiente pela equipe da CONTRATADA;

5.3.1.3. É parte integrante do escopo do treinamento a disponibilização de toda a documentação técnica, incluindo manuais de instalação, configuração e de usuário, relativa aos componentes integrantes da solução;

5.3.1.4. A CONTRATADA deverá realizar treinamento para 1 (uma) turma com até 5 (cinco) integrantes indicados pela CONTRATANTE;

5.3.1.5. A capacitação deverá ser realizada em Brasília-DF, preferencialmente nas dependências da CONTRATANTE, por técnicos com certificação(ões) técnica(s) emitida(s) pelo(s) fabricante(s) dos equipamentos.

5.3.1.6. As especificações do treinamento são detalhadas no **ANEXO I-A - ESPECIFICAÇÕES TÉCNICAS.**

5.4. ***Requisitos Legais***

5.4.1. **Grupo 1**

5.4.1.1. A CONTRATADA deverá observar, na execução do serviço, leis, políticas, modelos ou padrões de governo e as boas práticas no tema gestão e governança de dados.

5.4.1.2. A CONTRATADA deverá observar também os seguintes ornamentos jurídicos:

5.4.1.2.1. Lei Nº 13.709, de 14 de agosto de 2018, Lei Geral de Proteção de Dados Pessoais (LGPD)- dispõe sobre o tratamento de dados pessoais, inclusive nos meios digitais, por pessoa natural ou por pessoa jurídica de direito público ou privado, com o objetivo de proteger os direitos fundamentais de liberdade e de privacidade e o livre desenvolvimento da personalidade da pessoa natural.

5.4.1.2.2. Decreto Nº 6.666, de 27 de novembro de 2008, Infraestrutura Nacional de Dados Espaciais - INDE, com o objetivo de: I - promover o adequado ordenamento na geração, no armazenamento, no acesso, no compartilhamento, na disseminação e no uso dos dados geoespaciais de origem federal, estadual, distrital e municipal, em proveito do desenvolvimento do País; II - promover a utilização, na produção dos dados geoespaciais pelos órgãos públicos das esferas federal, estadual, distrital e municipal, dos padrões e normas homologados pela Comissão Nacional de Cartografia - CONCAR; e III - evitar a duplicidade de ações e o desperdício de recursos na obtenção de dados geoespaciais pelos órgãos da administração pública, por meio da divulgação dos metadados relativos a esses dados disponíveis nas entidades e nos órgãos públicos das esferas federal, estadual, distrital e municipal.

5.4.1.2.3. Lei Nº 12.527, de 18 de novembro de 2011, regula o acesso a informações previsto no inciso XXXIII do art. 5º , no inciso II do § 3º do art. 37 e no § 2º do art. 216 da Constituição Federal; altera a Lei nº 8.112, de 11 de dezembro de 1990; revoga a Lei nº 11.111, de 5 de maio de 2005, e dispositivos da Lei nº 8.159, de 8 de janeiro de 1991; e dá outras providências.

5.4.1.2.4. Decreto Nº 7.724, de 16 de maio de 2012, regulamenta a Lei nº 12.527, de 18 de novembro de 2011, que dispõe sobre o acesso a informações previsto no inciso XXXIII do caput do art. 5º , no inciso II do § 3º do art. 37 e no § 2º do art. 216 da Constituição.

5.4.1.2.5. Decreto Nº 8.777, de 11 de maio de 2016, institui a Política de Dados Abertos do Poder Executivo Federal.

5.4.1.2.6. Instrução Normativa Nº 01, da SGD/ME, de 4 de abril de 2019, que 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.

5.4.1.2.7. Portaria do Ministério da Justiça 3.530/2013 - Política da Segurança de Informação, ou outra que venha à substituí-la.

5.5. ***Requisitos de Manutenção***

5.5.1. **Grupo 1**

5.5.1.1. Para o Grupo 1, todos os requisitos de garantia estão inseridos no **ANEXO I-A - ESPECIFICAÇÕES TÉCNICAS.**

5.6. ***Requisitos Temporais***

5.6.1. Conforme detalhado no item 8.3 do Termo de Referência.

5.7. ***Requisitos de Segurança e Privacidade***

5.7.1. Os funcionários da Contratada deverão obedecer às diretrizes, normas e procedimentos da Política de Segurança da Informação e Comunicações do Órgão, assim como:

5.7.1.1. Manter sigilo sobre todo e qualquer assunto de interesse do Órgão ou de terceiros de que tomar conhecimento em razão da execução do contrato, devendo orientar seus empregados nesse sentido.

5.7.1.2. Não veicular publicidade acerca dos serviços contratados, sem prévia autorização, por escrito, do Ministério.

5.7.1.3. Manter em caráter confidencial, mesmo após o término do prazo de vigência ou rescisão do contrato, as informações relativas à Política de Segurança adotada pelo Órgão e às configurações de hardware e de softwares decorrentes, bem como as informações relativas ao processo de instalação, configuração e adaptações de produtos, ferramentas e equipamentos da solução.

5.8. ***Requisitos Sociais, Ambientais e Culturais***

5.8.1. Conforme disposto na IN nº 01/2010 do SLTI/MPOG, sobre os critérios de sustentabilidade ambiental, os bens adquiridos deverão:

5.8.1.1. Ser constituídos, no todo ou em parte, por material reciclado, atóxico, biodegradável, conforme ABNT NBR – 15448-1 e 15448-2;

5.8.1.2. Observar 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;

5.8.1.3. Ser, preferencialmente, acondicionados em embalagem individual adequada, com menor volume possível, que utilize materiais recicláveis, garantindo proteção máxima durante o transporte/armazenamento; e

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

5.8.2. A licitante deverá apresentar Declaração de Sustentabilidade Ambiental conforme modelo constante no **ANEXO I - J - MODELO DE DECLARAÇÃO DE SUSTENTABILIDADE AMBIENTAL** documento este, que deverá ser apresentado na fase de aceitação da proposta.

5.8.3. Tal exigência visa atender aos dispositivos normativos acima enumerados, bem como estabelecer que a licitante deva implementar ações ambientais por meio de treinamento de seus empregados, pela conscientização de todos os envolvidos na prestação dos serviços, bem como cumprir as ações concretas apontadas especialmente nas obrigações da CONTRATADA, que se estenderão na gestão contratual, refletindo na responsabilidade da Administração no desempenho do papel de consumidor potencial e na responsabilidade ambiental e socioambiental entre as partes.

5.9. ***Requisitos de Arquitetura Tecnológica***

5.9.1. **Grupo 1**

5.9.1.1. Todos os Requisitos de Arquitetura Tecnológica da solução de garantia dos equipamentos são detalhados no **ANEXO I-A - ESPECIFICAÇÕES TÉCNICAS.**

5.10. ***Requisitos de Projeto e de Implementação***

5.10.1. Antes do início das intervenções no ambiente, deverá ser elaborado Plano de Implantação conforme os requisitos técnicos e especificações do MJSP, para que seja aprovado pelo Órgão.

5.10.2. Todos os Requisitos de Projeto e de Implementação da solução são detalhados no **ANEXO I-A - ESPECIFICAÇÕES TÉCNICAS.**

5.11. ***Requisitos de Implantação***

5.11.1. Os serviços de implantação da solução, necessários para a operacionalização da Solução de Firewall devem ser executados pela CONTRATADA, contemplando em linhas gerais as seguintes etapas:

a) Preparo e Iniciação do Projeto;

b) Definição de Requisitos da Solução;

c) Plano e Arquitetura da Solução;

d) Configuração e Integração da Solução;

e) Migração;

f) Transferência de Conhecimento;

g) Garantia e suporte do fabricante;

5.11.1.1. Todos os Requisitos de Implantação da solução são detalhados no **ANEXO I-A - ESPECIFICAÇÕES TÉCNICAS**

5.12. **Requisitos de Garantia e Manutenção**

5.12.1. **Grupo 1**

5.12.1.1. A garantia para os equipamentos será de 60 (sessenta) meses contados a partir do **aceite definitivo da solução (Termo de Recebimento Definitivo (TRD))**

5.12.1.2. A Contratada deverá descrever, em sua proposta, os termos da garantia técnica oferecida pelo fabricante, incluindo o Part Number da garantia ofertada e fornecendo também, em momento oportuno, o número de contrato individual (em nome da CONRATANTE) junto ao fabricante;

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

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

5.12.1.5. 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.

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

5.12.1.7. Uma vez notificada, a Contratada realizará a reparação ou substituição dos bens que apresentarem vício ou defeito, utilizando a modalidade 24 (vinte e quatro) horas por dia, 7 (sete) dias por semana após a abertura do chamado, pela Contratada ou pela assistência técnica autorizada.

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

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

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

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

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

5.12.1.12.1. O equipamento substituto passará à propriedade da CONTRATANTE, devendo o mesmo ser imediatamente incluído no contrato de manutenção vigente em substituição ao equipamento danificado;

5.12.1.12.2. O equipamento substituído deverá ser devolvido ao fabricante às expensas do mesmo, em até 5 (cinco) dias úteis.

5.12.1.12.3. A CONTRATANTE deverá ter acesso direto ao centro de assistência técnica da fabricante dos equipamentos para abertura dos chamados, bem como para acompanhar e gerenciar os casos quando necessário. Esse acesso deverá ser provido 24 (vinte e quatro) horas por dia, 7 (sete) dias por semana através de login/senha individual;

5.12.1.12.4. Não será aceita garantia para reposição de equipamentos da empresa revendedora;

5.12.1.13. <u>Dos requisitos de atualização de software:</u>

5.12.1.13.1. Este serviço compreende também o acesso por parte do CONTRATANTE, às atualizações (versões e releases) de software dos equipamentos disponibilizadas pelo fabricante, com a habilidade de efetuar download de softwares do sistema operacional dos equipamentos.

5.12.1.13.2. Deverá haver garantia da atualização do sistema operacional/firmware, provendo o fornecimento de novas versões por necessidade de correção de problemas ou por implementação de novos releases;

5.12.1.14. <u>Dos requisitos de acesso à documentação:</u>

5.12.1.14.1. Este serviço compreende o acesso remoto por parte do CONTRATANTE às documentações técnicas dos equipamentos do fabricante;

5.12.1.14.2. O CONTRATANTE deverá ter acesso direto à base de dados de conhecimento do fabricante dos equipamentos que contenham especificações técnicas, informações, assistência e orientação para instalação, desinstalação, configuração e atualização de firmware e software, aplicação de correções (patches), diagnósticos, avaliações e resolução de problemas e demais atividades relacionadas à correta operação e funcionamento dos equipamentos.

5.12.2. **<u>Garantia da execução</u>**

5.12.2.1. **Grupo 1**

5.12.2.1.1. O adjudicatário prestará garantia de execução do contrato, nos moldes do art. 56 da Lei nº 8.666, de 1993, com validade durante a execução do contrato e por 90 (noventa) dias após o término da vigência contratual, em valor correspondente a **5% (cinco por cento)** do valor total do contrato.

5.12.2.2. No prazo máximo de 10 (dez) dias úteis, prorrogáveis por igual período, a critério do

contratante, contados da assinatura do contrato, a contratada deverá apresentar comprovante de prestação de garantia, podendo optar por caução em dinheiro ou títulos da dívida pública, seguro-garantia ou fiança bancária.

a) 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).

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

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

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

a) prejuízos advindos do não cumprimento do objeto do contrato e do não adimplemento das demais obrigações nele previstas;

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

c) multas moratórias e punitivas aplicadas pela Administração à contratada; e

d) obrigações trabalhistas e previdenciárias de qualquer natureza e para com o FGTS, não adimplidas pela contratada, quando couber.

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

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

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

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

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

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

5.12.2.11. 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 da Contratante, 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 "h2"do item 3.1 do Anexo VII-F da IN SEGES/MP n. 05/2017.

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

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

5.13. ***Requisitos de Experiência Profissional***

5.13.1. A qualidade dos serviços deve ser assegurada por meio da disponibilização de equipe técnica qualificada, profissional com conhecimento técnico da topologia completa de firewall e dos equipamentos que compõem a solução.

5.14. ***Requisitos de Segurança da Informação e Privacidade***

5.14.1. A CONTRATADA deverá observar as melhores práticas aplicadas:

a) À disponibilidade da solução de TIC contratada;

b) Ao vazamento de dados e fraudes digitais;

c) Ao processo de gestão de riscos de segurança da informação que envolvam a solução de TIC;

d) À rastreabilidade de forma a manter trilha de auditoria de segurança da informação;

e) À continuidade do negócio implementado pela solução;

f) À gestão e tratamento de incidentes de forma sistematizada.

6. RESPONSABILIDADES

6.1. ***Deveres e responsabilidades da CONTRATANTE***

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

6.1.2. Encaminhar formalmente a demanda por meio de Ordem de Fornecimento de Bens, de acordo com os critérios estabelecidos neste Termo de Referência;

6.1.3. Aplicar à contratada as sanções administrativas regulamentares e contratuais cabíveis, quando aplicável;

6.1.4. Liquidar o empenho e efetuar o pagamento à contratada, dentro dos prazos preestabelecidos em contrato;

6.1.5. Comunicar à contratada todas e quaisquer ocorrências relacionadas com o fornecimento da solução de TIC;

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

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

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

6.1.9. Acompanhar e fiscalizar o cumprimento das obrigações da Contratada, através de comissão/servidor especialmente designado;

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

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

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

6.1.13. Notificar a Contratada por escrito da ocorrência de eventuais imperfeições no curso da execução dos serviços, fixando prazo para a sua correção;

6.1.14. Efetuar as retenções tributárias devidas sobre o valor da Nota Fiscal/Fatura fornecida pela contratada, em conformidade com o item 6, ANEXO XI, da IN nº 05/2017;

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

6.2. ***Deveres e responsabilidades da CONTRATADA***

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

6.2.1.1. Efetuar a entrega do objeto em perfeitas condições, conforme especificações, prazo e local constantes no Edital 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;

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

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

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

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

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

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

6.2.2. Atender a todas as condições descritas no presente Termo de Referência e respectivo Contrato.

6.2.3. Entregar os ativos e disponibilizar a garantia da solução de firewall de acordo com os requisitos de quantidades, especificações técnicas e manuais de operação (quando couber).

6.2.4. Entregar os ativos e disponibilizar a garantia da solução de firewall nos prazos previstos e locais designados, conforme especificações constantes na proposta, no Edital, e seus anexos.

6.2.5. Entregar os ativos e disponibilizar a garantia da solução de firewall instalados e configurados, conforme especificações constantes na proposta, no Edital, e seus anexos.

6.2.6. Após o término da instalação e configuração da solução, realizar treinamento e garantir que toda a informação gerada durante os processos de instalação e migração seja integral e formalmente apresentada à equipe da CONTRATADA, conforme especificações constantes na proposta, no Edital, e seus anexos.

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

6.2.8. Apresentar os empregados devidamente uniformizados e identificados por meio de crachá, além de provê-los com os Equipamentos de Proteção Individual - EPI, quando for o caso;

6.2.9. Apresentar à Contratante, quando for o caso, a relação nominal dos empregados que adentrarão o órgão para a execução do serviço;

6.2.10. Responsabilizar-se por todas as obrigações trabalhistas, sociais, previdenciárias, tributárias e as demais previstas em legislação específica, cuja inadimplência não transfere responsabilidade à Contratante;

6.2.11. Instruir seus empregados quanto à necessidade de acatar as normas internas da Administração;

6.2.12. 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 sentido, a fim de evitar desvio de função;

6.2.13. Relatar à Contratante toda e qualquer irregularidade verificada no decorrer da prestação dos serviços;

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

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

6.2.16. Arcar com o ônus decorrente de eventual equívoco no dimensionamento dos quantitativos de sua proposta, devendo complementá-los, caso o previsto inicialmente em sua proposta não seja satisfatório para o atendimento ao objeto da licitação, exceto quando ocorrer algum dos eventos arrolados nos incisos do § 1º do art. 57 da Lei nº 8.666, de 1993;

6.2.17. Deter instalações, aparelhamento e pessoal técnico adequados e disponíveis para a realização do objeto da licitação.

7. MODELO DE EXECUÇÃO DO CONTRATO

7.1. *Rotinas de Execução*

7.1.1. Após a assinatura do contrato o CONTRATANTE agendará dia e hora para a reunião inicial, nos termos da Art. 31 da Instrução Normativa Nº 01, de 4 de abril de 2019.

7.1.2. Na reunião inicial a CONTRATADA deverá:

a) Apresentar o PREPOSTO nos termos dos Art. 31 da Instrução Normativa Nº 01, de 4 de abril de 2019;

b) Entregar o TERMO DE CIÊNCIA, conforme descrito no **ANEXO I - E**, devidamente assinado por todos os funcionários que atuarão diretamente na execução do serviço MJSP.

c) Entregar o TERMO DE COMPROMISSO DE MANUTENÇÃO DE SIGILO, conforme descrito no **ANEXO I - F**, devidamente assinado pelo representante legal da contratada.

d) Esclarecimentos sobre a forma de comunicação a ser adotada entre o Órgão e a CONTRATADA;

e) Esclarecimentos acerca dos níveis de serviço previstos no contrato, bem como sobre o período de adaptação e ajustes da CONTRATADA ao contrato;

f) Esclarecimentos relacionados ao funcionamento do Órgão, tais como: horário de trabalho, local disponível para a equipe da CONTRATADA, regimento interno do Órgão, forma de acesso dos colaboradores da CONTRATADA às dependências da CONTRATANTE e demais informações pertinentes;

g) Alinhamento sobre cronograma inicial e data de início das atividades do contrato;

h) Demais assuntos relevantes para o início do contrato pela empresa CONTRATADA.

7.1.3. Antes do início das intervenções no ambiente, a CONTRATADA deverá elaborar Planos de Implantações conforme os requisitos técnicos e especificações constantes no **ANEXO I-A -**

ESPECIFICAÇÕES TÉCNICAS, para que seja aprovado pelo Órgão.

7.1.4. A CONTRATADA deverá apresentar os Planos de Implantações com cronograma detalhado e todo o planejamento de execução do projeto, considerando os requisitos constantes no Termo de Referência, as boas práticas de mercado e os normativos vigentes.

7.1.5. A Equipe de Fiscalização será responsável pelo acompanhamento da execução do serviço, pelo auxílio aos profissionais da CONTRATADA e deve atuar para desimpedir ou dirimir qualquer problema que possa atrapalhar as entregas previstas.

7.1.6. A emissão da Ordem de Serviço deverá acontecer através do SEI.

7.2. ***Da Subcontratação***

7.2.1. Não será admitida a subcontratação do objeto licitatório.

7.2.2. Por se tratar de uma aquisição de equipamentos de TIC, não há necessidade de subcontratação.

7.3. **Prazos e condições**

7.3.1. Os Prazos e condições estão especificados no item 8.3.

7.3.2. **Locais da execução dos serviços**

Item	Descrição	Quantidade Total	Quantidade por localidade	Local de Instalação
1	FIREWALL TIPO I - APPLIANCE FÍSICO	04	02	Datacenter Primário - SEDE do MJSP
			02	Datacenter Secundário - CICCN
2	FIREWALL TIPO II - APPLIANCE FÍSICO	05	01	Penitenciária Federal Catanduvas (PR)
			01	Penitenciária Federal Campo Grande (MS)
			01	Penitenciária Federal Mossoró (RN)
			01	Penitenciária Federal Porto Velho (RO)
			01	Penitenciária Federal Brasília (DF)
3	APPLIANCE FÍSICO PARA ANÁLISE DO TRÁFEGO DE DADOS	01	01	Datacenter Primário - SEDE do MJSP
4	APPLIANCE VIRTUAL DE GERENCIAMENTO CENTRALIZADO	01	01	Datacenter Primário - SEDE do MJSP

Tabela 7 - Locais da execução dos serviços

7.3.3. **Transferência de conhecimento**

7.3.4. As especificações de treinamento são detalhadas no **ANEXO I-A.**

7.3.5. **Documentação mínima exigida**

7.3.6. Conforme descrito no item 7.1.2 do Termo de Referência.

7.3.7. **Mecanismos formais de comunicação**

7.3.8. A comunicação entre a CONTRATANTE e a CONTRATADA, para fins de encaminhamento de Ordens de Serviço ou outro documento, ocorrerá sempre via Preposto, ou seu substituto, designado pela CONTRATADA.

7.3.9. O MJSP utiliza como sistema oficial de processo eletrônico o Sistema Eletrônico de Informações – SEI, portanto a CONTRATADA deverá se cadastrar no sistema SEI, no endereço eletrônico https://sei.mj.gov.br/sei/controlador_externo.php?acao=usuario_externo_logar&id_orgao_acesso_externo=0, de forma que consiga assinar ou protocolar documentos.

7.3.10. Em caso de dúvidas, poderá entrar em contato com a gestão do sistema pelo e-mail **sei@mj.gov.br**.

7.3.11. A comunicação entre o CONTRATANTE e a CONTRATADA se dará preferencialmente por meio escrito, sempre que se entender necessário o registro de ocorrência relacionada a execução do objeto, nas formas da tabela abaixo:

Documento	Função	Emissor	Destinatário	Periodicidade
Ofício	Informações	Contratante/Contratada	Contratante/Contratada	Sempre que

Ofício	diversas	Contratante/Contratada	Contratante/Contratada	necessário
E-mail	Informações diversas	Contratante/Contratada	Contratante/Contratada	Sempre que necessário
Ordem de serviço	Autorização para prestação de serviço	Contratante	Contratada	Sempre que necessário
Termo de Recebimento Provisório	Recebimento provisório dos serviços	Contratante	Contratada	Sempre que necessário
Termo de Recebimento Definitivo	Recebimento definitivo dos serviços	Contratante	Contratada	Sempre que necessário
Ata de reunião	Informações diversas	Contratante/Contratada	Contratante/Contratada	Sempre que necessário

Tabela 8 - Mecanismos formais de comunicação

7.4. ***Manutenção de Sigilo e Normas de Segurança***

7.4.1. A Contratada deverá manter sigilo absoluto sobre quaisquer dados e informações contidos em quaisquer documentos e mídias, incluindo os equipamentos e seus meios de armazenamento, de que venha a ter conhecimento durante a execução dos serviços, não podendo, sob qualquer pretexto, divulgar, reproduzir ou utilizar, sob pena de lei, independentemente da classificação de sigilo conferida pelo CONTRATANTE a tais documentos, conforme previsões no **ANEXO I - F - TERMO DE COMPROMISSO.**

7.4.2. A CONTRATADA deverá credenciar junto ao MJSP todos os profissionais designados para prestar serviços nas dependências do Ministério, por meio do **ANEXO I - E - TERMO DE CIÊNCIA.**

7.4.3. A CONTRATADA deverá abster-se, qualquer que seja a hipótese, de veicular publicidade ou qualquer outra informação acerca das atividades objeto do contrato sem prévia autorização por escrito do MJSP.

7.4.4. Obedecer aos critérios, padrões, políticas, normas e procedimentos operacionais adotados ou que venham a ser adotados pelo CONTRATANTE.

8. MODELO DE GESTÃO DO CONTRATO

8.1. **Critérios de Aceitação Grupo 1**

8.1.1. A Solução será recebida provisoriamente no prazo de 5 (cinco) dias, pelo(a) responsável pelo acompanhamento e fiscalização do contrato, para efeito de posterior verificação de sua conformidade com as especificações constantes neste Termo de Referência e na proposta, devendo ser elaborado relatório circunstanciado, contendo o registro, a análise e a conclusão acerca das ocorrências na execução do contrato e demais documentos que julgarem necessários, devendo encaminhá-los ao gestor do contrato para recebimento definitivo.

8.1.2. A solução poderá ser rejeitada, no todo ou em parte, quando em desacordo com as especificações constantes neste Termo de Referência e na proposta, devendo ser corrigidos/refeitos/substituídos no prazo fixado pelo fiscal técnico do contrato, às custas da Contratada, sem prejuízo da aplicação de penalidades.

8.1.3. O prazo para entrega dos equipamentos será de 60 (sessenta) dias corridos, após o recebimento da OS/OFB pela contratada;

8.1.4. **Grupo 1**

8.1.4.1. A solução será recebida definitivamente no prazo de até 45 (quarenta e cinco) dias corridos, após a entrega dos equipamentos (item 8.1.3), completa instalação e configuração dos equipamentos e licenças em perfeito funcionamento, bem como consideradas as análises e elaboração de relatórios pela equipe de fiscalização.

8.1.5. O recebimento definitivo, ato que concretiza o ateste da execução dos serviços, será realizado pelo pelo fiscal técnico, em conjunto com o fiscal requisitante.

8.1.6. O gestor do contrato analisará os relatórios e toda documentação apresentada pela fiscalização técnica e, caso haja irregularidades que impeçam a liquidação e o pagamento da despesa, indicará as cláusulas contratuais pertinentes, solicitando à CONTRATADA, por escrito, as respectivas correções.

8.1.7. O gestor emitirá termo circunstanciado para efeito de recebimento definitivo dos serviços prestados, com base nos relatórios e documentação apresentados, e comunicará a CONTRATADA para que emita a Nota Fiscal ou Fatura com o valor exato dimensionado pela fiscalização.

8.1.8. A CONTRATADA só estará autorizada a emitir a Nota Fiscal, **após autorização formal do gestor do contrato.**

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

8.2. **Procedimentos de Teste e Inspeção**

8.2.1. O acompanhamento e a fiscalização da execução do Contrato serão realizados por servidores da CONTRATANTE, em atendimento ao disposto no Art. 67 da Lei 8.666/93, designados como Fiscais do Contrato, os quais obedecerão às disposições de normas e resoluções internas do órgão, bem como ao contido no artigo 29 da INSTRUÇÃO NORMATIVA Nº 01, DA SGD/ME, DE 4 DE ABRIL DE 2019.

8.2.2. Quaisquer exigências da fiscalização, inerentes ao objeto da licitação, deverão ser prontamente atendidas pela CONTRATADA, sem quaisquer ônus para o MJSP.

8.2.3. O MJSP designará formalmente o Gestor e os Fiscais Requisitante, Técnico e Administrativo para realizar a fiscalização contratual em todas as suas fases de acordo com o que preceitua a IN 01, DA SGD/ME com relação aos aspectos de gerenciamento do contrato.

8.2.4. Caberá à equipe de fiscalização designada rejeitar no todo ou em parte, qualquer material ou serviço que não esteja de acordo com as exigências e especificações deste termo de referência, ou aquele que não seja comprovadamente original e novo, assim considerado de primeiro uso, com defeito de fabricação ou vício de funcionamento, bem como determinar prazo para substituição do material ou serviço.

8.2.5. Os servidores designados para executarem atribuições de fiscal (is) requisitante (s), fiscal (is) técnico(s), fiscal (is) administrativo (s) e gestor (es) do Contrato, desenvolverão atividades específicas além das detalhadas a seguir:

8.2.6. Fiscal (is) Técnico (s) (Incluído pela Instrução Normativa nº 31, de 23 de março de 2021):

a) confecção e assinatura do Termo de Recebimento Provisório quando da entrega do objeto constante na Ordem de Serviço ou de Fornecimento de Bens;

b) avaliação da qualidade dos serviços realizados ou dos bens entregues e justificativas, a partir da aplicação das listas de verificação e de acordo com os critérios de aceitação definidos em contrato, em conjunto com o Fiscal Requisitante do Contrato;

c) identificação de não conformidade com os termos contratuais, em conjunto com o Fiscal Requisitante do Contrato;

d) verificação da manutenção das condições classificatórias referentes à pontuação obtida e à habilitação técnica, em conjunto com o Fiscal Administrativo do Contrato;

e) encaminhamento das demandas de correção à contratada, caso disponha de delegação de competência do Gestor do Contrato;

f) confecção e assinatura do Termo de Recebimento Definitivo, com base nas informações produzidas no recebimento provisório, na avaliação da qualidade dos serviços realizados ou dos bens entregues e na conformidade e aderência aos ternos contratuais, em conjunto com o Fiscal Requisitante do Contrato;

g) apoio ao Fiscal Requisitante do Contrato na verificação da manutenção da necessidade, economicidade e oportunidade da contratação;

h) verificação de manutenção das condições definidas nos Modelos de Execução e de Gestão do contrato, em conjunto com o Fiscal Requisitante do Contrato; e

i) apoio ao Gestor do Contrato na manutenção do Histórico de Gestão do Contrato;

8.2.7. Fiscal (is) Administrativo (s):

a) verificação de aderência aos termos contratuais;

b) verificação da manutenção das condições classificatórias referentes à pontuação obtida e à habilitação técnica, em conjunto com o Fiscal Técnico do Contrato;

c) encaminhamento das demandas de correção à contratada, caso disponha de delegação de competência do Gestor do Contrato;

d) verificação das regularidades fiscais, trabalhistas e previdenciárias para fins de pagamento;

e) apoio ao Fiscal Requisitante do Contrato na verificação da manutenção da necessidade, economicidade e oportunidade da contratação; e

f) apoio ao Gestor do Contrato na manutenção do Histórico de Gestão do Contrato.

g) 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.

8.2.8. Fiscal (is) Requisitante (s):

a) avaliação da qualidade dos serviços realizados ou dos bens entregues e justificativas, a partir da aplicação das listas de verificação e de acordo com os critérios de aceitação definidos em contrato, em conjunto com o Fiscal Técnico do Contrato;

b) identificação de não conformidade com os termos contratuais, em conjunto com o Fiscal Técnico do Contrato;

c) encaminhamento das demandas de correção à contratada, caso disponha de

delegação de competência do Gestor do Contrato;

d) confecção e assinatura do Termo de Recebimento Definitivo, com base nas informações produzidas no recebimento provisório, na avaliação da qualidade dos serviços realizados ou dos bens entregues e na conformidade e aderência aos ternos contratuais, em conjunto com o Fiscal Técnico do Contrato;

e) verificação da manutenção da necessidade, economicidade e oportunidade da contratação, com apoio do Fiscal Técnico do Contrato;

f) verificação de manutenção das condições definidas nos Modelos de Execução e de Gestão do contrato, em conjunto com o Fiscal Técnico do Contrato; e

g) apoio ao Gestor do Contrato na manutenção do Histórico de Gestão do Contrato;

8.2.9. Gestor do Contrato:

a) Servidor 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;

b) Promover a realização da reunião inicial, a ser registrada em ata, convocada pelo Gestor do Contrato com a participação dos Fiscais Técnico, Requisitante e Administrativo do Contrato, da contratada e dos demais interessados por ele identificados;

c) Encaminhamento formal de demandas, devendo ocorrer por meio de Ordens de Serviço ou de Fornecimento de Bens ou conforme definido no Modelo de Execução do Contrato;

d) Encaminhamento das demandas de correção à contratada;

e) Encaminhar a indicação de glosas e sanções para a Área Administrativa;

f) Autorizar a emissão de nota (s) fiscal (is), a ser (em) encaminhada (s) ao preposto da CONTRATADA;

g) Encaminhar às autoridades competentes eventuais pedidos de modificação contratual;

h) Manter o Histórico de Gerenciamento do Contrato, contendo registros de todas as ocorrências relacionadas com a execução deste Contrato, determinando todas as ações necessárias para a regularização das faltas ou defeitos, por ordem histórica.

i) No caso de aditamento contratual, encaminhar documentação contida no Histórico de Fiscalização deste Contrato e com base nos princípios da manutenção da necessidade, economicidade e oportunidade da contratação, enviar à Área Administrativa, com pelo menos 90 (noventa) dias de antecedência do término deste Contrato, documentação explicitando os motivos para tal aditamento;

j) Manter registro de aditivos;

k) Controlar o prazo de vigência do instrumento contratual sob sua responsabilidade e verificar o cumprimento integral da execução dos serviços;

l) Encaminhar à CONTRATADA deficiências e Receber e atestar os documentos da despesa, quando comprovado o fiel e correto fornecimento dos serviços para fins de pagamento;

m)Comunicar, formalmente, irregularidades cometidas passíveis de penalidades, bem como indicar as glosas na Nota Fiscal;

n) Promover por meio da Equipe de Fiscalização do Contrato, a atualização contínua do Mapa de Gerenciamento de Riscos, identificando, analisando, avaliando e tratando novos riscos.

8.3. ***Níveis Mínimos de Serviço Exigidos***

8.3.1. **Entrega de Equipamentos**

8.3.1.1. Os equipamentos devem ser entregues após a Ordem de Fornecimento de Bens (OFB);

8.3.1.2. Os equipamentos devem ser novos, de primeiro uso e estar em linha de fabricação na data de entrega da solução;

8.3.1.3. O prazo para entrega será de 60 (sessenta) dias corridos, após o recebimento da OS/OFB pela contratada;

8.3.1.4. A entrega deve ser informada com, no mínimo, 5 (cinco) dias corridos de antecedência, no local indicado, de segunda a sexta-feira, em horário comercial;

8.3.1.5. As despesas de custeio com deslocamento dos equipamentos técnicos da proponente ao local de entrega, bem como todas as despesas de transporte, diárias, seguro ou quaisquer outros custos envolvidos ficarão a cargo exclusivo da CONTRATADA;

8.3.1.6. Os equipamentos (hardwares) ofertados na composição dos itens não devem estar listados como “End of Sale” ou “End of Life” por seus respectivos fabricantes até a data da abertura das propostas;

8.3.1.7. Para atendimento do Inciso III, Art. 3º do Decreto 7.174/2010, quando da entrega dos

equipamentos, o licitante deverá comprovar a origem dos bens importados e apresentar comprovante de quitação dos tributos de importação a eles referentes, sob pena de suspensão do(s) pagamento(s), rescisão contratual e multa;

8.3.2. **Instalação Física e Lógica**

8.3.2.1. A CONTRATADA deverá providenciar todos os materiais necessários à instalação física e lógica dos equipamentos e licenças;

8.3.2.2. A instalação deverá ser efetuada em até 30 (trinta) dias corridos, após a entrega dos equipamentos à CONTRATANTE.

8.3.2.3. Todos os parâmetros a serem configurados deverão ser alinhados entre as partes em reuniões de pré-projeto, podendo estas ser realizadas presencialmente, por telefone ou via conferência web, devendo a CONTRATADA sugerir as configurações de acordo com normas e boas práticas, cabendo à CONTRATANTE a sua aceitação expressa ou recusa nos casos de não atendimento das condições estabelecidas.

8.3.2.4. O planejamento da instalação contempla a confecção de documento do tipo SOW (em tradução livre, escopo de trabalho), que deverá detalhar a topologia de firewall e a migração das configurações e dos equipamentos adquiridos;

8.3.2.5. A migração de todas as configurações e serviços para os novos equipamentos adquiridos deverá ser realizada pela CONTRATADA, podendo esta realizar o levantamento dos atuais equipamentos e configurações durante a vistoria técnica.

8.3.3. **Níveis de Severidade dos Chamados de Garantia (Grupo 1)**

GRAU	DESCRIÇÃO	TIPO DE ATENDIMENTO	TEMPO DE ATENDIMENTO	TEMPO DE SOLUÇÃO OU DE CONTORNO	DA EXTRAPOLAÇÃO DOS PRAZOS
1 - MÁXIMA	Chamados referentes a situações de urgência ou problema crítico, caracterizados pela existência de ambiente paralisado, com equipamentos parcialmente ou totalmente inoperantes e/ou que envolvam paralisações ou severa perda de desempenho nos serviços, inclusive aqueles que envolvam a troca do equipamento.	Remoto/Presencial	O atendimento remoto/presencial deverá ser iniciado em no máximo 01 (uma) hora após a abertura do registro do chamado na CONTRATADA para início das ações correspondentes à solução definitiva ou contorno.	No máximo 6 (seis) horas corridas após a abertura do chamado.	O atraso superior ao prazo estabelecido será passível das sanções previstas neste instrumento.
2 - ALTA	Chamados associados a situações de alto impacto, referentes ao uso do produto, com equipamentos parcialmente ou totalmente inoperantes e/ou que envolvam paralisações ou severa perda de desempenho nos serviços, inclusive aqueles que envolvam a troca do equipamento.	Remoto/Presencial	O atendimento remoto/presencial deverá ser iniciado em no máximo 03 (três) horas após a abertura do registro do chamado na CONTRATADA para início das ações correspondentes à solução definitiva ou contorno.	No máximo 12 (doze) horas corridas após a abertura do chamado.	O atraso superior ao prazo estabelecido será passível das sanções previstas neste instrumento.
3 - MÉDIA	Chamados referentes a situações de baixo impacto ou para aqueles problemas que se apresentem de forma intermitente, que não envolvam paralisações ou severa perda de desempenho nos serviços, ou que não impliquem em equipamentos ou módulos de equipamentos total ou parcialmente inoperantes.	Remoto/Presencial	O atendimento remoto/presencial deverá ser iniciado em no máximo 06 (seis) horas após a abertura do registro do chamado na CONTRATADA para início das ações correspondentes à solução definitiva ou contorno.	No máximo 24 (vinte e quatro) horas corridas após a abertura do chamado.	O atraso superior ao prazo estabelecido será passível das sanções previstas neste instrumento.
			O atendimento remoto/presencial deverá ser		

4 - BAIXA	Chamados com o objetivo de sanar dúvidas quanto ao uso ou à implementação do produto, que não envolvam paralisações ou severa perda de desempenho nos serviços, ou que não impliquem em equipamentos ou módulos de equipamentos total ou parcialmente inoperantes	Remoto/Presencial	deverá ser iniciado em no máximo 12 (doze) horas após a abertura do registro do chamado na CONTRATADA para início das ações correspondentes à solução definitiva ou contorno.	No máximo 48 (quarenta e oito) horas corridas após a abertura do chamado.	O atraso superior ao prazo estabelecido será passível das sanções previstas neste instrumento.

Tabela 9 **- Atendimento dos Chamados de Garantia**

8.4. **Sanções Administrativas**

8.4.1. Comete infração administrativa nos termos da Lei nº 8.666, de 1993 e da Lei nº 10.520, de 2002, a Contratada que:

8.4.1.1. inexecutar total ou parcialmente qualquer das obrigações assumidas em decorrência da contratação;

8.4.1.2. ensejar o retardamento da execução do objeto;

8.4.1.3. fraudar na execução do contrato;

8.4.1.4. comportar-se de modo inidôneo; cometer fraude fiscal;

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

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

8.4.2.2. Multa de:

8.4.2.2.1. 0,2% (dois décimos por cento) por dia sobre o valor adjudicado em caso de atraso na execução do contrato, limitada a incidência a 15 (quinze) dias. Após o décimo quinto dia e a critério da Administração, no caso de execução com atraso, poderá ocorrer a não-aceitação do objeto, de forma a configurar, nessa hipótese, inexecução total da obrigação assumida, sem prejuízo da rescisão unilateral da avença;

8.4.2.2.2. 10% (dez por cento) sobre o valor adjudicado, em caso de atraso na execução do objeto, por período superior ao previsto no subitem acima, ou de inexecução parcial da obrigação assumida;

8.4.2.2.3. 15% (quinze por cento) sobre o valor adjudicado, em caso de inexecução total da obrigação assumida;

8.4.2.2.4. 0,2% a 1,6% por dia sobre o valor do contrato, conforme detalhamento constante das tabelas 1 e 2, abaixo; e

8.4.2.2.5. 0,07% (sete centésimos por cento) do valor do contrato por dia de atraso na apresentação da garantia (seja para reforço ou por ocasião de prorrogação), observado o máximo de 2% (dois por cento). O atraso superior a 25 (vinte e cinco) dias autorizará a Administração CONTRATANTE a promover a rescisão do contrato;

8.4.2.2.6. as penalidades de multa decorrentes de fatos diversos serão consideradas independentes entre si.

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

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

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

8.4.3. A Sanção de impedimento de licitar e contratar prevista no subitem 8.4.2.4 também é aplicável em quaisquer das hipóteses previstas como infração administrativa neste Termo de Referência.

8.4.4. As sanções previstas nos subitens 8.4.2.1, 8.4.2.3, 8.4.2.4 e 8.4.2.5 poderão ser aplicadas à CONTRATADA juntamente com as de multa, descontando-a dos pagamentos a serem efetuados

8.4.5. Para efeito de aplicação de multas, que serão sobre o valor do contrato, voltadas ao não cumprimento dos prazos de garantia, suporte e instalação da solução, às infrações são atribuídos graus, de acordo com as tabelas 1 e 2:

GRAU	CORRESPONDÊNCIA
1	0,2% por hora sobre o valor do contrato
2	0,4% por hora sobre o valor do contrato
3	0,8% por hora sobre o valor do contrato
4	1,6% por hora sobre o valor do contrato

Tabela 1

INFRAÇÃO		
Para os itens a seguir, DEIXAR DE:		
1	Cumprir os prazos estabelecidos para execução da garantia, suporte e instalação da solução relacionada aos chamados de criticidade máxima.	4
2	Cumprir os prazos estabelecidos para execução da garantia, suporte e instalação da solução relacionada aos chamados de criticidade alta.	3
3	Cumprir os prazos estabelecidos para execução da garantia, suporte e instalação da solução relacionada aos chamados de criticidade média.	2
4	Cumprir os prazos estabelecidos para execução da garantia, suporte e instalação da solução relacionada aos chamados de criticidade baixa.	1

Tabela 2

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

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

8.4.6.2. tenham praticado atos ilícitos visando a frustrar os objetivos da licitação;

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

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

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

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

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

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

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

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

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

8.4.14. As penalidades serão obrigatoriamente registradas no SICAF.

8.5. ***Do Pagamento***

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

8.5.12.2. Com o intuito de evitar quaisquer problemas no momento do pagamento, no que diz respeito ao recolhimento de tributos, sugere-se que, caso a empresa vencedora da licitação não seja domiciliada em Brasília e a prestação de serviços venha a ser realizada na citada localidade, providencie seu Cadastro Fiscal do Distrito Federal, antes da emissão da Nota Fiscal.

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

EM = I x N x VP, sendo:

EM = Encargos moratórios;

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

VP = Valor da parcela a ser paga.

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

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

9. ESTIMATIVA DE PREÇOS DA CONTRATAÇÃO

9.1. A estimativa de preço da contratação foi realizada pela Equipe de Planejamento da Contratação, com a elaboração do orçamento detalhado, composta por preços unitários e fundamentada em pesquisa de preços realizada em conformidade com os procedimentos administrativos estabelecidos na Instrução Normativa SLTI/MP n° 05, de 27 de julho de 2014, e suas atualizações. Os documentos utilizados para embasar a pesquisa de preços integram o Processo Administrativo.

9.2. O valor máximo previsto para o Grupo 1 é de **R$ 6.007.067,50 (seis milhões, sete mil sessenta e sete reais e cinquenta centavos).**

9.3. No valor acima devem estar 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.

Grupo	Item	Descrição	Unidade	QTDE	Valor unitário máximo (R$)	Valor total máximo (R$)
1	1	FIREWALL TIPO I - APPLIANCE FÍSICO	Unitário	04	R$ 1.276.800,00	R$ 5.107.200,00
	2	FIREWALL TIPO II - APPLIANCE FÍSICO	Unitário	05	R$ 102.067,50	R$ 510.337,50
	3	APPLIANCE FÍSICO PARA ANÁLISE DO TRÁFEGO DE DADOS	Unitário	01	R$ 210.030,00	R$ 210.030,00
	4	APPLIANCE VIRTUAL DE GERENCIAMENTO CENTRALIZADO	Unitário	01	R$ 179.500,00	R$ 179.500,00
	VALOR TOTAL DA CONTRATAÇÃO				**R$ 6.007.067,50**	

Tabela 10 - Descrição dos itens

10. ADEQUAÇÃO ORÇAMENTÁRIA E CRONOGRAMA FÍSICO-FINANCEIRO

10.1. As despesas decorrentes desta contratação estão programadas em dotação orçamentária própria, prevista no orçamento da União, para o exercício de 2023, na classificação abaixo:

10.1.1. Programa de Trabalho: 04122003220000000001

10.1.2. Plano de Trabalho Resumido (PTRES): 172184

10.1.3. Fonte: 1000

10.1.4. Ação: 2000

10.1.5. Plano Orçamentário (PO): 000C

10.1.6. Plano Interno (PI): GL67OTCGLTI

10.1.7. As Naturezas de despesas serão detalhadas da tabela abaixo:

Grupo	Item	Descrição do Bem ou Serviço	Natureza de Despesa
1	1	FIREWALL TIPO I - APPLIANCE FÍSICO	449052
	2	FIREWALL TIPO II - APPLIANCE FÍSICO	449052
	3	APPLIANCE FÍSICO PARA ANÁLISE DO TRÁFEGO DE DADOS	449052
	4	APPLIANCE VIRTUAL DE GERENCIAMENTO CENTRALIZADO	449040

Tabela 11 - Natureza de despesa dos bens

11. DA VIGÊNCIA DO CONTRATO

11.1. O prazo de vigência da contratação será de 12 (doze) meses, a partir da assinatura do contrato, prorrogáveis conforme art. 57, §1º, da Lei nº 8.666/93.

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

11.3. A licitante vencedora terá o prazo de 5 (cinco) dias úteis, contados do recebimento da notificação, para assinar o contrato junto à Administração, sob pena de decair do direito à contratação, sem prejuízo das penalidades previstas cabíveis.

11.4. A recusa injustificada da licitante em assinar o contrato no prazo acima, caracteriza o descumprimento total da obrigação assumida, ficando sujeita as sanções previstas no Termo de Referência.

11.5. O prazo previsto para assinatura poderá ser prorrogado, por igual período, por solicitação justificada do adjudicatário e aceita pela Administração.

11.6. A CONTRATADA não tem direito subjetivo à prorrogação contratual.

11.7. A prorrogação de contrato deverá ser promovida mediante celebração de termo aditivo.

12. ALTERAÇÃO SUBJETIVA

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

13. REAJUSTES DE PREÇOS

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

13.2. Após o interregno de um ano, e mediante pedido da CONTRATADA, os preços iniciais serão reajustados, mediante a aplicação, pela CONTRATANTE, do índice ICTI, exclusivamente para as obrigações iniciadas e concluídas após a ocorrência da anualidade, com base na seguinte fórmula (art. 5º do Decreto n.º 1.054, de 1994):

R = V (I – Iº) / Iº, onde:

R = Valor do reajuste procurado;

V = Valor contratual a ser reajustado;

Iº = índice inicial - refere-se ao índice de custos ou de preços correspondente à data fixada para entrega da proposta na licitação;

I = Índice relativo ao mês do reajustamento;

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

13.4. No caso de atraso ou não divulgação do índice de reajustamento, o CONTRATANTE pagará à CONTRATADA a importância calculada pela última variação conhecida, liquidando a diferença correspondente tão logo seja divulgado o índice definitivo.

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

13.6. Caso o índice estabelecido para reajustamento venha a ser extinto ou de qualquer forma não possa mais ser utilizado, será adotado, em substituição, o que vier a ser determinado pela legislação então em vigor.

13.7. 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.

13.8. O reajuste será realizado por apostilamento.

14. DOS CRITÉRIOS DE SELEÇÃO DO FORNECEDOR

14.1. ***Regime, Tipo e Modalidade da Licitação***

14.1.1. A presente contratação adotará como regime de execução a Empreitada por Preço Unitário.

14.1.2. De acordo com o Art. 1º, § 1º , do Decreto nº 10.024/2019 a licitação será realizada na modalidade pregão eletrônico, com julgamento pelo critério de **MENOR PREÇO POR GRUPO** atendidas as especificações e características técnicas exigidas no presente Termo de Referência.

14.1.3. O objeto desta contratação encontra fundamentação legal nos termos do parágrafo único, do Art. 1º, da Lei 10.520, de 2002, c/c Art. 3º do Decreto nº 10.024/2019 e Art. 9º, §2º do

Decreto 7.174/2010, e enquadra-se como "**BEM OU SERVIÇO COMUM**" por apresentar padrões de desempenho e qualidade que possam ser objetivamente definidos pelo edital, por meio de especificações usuais no mercado.

14.2. ***Da Inaplicabilidade das Margens de Preferências***

14.2.1. Considerando a característica e a complexidade do objeto da presente contratação, é inviável a definição de margens de preferência aplicáveis a produtos produzidos no país ou a serviços.

14.3. ***Critérios de Qualificação Técnica para a Habilitação***

14.3.1. **Da vistoria técnica**

14.3.1.1. Para o correto dimensionamento e elaboração de sua proposta, o licitante *poderá* realizar vistoria nas instalações do local onde serão instalados os firewalls, acompanhado por servidor designado para esse fim, de segunda à sexta-feira, das 08:00 horas às 18:00 horas, agendada com antecedência mínima de 12 (doze) horas através do e-mail (correio eletrônico): **citic@mj.gov.br**.

14.3.1.2. O prazo para vistoria iniciar-se-á no dia útil seguinte ao da publicação do Edital, estendendo-se até o dia útil anterior à data prevista para a abertura da sessão pública.

14.3.1.3. Para a vistoria o licitante, ou o seu representante legal, deverá estar devidamente identificado, apresentando documento de identidade civil e documento expedido pela empresa comprovando sua habilitação para a realização da vistoria.

14.3.1.4. Por ocasião da vistoria, ao licitante, ou ao seu representante legal, poderá ser entregue CD-ROM, "pen-drive" ou outra forma compatível de reprodução, contendo as informações relativas ao objeto da licitação, para que a empresa tenha condições de bem elaborar sua proposta.

14.3.1.5. A não realização da vistoria, quando facultativa, não poderá embasar posteriores alegações de desconhecimento das instalações, dúvidas ou esquecimentos de quaisquer detalhes dos locais da prestação dos serviços, devendo a licitante vencedora assumir os ônus dos serviços decorrentes.

14.3.1.6. A licitante deverá declarar que tomou conhecimento de todas as informações e das condições locais para o cumprimento das obrigações objeto da licitação.

14.3.2. **Qualificação técnica**

14.3.2.1. Para efeito de aferição da qualificação técnica do fornecedor, o(s) licitante(s) deverá(ão) apresentar atestado(s) de capacidade técnica em seu(s) nome(s), fornecido por pessoa jurídica de direito público ou privado, comprovando:

14.3.2.1.1. **Grupo I:**

14.3.2.1.1.1. No mínimo o fornecimento de 50% do quantitativo do item 1 e 50% do item 2 com características compatíveis com as especificadas nesse Termo de Referência.

14.3.2.1.1.1.1. O quantitativo previsto para o item 2 é de 5 (cinco) equipamentos, o que resultará em número fracionado. Sendo assim, considera-se o mínimo exigido de 2 (dois) equipamentos.

14.3.2.2. Poderá ser apresentado mais de um atestado para fim de comprovação da qualificação técnica.

14.3.2.3. Caso não haja menção explícita no atestado quanto às funcionalidades solicitadas, deve ser apresentada documentação oficial do fabricante que comprove tal suporte nos modelos constantes no atestado.

14.3.2.4. É vetada a indicação de entidade certificadora, exceto nos casos previamente dispostos em normas da Administração Pública.

14.3.2.5. É vetada a exigência, para fins de qualificação técnica na fase de habilitação, de atestado, declaração, carta de solidariedade, comprovação de parceria ou credenciamento emitidos por fabricantes.

14.3.2.6. As competências exigidas correspondem às quantidades relevantes dos itens mais críticos para assegurar que a LICITANTE tenha efetiva capacidade de prestar os serviços considerando a complexidade da infraestrutura de TI que a CONTRATANTE deseja implementar. Além disso, conforme exposto na justificativa da contratação, pretende-se realizar melhorias na topologia de firewall do MJSP, o que torna essencial, para garantir a correta implementação do projeto, que configurações adequadas, desempenho, qualidade, além da disponibilidade, confiabilidade e integridade das informações, sejam garantidas pela LICITANTE, sendo isso exposto pelas qualificações técnicas solicitadas.

15. DOS ANEXOS

15.1. São partes integrantes deste Termo de Referência os seguintes anexos:

- ANEXO I - A - ESPECIFICAÇÕES TÉCNICAS
- ANEXO I - B - PROPOSTA DE PREÇOS
- ANEXO I - C - MODELO DE ORDEM DE SERVIÇO – O.S.

- ANEXO I - D - MODELO DE DECLARAÇÃO DE VISTORIA
- ANEXO I - E - TERMO DE CIÊNCIA
- ANEXO I - F - TERMO DE COMPROMISSO
- ANEXO I - G - MODELO DE DECLARAÇÃO DE RENÚNCIA À VISTORIA
- ANEXO I - H - MODELO DE PLANO DE INSERÇÃO
- ANEXO I - I - MODELO DE PLANO DE FISCALIZAÇÃO
- ANEXO I - J - MODELO DE DECLARAÇÃO DE SUSTENTABILIDADE AMBIENTAL

16. DA EQUIPE DE PLANEJAMENTO DA CONTRAÇÃO E DA APROVAÇÃO

16.0.1. A Equipe de Planejamento da Contratação foi instituída pela Portaria SAA nº 21, de 13 de Abril de 2023 (23936325).

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

Integrante Requisitante		**Integrante Técnico**		**Integrante Administrativo**	
Nome	Rodrigo Albernaz Bezerra	Nome	Henrique Eiti Otaguiri Nagazawa	Nome	Elizaneide Almeida de Lima
Cargo	Coordenador-Geral de Infraestrutura e Serviços	Cargo	Analista Técnico-Administrativo	Cargo	Chefe da Divisão de Contratos
Matrícula	05120406	Matrícula	1796323	Matrícula	2192119

Aprovo,

Autoridade Máxima da Área de TIC e Autoridade Competente	
Nome	Ney Rego Barros Junior
Cargo	Subsecretário de Tecnologia da Informação e Comunicação
Matrícula	1908003

Documento assinado eletronicamente por **HENRIQUE EITI OTAGUIRI NAGAZAWA**, **Integrante Técnico(a)**, em 07/08/2023, às 17:10, com fundamento no § 3º do art. 4º do Decreto nº 10.543, de 13 de novembro de 2020.

Documento assinado eletronicamente por **RODRIGO ALBERNAZ BEZERRA**, **Coordenador(a)-Geral de Infraestrutura e Serviços**, em 08/08/2023, às 17:01, com fundamento no § 3º do art. 4º do Decreto nº 10.543, de 13 de novembro de 2020.

Documento assinado eletronicamente por **Ney Rego Barros Junior**, **Subsecretário(a) de Tecnologia da Informação e Comunicação**, em 09/08/2023, às 18:15, com fundamento no § 3º do art. 4º do Decreto nº 10.543, de 13 de novembro de 2020.

ANEXOS DO TERMO DE REFERÊNCIA

ANEXO I-A - ESPECIFICAÇÕES TÉCNICAS

1. ESPECIFICAÇÕES TÉCNICAS

1.1. **Grupo 1**

1.1.1. **Item 1 – FIREWALL TIPO I (SD-WAN/NGFW) - APPLIANCE FÍSICO**

1.1.2. **A solução de segurança (NGFW) deve possuir a capacidade e as características abaixo:**

1.1.2.1. Throughput de, no mínimo, 15Gbps com a funcionalidade de Threat Prevention, ou seja, com funcionalidades de Firewall, IPS, Controle de Aplicação e Antivírus habilitadas;

1.1.2.2. Throughput de, no mínimo, 50 Gbps de VPN IPSec;

1.1.2.3. Estar licenciado para, ou suportar sem o uso de licença, 10.000 túneis de VPN IPSEC Site-to-Site simultâneos;

1.1.2.4. Suporte a, no mínimo, 500 mil novas conexões por segundo;

1.1.2.5. Suportar no mínimo 10 Gbps de throughput de Inspeção SSL;

1.1.2.6. Possuir ao menos 12 interfaces 1 GE RJ45;

1.1.2.7. Possuir ao menos 8interfaces 1 GE SFP com transceivers inclusos;

1.1.2.8. Possuir ao menos 8interfaces 10 GE SFP+ com transceivers inclusos;

1.1.2.9. Possuir ao menos 4 interfaces 25 GE SFP28 com transceivers inclusos;

1.1.2.10. Possuir ao menos 2 interfaces 40 GE QSFP+ com transceivers inclusos;

1.1.2.11. Suportar a criação de no mínimo 10 instâncias virtuais;

1.1.2.12. Possuir armazenamento de no mínimo de 1 TB com 2 (dois) discos em RAID1, por equipamento, pois a falha do disco, se único, ocasionará indisponibilidade da solução bem como os dados de log nele existentes;

1.1.2.13. Possuir fonte de alimentação interna, redundante e hot-swap;

1.1.2.14. Deve suportar a instalação em rack padrão 19";

1.1.3. **Item 2 - FIREWALL TIPO II (SD-WAN/NGFW) - APPLIANCE FÍSICO**

1.1.3.1. Throughput de, no mínimo, 1Gbps com a funcionalidade de Threat Prevention, ou seja, com funcionalidades de Firewall, IPS, Controle de Aplicação e Antivírus habilitadas;

1.1.3.2. Throughput de, no mínimo, 8 Gbps de VPN IPSec para ser utilizado no SD-WAN;

1.1.3.3. Estar licenciado para, ou suportar sem o uso de licença, 500 túneis de VPN IPSEC Site-to-Site simultâneos;

1.1.3.4. Suporte a, no mínimo, 55 mil novas conexões por segundo;

1.1.3.5. Suportar no mínimo 1 Gbps de throughput de Inspeção SSL;

1.1.3.6. Possuir ao menos 16 interfaces 1 GE RJ45;

1.1.3.7. Possuir ao menos 4interfaces 1 GE SFP com transceivers inclusos;

1.1.3.8. Possuir ao menos 2 interfaces 10 GE SFP+ com transceivers inclusos;

1.1.3.9. Suportar a criação de no mínimo 5 instâncias virtuais;

1.1.3.10. Deve incluir porta USB compatível com modem 3G/4G, permitindo ainda que este link WAN seja utilizado nas regras de SD-WAN;

1.1.3.11. Possuir armazenamento de no mínimo de 480GB;

1.1.3.12. Possuir fonte de alimentação interna redundante;

1.1.3.13. Deve suportar a instalação em rack padrão 19";

1.1.4. **Características gerais para os equipamentos NGFW e SD-WAN:**

1.1.4.1. A solução deve consistir em plataforma de proteção de rede baseada em appliance físico com funcionalidades de Next Generation Firewall (NGFW) e SD-WAN, não sendo permitido appliances virtuais ou solução open source (produto montado);

1.1.4.2. Os hardwares e os softwares que compõem a solução devem ser do mesmo fabricante;

1.1.4.3. As funcionalidades de NGFW e SD-WAN devem ser ofertadas no mesmo appliance, não sendo permitido a composição de equipamentos separados para cada uma das funções;

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

1.1.4.5. Por funcionalidades de SD-WAN entende-se: roteamento inteligente, uso do melhor link por aplicação, abstração do tráfego em relação aos circuitos físicos e controle do tráfego por aplicação;

1.1.4.6. As funcionalidades de NGFW e SD-WAN que compõem a solução devem funcionar em um único equipamento e devem obedecer a todos os requisitos desta especificação, como termo de garantia, atualizações e manutenção, suporte e gerenciamento centralizado;

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

1.1.4.8. Para todos os equipamentos deverá ser fornecido bandeja ou suporte para montagem em rack;

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

1.1.4.10. Deverá suportar tags de VLAN (802.1Q);

1.1.4.11. Deverá possuir suporte a agregação de links via 802.3ad LACP;

1.1.4.12. Deverá possuir ferramenta de diagnóstico do tipo tcpdump e ainda dispor de ferramenta integrada à interface web para capturar informações dos pacotes em tempo real, podendo aplicar filtros, tais como IPs e portas, e ainda ter disponível a possibilidade de exportar a captura para um arquivo do tipo PCAP visando estender a análise para um software terceiro, tal como Wireshark;

1.1.4.13. Deverá possuir integração com servidores de autenticação RADIUS, LDAP e Microsoft Active Directory;

1.1.4.14. Deverá possuir integração com tokens para autenticação de duplo fator;

1.1.4.15. Deverá suportar single-sign-on;

1.1.4.16. Deve possuir a funcionalidade de tradução de endereços estáticos – NAT (Network Address Translation), um para um, N-para-um, vários para um, NAT64, NAT66, NAT46 e PAT;

1.1.4.17. Deverá suportar roteamento estático para IPv4 e IPv6;

1.1.4.18. Deverá suportar roteamento dinâmico para IPv4 e IPv6 (OSPF, BGP, RIP);

1.1.4.19. Deverá suportar ECMP;

1.1.4.20. Os dispositivos de proteção de rede devem possuir suporte a roteamento multicast (PIM-SM e PIM-DM);

1.1.4.21. Deverá possuir funcionalidades de DHCP Cliente, Servidor e Relay;

1.1.4.22. Deverá suportar aplicações multimídia, tais como: H.323 e SIP;

1.1.4.23. Deverá suportar alta disponibilidade (HA), trabalhando no esquema de redundância do tipo Ativo-Passivo e também Ativo-Ativo;

1.1.4.24. Deverá permitir o funcionamento em modo transparente tipo "*bridge*";

1.1.4.25. Deverá suportar PBR – Policy Based Routing;

1.1.4.26. Deverá possuir conexão entre estação de gerência e appliance criptografada, tanto em interface gráfica, quanto em CLI (linha de comando);

1.1.4.27. Deverá possuir mecanismo de anti-spoofing;

1.1.4.28. Deverá permitir criação de regras definidas pelo usuário;

1.1.4.29. Deverá suportar sFlow ou Netflow;

1.1.4.30. Os dispositivos de proteção de rede devem possuir suporte a Jumbo Frames;

1.1.4.31. Deverá permitir autenticação de usuários em base local, servidor LDAP, RADIUS e TACACS;

1.1.4.32. Deverá permitir funcionamento em modo bridge em camada 2, roteador em camada 3, proxy explícito e sniffer via espelhamento;

1.1.4.33. Deverá possuir mecanismo de tratamento de sessão (session-helpers ou ALGs);

1.1.4.34. Deve possuir suporte a criação de sistemas virtuais no mesmo appliance e que possam ser administrados por equipes distintas;

1.1.4.35. Deverá permitir limitar o uso de recursos utilizados por cada sistema virtual;

1.1.4.36. Deve suportar o protocolo padrão da indústria VXLAN;

1.1.4.37. Permitir, para o gerenciamento da solução, interface de administração via web no próprio dispositivo;

1.1.4.38. Deve permitir monitorar via SNMP o uso de CPU, memória, espaço em disco, VPN, situação do cluster, eventos de segurança e estatísticas das verificações de saúde da camada SD-WAN;

1.1.4.39. Deve disponibilizar controle, inspeção e de-criptografia de SSL para tráfego de entrada e saída, sendo que deve suportar ainda o controle dos certificados individualmente dentro de cada sistema virtual, ou seja, isolamento das operações de adição, remoção e utilização dos certificados diretamente nos sistemas virtuais;

1.1.4.40. Em caso de ser gerenciado de forma centralizada, o equipamento ofertado deverá continuar tratando o tráfego corretamente, sem causar interrupção das comunicações, mesmo no caso de queda da comunicação dos equipamentos com a solução de gerência centralizada;

1.1.4.41. Deverá possuir conectores de SDN e dessa forma ser capaz de sincronizar de forma automática objetos;

1.1.4.42. Deverá suportar ambientes multi-cloud;

1.1.4.43. Deverá possuir a capacidade de criar automações através de gatilhos e ações,

possibilitando uma atuação mais proativa;

1.1.4.44. Suporte a configuração de alta disponibilidade Ativo/Passivo e Ativo/Ativo;

1.1.4.45. A configuração em alta disponibilidade deve sincronizar:

1.1.4.45.1. Sessões;

1.1.4.45.2. Configurações, incluindo, mas não limitado às políticas de Firewall, NAT, QoS e objetos de rede;

1.1.4.45.3. Associações de Segurança das VPNs;

1.1.4.45.4. Tabelas FIB;

1.1.4.45.5. Assinaturas de IPS, Antivírus e AntiSpyware;

1.1.4.46. A configuração de alta disponibilidade deve possibilitar monitoração de falha de link;

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

1.1.4.48. Os equipamentos devem ser novos, ou seja, de primeiro uso, de um mesmo fabricante. Na data da proposta, nenhum dos modelos ofertados poderão estar listados no site do fabricante em listas de end-of-life e end-of-sale;

1.1.4.49. Os equipamentos que compõem a solução devem estar homologados pela Anatel.

1.1.5. **Funcionalidades de Firewall:**

1.1.5.1. Deverá possuir controle de acesso à Internet por endereço IP de origem e destino;

1.1.5.2. Deverá possuir controle de acesso à Internet por subrede;

1.1.5.3. Deverá ter a capacidade de criar políticas de firewall baseando-se em endereços MAC;

1.1.5.4. Deverá suportar controles por zonas de segurança;

1.1.5.5. Deverá suportar controles de políticas por porta e protocolo;

1.1.5.6. Deverá suportar controles de políticas por aplicações, grupos estáticos de aplicações e grupos dinâmicos de aplicações;

1.1.5.7. Controle de políticas por usuários, grupos de usuários, IPs, range de IPs, subrede, FQDN e zonas de segurança;

1.1.5.8. Deve suportar a criação de políticas por geo-localização, permitindo que o tráfego de determinado País/Países seja bloqueado;

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

1.1.5.10. Deve ser viável criar políticas com exceções, onde seja possível especificar que uma política será aplicada somente caso a origem ou destino do tráfego não seja um determinado objeto, tal como uma subrede, por exemplo, ou seja, se a subrede não for 192.168.0.0/24, o tráfego deverá ser tratado.

1.1.5.11. Controle, inspeção e de-criptografia de SSL por política para tráfego de saída;

1.1.5.12. Deve ser possível realizar um espelhamento do tráfego de-criptografado.

1.1.5.13. Deve de-criptografar tráfego de saída em conexões negociadas com TLS 1.2 e TLS 1.3;

1.1.5.14. A inspeção SSL deve ser compatível com HTTP3. Tal inspeção é essencial uma vez que uma grande quantidade de sítios públicos está utilizando o protocolo em questão, tais como serviços de compartilhamento de vídeos, sites de busca e redes sociais, os quais estão sendo diariamente consumidos por usuários corporativos e externos.

1.1.5.15. Deve permitir o bloqueio de arquivo por sua extensão e possibilitar a correta identificação do arquivo por seu tipo mesmo quando sua extensão for renomeada;

1.1.5.16. Deve suportar objetos de endereço IPv4 e IPv6 consolidados na mesma política de firewall

1.1.5.17. Suporte a objetos e regras multicast;

1.1.5.18. Deve ser possível criar políticas de firewall utilizando serviços de ameaças de terceiros, onde o firewall receberá uma lista de endereços IPs maliciosos, por exemplo, a qual poderá ser utilizada para bloqueio do tráfego.

1.1.5.19. Deve ser possível criar política de firewall em modo de aprendizado, onde o equipamento deverá monitorar o tráfego que transita nas interfaces de origem e destino e registrar logs de eventos.

1.1.5.20. Deve possuir base com objetos contendo endereços IPs de serviços da Internet como, a citar, mas não se limitando a AWS S3, Microsoft Azure, Oracle, SAP, Google e Microsoft Office 365, atualizados dinamicamente pela solução.

1.1.5.21. Suportar a atribuição de agendamento das políticas com o objetivo de habilitar e desabilitar políticas em horários pré-definidos automaticamente;

1.1.5.22. Deve dispor de ferramenta para auxiliar a descobrir quais políticas correspondem a um

determinado perfil de tráfego, facilitando assim a administração diária da solução e facilmente encontrando quais políticas estão sendo atribuídas a um determinado IP, por exemplo.

1.1.6. **Funcionalidades de SD-WAN:**

1.1.6.1. Entende-se como tecnologia SD-WAN (Software-Defined WAN) a rede de área ampla definida por software que centraliza a gerência da rede WAN em uma console única, eliminando a necessidade de intervenções manuais em roteadores em localidades remotas, proporcionando visibilidade do tráfego, seleção de caminho dinâmico baseado em políticas de QoS, aplicação ou desempenho e utilização de túneis VPN para comunicação entre as localidades;

1.1.6.2. A solução deve prover recursos de roteamento inteligente, definindo, mediante regras pré-estabelecidas, o melhor caminho a ser tomado para uma aplicação;

1.1.6.3. Deve ser possível criar políticas para modelagem do tráfego definido pelo menos os parâmetros:

1.1.6.4. IP de origem;

1.1.6.5. VLAN de origem;

1.1.6.6. IP de destino;

1.1.6.7. Porta TCP/UDP de destino;

1.1.6.8. Domínio e URL de destino;

1.1.6.9. Aplicação de camada 7 utilizada (O365 Exchange, AWS, Dropbox e etc);

1.1.6.10. A solução deverá ser capaz de monitorar e identificar falhas mediante a associação de health check, permitindo testes de resposta por ping, http, tcp/udp echo, dns, tcp-connect e twamp;

1.1.6.11. O SD-WAN deverá balancear o tráfego das aplicações entre múltiplos links simultaneamente;

1.1.6.12. O SD-WAN deverá analisar o tráfego em tempo real e realizar o balanceamento dos pacotes de um mesmo fluxo entre múltiplos links simultaneamente em uma extremidade e realizar a reordenação dos pacotes desse mesmo fluxo no outro extremo;

1.1.6.13. Deverá ser permitida a criação de políticas de roteamento com base nos seguintes critérios: latência, jitter, perda de pacote, banda ocupada ou todos ao mesmo tempo;

1.1.6.14. A solução deve permitir a definição do roteamento para cada aplicação;

1.1.6.15. Deverá ser permitida a criação de políticas de roteamento com base nos seguintes critérios: latência, jitter, perda de pacote, banda ocupada ou todos ao mesmo tempo;

1.1.6.16. Diversas formas de escolha do link devem estar presentes, incluindo: melhor link, menor custo e definição de níveis máximos de qualidade a serem aceitos para que tais links possam ser utilizados em um determinado roteamento de aplicação;

1.1.6.17. Deve possibilitar a definição do link de saída para uma aplicação específica;

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

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

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

1.1.6.21. A solução de SD-WAN deve possuir suporte a Policy based routing ou policy based forwarding;

1.1.6.22. Deve suportar o uso de VRF (Virtual Routing and Forwarding);

1.1.6.23. Deve suportar roteamento estático e dinâmico (OSPFv2/v3, BGPv4/BGP4+);

1.1.6.24. Deve possibilitar a agregação de túneis IPSec, realizando balanceamento por pacote entre os mesmos;

1.1.6.25. Deve possuir recurso para correção de erro (FEC), possibilitando a redução das perdas de pacotes nas transmissões;

1.1.6.26. A solução deve permitir a duplicação de pacotes entre dois ou mais links, que atendam os parâmetros de qualidade estabelecidos, objetivando uma melhor experiência de uso de aplicações;

1.1.6.27. A solução deve possuir recurso para controlar e corrigir erros na transmissão de dados, enviando dados redundantes através de túnel VPN em antecipação à perda de pacotes que pode ocorrer durante o trânsito;

1.1.6.28. Deve permitir configurar o código de DiffServ (DSCP) do pacote ESP do túnel IPSec;

1.1.6.29. Deve permitir a customização dos timers para detecção de queda de link, bem como tempo necessário para retornar com o link para o balanceamento após restabelecido;

1.1.6.30. Com a finalidade de controlar aplicações e tráfego cujo consumo possa ser excessivo, (como youtube, Facebook, etc), impactando no bom uso das aplicações de negócio, se requer que a solução, além de poder permitir ou negar esse tipo de aplicações, deve ter a capacidade de controlá-las por políticas de shaping. Dentre as tratativas possíveis, a solução deve contemplar:

1.1.6.31. Suportar a criação de políticas de QoS e Traffic Shaping por endereço de origem, endereço de destino, usuário e grupo de usuários, aplicações e porta;

1.1.6.32. O QoS deve possibilitar a definição de tráfego com banda garantida. Ex: banda mínima disponível para aplicações de negócio;

1.1.6.33. O QoS deve possibilitar a definição de tráfego com banda máxima. Ex: banda máxima permitida para aplicações do tipo best-effort/não corporativas, tais como Youtube, Facebook etc;

1.1.6.34. Deve ainda possibilitar a marcação de DSCP, a fim de que essa informação possa ser utilizada ao longo do backbone para fins de reserva de banda;

1.1.6.35. O QoS deve possibilitar a definição de fila de prioridade;

1.1.6.36. Além de possibilitar a definição de banda máxima e garantida por aplicação, deve também suportar o match em categorias de URL, IPs de origem e destino, logins e portas;

1.1.6.37. A capacidade de agendar intervalos de tempo onde as políticas de shaping/QoS serão válidas é mandatória. Ex: regra de controle de banda mais permissivas durante o horário de almoço;

1.1.6.38. Deve possibilitar a definição de bandas distintas para download e upload;

1.1.6.39. A solução de SD-WAN deve prover estatísticas em tempo real a respeito da ocupação de banda (upload e download) e performance do health check (packet loss, jitter e latência);

1.1.6.40. A solução de SD-WAN deve suportar IPv6;

1.1.6.41. Deve possibilitar roteamento distinto a depender do grupo de usuário selecionado na regra de SD-WAN;

1.1.6.42. Suporte a configuração de alta disponibilidade Ativo/Passivo e Ativo/Ativo;

1.1.6.43. O SD-WAN deverá possuir serviço de Firewall Stateful;

1.1.6.44. A solução SD-WAN deverá fornecer criptografia AES de 128 bits ou AES de 256 bits em sua VPN;

1.1.6.45. A solução SD-WAN deverá simplificar a implantação de túneis criptografados de site para site;

1.1.6.46. Deve ser capaz de bloquear acesso às aplicações;

1.1.6.47. Deve suportar NAT dinâmico bem como NAT de saída;

1.1.6.48. Deve suportar balanceamento de tráfego por sessão e pacote;

1.1.6.49. As funcionalidades de SD-WAN podem ser fornecidas no NGFW ofertado ou em uma solução à parte, na mesma quantidade de equipamentos definida para os firewalls;

1.1.6.50. Em caso de composição de solução, a solução de SD-WAN deverá suportar tráfego compatível com a capacidade do equipamento de NGFW;

1.1.7. **Controle de Aplicações:**

1.1.7.1. Os dispositivos de proteção de rede deverão possuir a capacidade de reconhecer aplicações, independente de porta e protocolo;

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

1.1.7.3. Reconhecer pelo menos 2000 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;

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

1.1.7.5. Deve inspecionar o payload de pacote de dados com o objetivo de detectar assinaturas de aplicações conhecidas pelo fabricante independente de porta e protocolo;

1.1.7.6. Identificar o uso de táticas evasivas, ou seja, deve ter a capacidade de visualizar e controlar as aplicações e os ataques que utilizam táticas evasivas via comunicações criptografadas, tais como Skype e utilização da rede Tor;

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

1.1.7.8. Deve realizar decodificação de protocolos com o objetivo de detectar aplicações encapsuladas dentro do protocolo e validar se o tráfego corresponde com a especificação do protocolo. A decodificação de protocolo também deve identificar funcionalidades especificas dentro de uma aplicação;

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

1.1.7.10. Atualizar a base de assinaturas de aplicações automaticamente;

1.1.7.11. Os dispositivos de proteção de rede devem possuir a capacidade de identificar o

usuário de rede com integração ao Microsoft Active Directory, sem a necessidade de instalação de agente no Domain Controller, nem nas estações dos usuários;

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

1.1.7.13. Deve suportar vários métodos de identificação e classificação das aplicações, por pelo menos checagem de assinaturas e decodificação de protocolos;

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

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

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

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

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

1.1.7.19. Deve possibilitar a diferenciação e controle de partes das aplicações como por exemplo permitir o Hangouts e bloquear a chamada de vídeo;

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

1.1.7.21. Deve ser possível a criação de grupos dinâmicos de aplicações baseados em características das aplicações como: tecnologia utilizada nas aplicações (Client-Server, Browse Based, Network Protocol, etc);

1.1.7.22. Deve ser possível a criação de grupos dinâmicos de aplicações baseados em características das aplicações como: nível de risco da aplicação e categoria da aplicação;

1.1.7.23. Deve ser possível sobrescrever uma determinada ação para uma aplicação e para um filtro, sendo que os filtros devem ter a possibilidade de ser adicionados com base no comportamento da aplicação, tais como aplicações com alto consumo de banda, evasivas e com comportamento de botnet;

1.1.7.24. Deve ser possível editar uma aplicação associando parâmetros a serem analisados, tal como parâmetros associados a comandos na aplicação FTP;

1.1.8. **Prevenção de ameaças:**

1.1.8.1. Para proteção do ambiente contra-ataques, os dispositivos de proteção devem possuir módulo de IPS, Antivírus e Anti-Spyware integrados no próprio appliance de firewall;

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

1.1.8.3. Deverá possuir antivírus em tempo real, para ambiente de gateway Internet, integrado à plataforma de segurança para os seguintes protocolos: HTTP, SMTP, IMAP, POP3, CIFS e FTP;

1.1.8.4. Deve sincronizar as assinaturas de IPS, Antivírus, Anti-Spyware quando implementado em alta disponibilidade;

1.1.8.5. Deve implementar os seguintes tipos de ações para ameaças detectadas pelo IPS: permitir, permitir e gerar log, bloquear e quarentenar IP do atacante por um intervalo de tempo;

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

1.1.8.7. Deve ser possível a criação de políticas por usuários, grupos de usuários, IPs, redes ou zonas de segurança;

1.1.8.8. Exceções por IP de origem ou de destino devem ser possíveis nas regras ou assinatura a assinatura;

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

1.1.8.10. Deve permitir o bloqueio de vulnerabilidades;

1.1.8.11. Deve permitir o bloqueio de exploits conhecidos;

1.1.8.12. Deve incluir proteção contra-ataques de negação de serviços;

1.1.8.13. Ser imune e capaz de impedir ataques básicos como: Syn flood, ICMP flood, UDP flood, etc;

1.1.8.14. Detectar e bloquear a origem de portscans;

1.1.8.15. Bloquear ataques efetuados por worms conhecidos;

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

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

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

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

1.1.8.20. Identificar e bloquear comunicação com botnets;

1.1.8.21. Registrar na console de monitoração as seguintes informações sobre ameaças identificadas: o nome da assinatura ou do ataque, aplicação, usuário, origem e o destino da comunicação, além da ação tomada pelo dispositivo;

1.1.8.22. Deve possuir a função de proteção a resolução de endereços via DNS, identificando requisições de resolução de nome para domínios maliciosos de botnets conhecidas;

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

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

1.1.8.25. Possuir proteção contra downloads involuntários usando HTTP de arquivos executáveis e maliciosos;

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

1.1.8.27. Deve ser capaz de mitigar ameaças avançadas persistentes (APT), através de análises dinâmicas para identificação de malwares desconhecidos;

1.1.8.28. Dentre as análises efetuadas, a solução deve suportar antivírus, consulta na nuvem, emulação de código, sandboxing e verificação de call-back;

1.1.8.29. A solução deve analisar o comportamento de arquivos suspeitos em um ambiente controlado de sandbox. Deve ainda disponibilizar um relatório completo da análise realizada em cada arquivo submetido, o qual poderá ser baixado para auxiliar na análise forense de um evento;

1.1.8.30. Deve ser possível filtrar assinaturas com base no identificador CVE;

1.1.8.31. Deve ser possível criar uma assinatura de IPS utilizando o identificador CVE, bem como um “wildcard” do CVE para abranger mais de um identificador;

1.1.8.32. As assinaturas devem dispor de um resumo explicando o ataque associado, nível de severidade, impacto e uma possível recomendação, bem como deve vincular o(s) CVE(s) correspondente(s) quando aplicável;

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

1.1.8.34. Registrar na console de monitoramento as seguintes informações sobre ameaças identificadas: o nome da assinatura ou do ataque, aplicação, usuário, origem e o destino da comunicação, além da ação tomada pelo dispositivo;

1.1.9. **Filtro de URLs:**

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

1.1.9.2. Deve ser possível a criação de políticas por grupos de usuários, IPs, redes ou zonas de segurança;

1.1.9.3. Deve possuir a capacidade de criação de políticas baseadas na visibilidade e controle de quem está utilizando quais URLs através da integração com serviços de diretório, Active Directory e base de dados local;

1.1.9.4. A identificação pela base do Active Directory deve permitir SSO, de forma que os usuários não precisem logar novamente na rede para navegar pelo firewall;

1.1.9.5. Suportar a capacidade de criação de políticas baseadas no controle por URL e categoria de URL;

1.1.9.6. Possuir categorias de URLs previamente definidas pelo fabricante e atualizáveis a qualquer tempo;

1.1.9.7. Possuir pelo menos 70 categorias de URLs;

1.1.9.8. Deve possuir a função de exclusão de URLs do bloqueio;

1.1.9.9. Permitir a customização de página de bloqueio;

1.1.9.10. Permitir a restrição de acesso a canais específicos do Youtube, possibilitando configurar uma lista de canais liberado ou uma lista de canais bloqueados;

1.1.9.11. Deve bloquear o acesso a conteúdo indevido ao utilizar a busca em sites como Google, Bing e Yahoo, independentemente de a opção Safe Search estar habilitada no navegador do usuário;

1.1.9.12. Deve dispor de funcionalidade de prevenção contra phishing de credenciais analisando

quais estão sendo submetidas em sites externos, permitindo ainda bloquear ou alertar o usuário.

1.1.9.13. Deve possuir a possibilidade de definir uma quota diária de uso web baseado em categoria, sendo possível estipular a quota com base em, no mínimo, tempo de uso e volume de tráfego.

1.1.9.14. Deve ser possível bloquear tráfego HTTP POST, método utilizado para envio de informação a um determinado website.

1.1.9.15. Deve ser possível filtrar e remover Java applets, ActiveX e cookies do tráfego web inspecionado.

1.1.9.16. Deverá possuir em sua base de dados uma lista de bloqueio contendo URLs de certificados maliciosos;

1.1.9.17. Deve ser possível filtrar tráfego de vídeo baseado em categoria e até mesmo baseado no identificador de um canal do YouTube, por exemplo.

1.1.9.18. Deverá permitir além do Web Proxy explícito, suportar proxy Web transparente;

1.1.10. **Identificação de usuários:**

1.1.10.1. Deve incluir a capacidade de criação de políticas baseadas na visibilidade e controle de quem está utilizando quais aplicações através da integração com serviços de diretório, autenticação via LDAP, Active Directory, E-directory e base de dados local;

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

1.1.10.3. Deve possuir integração e suporte a Microsoft Active Directory para o sistema operacional Windows Server 2012 R2;

1.1.10.4. 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, suportando single sign-on. Essa funcionalidade não deve possuir limites licenciados de usuários;

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

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

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

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

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

1.1.10.10. Deve suportar Security Assertion Markup Language (SAML), agindo como um Provedor de Identidade (Indentity Provider - IDP) estabelecendo um relacionamento de confiança para autenticação segura de usuários tentando acessar um Provedor de Serviços (Service Provider -SP);

1.1.11. **Filtro de dados:**

1.1.11.1. Permitir identificar e opcionalmente prevenir a transferência de vários tipos de arquivos (MS Office, PDF, etc) identificados sobre aplicações (HTTP, FTP, SMTP, etc);

1.1.11.2. Suportar identificação de arquivos compactados ou a aplicação de políticas sobre o conteúdo desses tipos de arquivos;

1.1.11.3. Suportar a identificação de arquivos criptografados e a aplicação de políticas sobre o conteúdo desses tipos de arquivos;

1.1.11.4. Permitir identificar e opcionalmente prevenir a transferência de informações sensíveis, incluindo, mas não limitado a número de cartão de crédito, possibilitando a criação de novos tipos de dados via expressão regular.

1.1.12. **Geolocalização:**

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

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

1.1.13. **VPN**

1.1.13.1. Suportar VPN IPSec Site-to-Site;

1.1.13.2. A VPN IPSEC deve suportar criptografia 3DES, AES128, AES192 e AES256 (Advanced Encryption Standard);

1.1.13.3. A VPN IPSEc deve suportar Autenticação MD5, SHA1, SHA256, SHA384 e SHA512;

1.1.13.4. A VPN IPSEc deve suportar Diffie-Hellman Group 1, Group 2, Group 5 e Group 14, Group 15 até 21 e Group 27 até 32;

1.1.13.5. A VPN IPSEc deve suportar Algoritmo Internet Key Exchange (IKEv1 e v2);

1.1.13.6. A VPN IPSEc deve suportar Autenticação via certificado IKE PKI;

1.1.13.7. A VPN IPSec deve suportar Forward Error Correction (FEC);

1.1.13.8. Solução deverá ser capaz de prover uma arquitetura similar ao conceito de Auto Discovery VPN – ADVPN;

1.1.13.9. Deve possuir interoperabilidade com os seguintes fabricantes: Cisco, Check Point, Juniper, Palo Alto Networks, Fortinet, SonicWall;

1.1.14. **Item 3 - APPLIANCE FÍSICO PARA ANÁLISE DO TRÁFEGO DE DADOS**

1.1.14.1. Deverá estar devidamente licenciada para:

1.1.14.1.1. Suportar a coleta de, no mínimo, 200 GB de logs diários;

1.1.14.1.2. Permitir espaço de armazenamento de, no mínimo, 20 TB;

1.1.14.2. Deve suportar:

1.1.14.2.1. Pelo menos duas interfaces 10GE padrão RJ45 ou SFP+;

1.1.14.2.2. Suportar a configuração de RAID 0, 1, 5, 10, e 50 para os discos internos;

1.1.14.2.3. Possuir fonte de alimentação interna, redundante e hot-swap;

1.1.14.2.4. Na data da proposta, nenhum dos modelos ofertados poderão estar listados no site do fabricante em listas de end-of-life e end-of-sale;

1.1.14.3. Deve oferece um portal do cliente fácil de usar, permitindo acesso às capacidades seguras de SD-WAN, como monitoramento e modelos SD-WAN, políticas e objetos, painéis analíticos, visualizações e relatórios, auditoria e recursos adicionais, como documentação e links;

1.1.14.4. Suporte a definição de perfis de acesso ao console com permissão granular, como: acesso de gravação, acesso de leitura, criação de novos usuários e alterações nas configurações gerais;

1.1.14.5. Deve conter um assistente gráfico para adicionar novos dispositivos, usando seu endereço IP, usuário e senha;

1.1.14.6. A gerência centralizada deve vir acompanhada com solução de visualização de logs e geração de relatórios. Esta solução pode ser disponibilizada no mesmo equipamento de gerenciamento centralizado, ou fornecido em equipamento externo do mesmo fabricante;

1.1.14.7. Suporte a geração de relatórios de tráfego em tempo real, em formato de mapa geográfico;

1.1.14.8. Suporte a geração de relatórios de tráfego em tempo real, no formato de gráfico de bolhas;

1.1.14.9. Suporte a geração de relatórios de tráfego em tempo real, em formato de tabela gráfica;

1.1.14.10. Deve ser possível ver a quantidade de logs enviados de cada dispositivo monitorado;

1.1.14.11. Deve possuir mecanismos de remoção automática para logs antigos;

1.1.14.12. Permitir importação e exportação de relatórios

1.1.14.13. Deve ter a capacidade de criar relatórios no formato HTML, PDF, XML e CSV;

1.1.14.14. Deve permitir exportar os logs no formato CSV;

1.1.14.15. Deve permitir a geração de logs de auditoria, com detalhes da configuração efetuada, o administrador que efetuou a alteração e seu horário;

1.1.14.16. Os logs gerados pelos dispositivos gerenciados devem ser centralizados nos servidores da plataforma, mas a solução também deve oferecer a possibilidade de usar um servidor Syslog externo ou similar;

1.1.14.17. A solução deve ter relatórios predefinidos;

1.1.14.18. Deve permitir o envio automático dos logs para um servidor FTP externo a solução;

1.1.14.19. Deve ter a capacidade de personalizar a capa dos relatórios obtidos;

1.1.14.20. Deve permitir centralmente a exibição de logs recebidos por um ou mais dispositivos, incluindo a capacidade de usar filtros para facilitar a pesquisa nos logs;

1.1.14.21. Os logs de auditoria das regras e alterações na configuração do objeto devem ser exibidos em uma lista diferente dos logs relacionados ao tráfego de dados;

1.1.14.22. Deve ter a capacidade de personalizar gráficos em relatórios, como barras, linhas e tabelas;

1.1.14.23. Deve ter um mecanismo de "pesquisa detalhada" ou "Drill-Down" para navegar pelos relatórios em tempo real;

1.1.14.24. Deve permitir que os arquivos de log sejam baixados da plataforma para uso externo;

1.1.14.25. Deve ter a capacidade de gerar e enviar relatórios periódicos automaticamente;

1.1.14.26. Permitir a personalização de qualquer relatório pré-estabelecido pela solução, exclusivamente pelo Administrador, para adotá-lo de acordo com suas necessidades;

1.1.14.27. Permitir o envio por e-mail relatórios automaticamente;

1.1.14.28. Deve permitir que o relatório seja enviado por e-mail para o destinatário específico;

1.1.14.29. Permitir a programação da geração de relatórios, conforme calendário definido pelo administrador;

1.1.14.30. Permitir a exibição graficamente e em tempo real da taxa de geração de logs para cada dispositivo gerenciado;

1.1.14.31. Deve permitir o uso de filtros nos relatórios;

1.1.14.32. Deve permitir definir o design dos relatórios, incluir gráficos, adicionar texto e imagens, alinhamento, quebras de página, fontes, cores, entre outros;

1.1.14.33. Permitir especificar o idioma dos relatórios criados;

1.1.14.34. Gerar alertas automáticos via e-mail, SNMP e Syslog, com base em eventos especiais em logs, gravidade do evento, entre outros;

1.1.14.35. Deve permitir o envio automático de relatórios para um servidor SFTP ou FTP externo;

1.1.14.36. Deve ser capaz de criar consultas SQL ou similares nos bancos de dados de logs, para uso em gráficos e tabelas em relatórios;

1.1.14.37. Possibilidade de exibir nos relatórios da GUI as informações do sistema, como licenças, memória, disco rígido, uso da CPU, taxa de log por segundo recebido, total de logs diários recebidos, alertas do sistema, entre outros;

1.1.14.38. Deve fornecer as informações da quantidade de logs armazenados e as estatísticas do tempo restante armazenado;

1.1.14.39. Deve permitir aplicar políticas para o uso de senhas para administradores de plataforma, como tamanho mínimo e caracteres permitidos;

1.1.14.40. Deve permitir visualizar em tempo real os logs recebidos;

1.1.14.41. Deve permitir o encaminhamento de log no formato syslog;

1.1.14.42. Deve permitir o encaminhamento de log no formato CEF (Common Event Format);

1.1.14.43. Deve suportar a configuração Master / Slave de alta disponibilidade em camada 3;

1.1.14.44. Deve permitir gerar alertas de eventos a partir de logs recebidos;

1.1.14.45. A solução deve possuir garantia, suporte e atualizações ao software durante a vigência do contrato;

1.1.15. **Item 4 - APPLIANCE VIRTUAL DE GERENCIAMENTO CENTRALIZADO (SD-WAN e NGFW)**

1.1.15.1. A solução deve ser baseada em máquina virtual do mesmo fabricante da solução de NGFW e SD-WAN, e ter como objetivo gerenciar de modo centralizado todos os equipamentos a partir de uma única console de administração;

1.1.15.2. Deverá ser entregue em formato appliance virtual;

1.1.15.3. Deverá estar devidamente licenciada para:

1.1.15.3.1. Gerenciar, no mínimo, unidades (NGFW/SD-WAN ou Sistemas Virtuais) dos equipamentos da solução de NGFW e SD-WAN de forma simultânea;

1.1.15.3.2. Suportar a coleta de, no mínimo, GB de logs diários;

1.1.15.4. A solução deve suportar:

1.1.15.4.1. Deve ser compatível com os hypervisor VMWare 6.5 e superiores, Hyper-V 2016 e superiores, e KVM;

1.1.15.4.2. Não deverá existir limite para o número de vCPUs no appliance virtual;

1.1.15.4.3. Não deverá existir limite para a expansão da memória RAM no appliance virtual;

1.1.15.4.4. Deve suportar vMotion com o intuito de possibilitar alta disponibilidade da máquina virtual a nível de servidor físico. Caso esta funcionalidade não seja suportada, a solução deve ser entregue em alta disponibilidade;

1.1.15.5. Na data da proposta, nenhum dos modelos ofertados poderão estar listados no site do fabricante em listas de end-of-life e end-of-sale;

1.1.15.6. Deve suportar o conceito de multi-tenancy visando permitir a gestão de ambientes independentes uns dos outros a partir da mesma solução.

1.1.15.7. A solução deve permitir o uso de APIs RESTful para permitir a interação com portais

personalizados na configuração de objetos e políticas de segurança;

1.1.15.8. Deverá garantir a integridade do item de configuração, através de bloqueio de alterações, em caso de acesso simultâneo de dois ou mais administradores no mesmo ativo;

1.1.15.9. Permitir acesso concorrente de administradores, permitindo ainda que seja definida uma cadeia de aprovação das alterações realizadas;

1.1.15.10. Possibilitar a criação e administração de políticas de firewall, controle de aplicação, sistema de prevenção a intrusão (IPS – Intrusion Prevention System), antivírus, filtro de URL e SD-WAN;

1.1.15.11. Como parte da visibilidade dos dispositivos gerenciados centralmente, a solução deve ter visibilidade das verificações de saúde do link, desempenho da aplicação, utilização da largura de banda e conformidade com o nível de serviço definido;

1.1.15.12. Deve ter a capacidade de permitir o provisionamento de comunidades VPN e monitorar as conexões VPN de todos os dispositivos gerenciados a partir de uma única console, além de exibir sua localização geográfica em um mapa;

1.1.15.13. Permitir usar palavras chaves ou cores para facilitar identificação de regras;

1.1.15.14. Permitir localizar em quais regras um objeto (ex. computador, serviço etc.) está sendo utilizado;

1.1.15.15. Atribuir sequencialmente um número a cada regra de firewall, de NAT ou de QoS;

1.1.15.16. Permitir criação de regras que fiquem ativas em horário definido;

1.1.15.17. Permitir criação de regras com data de expiração;

1.1.15.18. Realizar o backup das configurações para permitir o retorno de uma configuração salva;

1.1.15.19. Possuir mecanismo de validação das políticas, avisando quando houver regras que ofusquem ou conflitem com outras, ou garantir que esta exigência seja plenamente atendida por meio diverso.

1.1.15.20. Possibilitar a visualização e comparação de configurações atuais, configuração anterior e configurações antigas;

1.1.15.21. Possuir um sistema de backup/restauração de todas as configurações da solução de gerência incluso assim como permitir ao administrador agendar backups da configuração em um determinado dia e hora;

1.1.15.22. Garantir que quando houver novas versões de software dos equipamentos, seja realizada a distribuição e instalação remota de maneira centralizada;

1.1.15.23. Permitir criar os objetos que serão utilizados nas políticas de forma centralizada;

1.1.15.24. Deve suportar a definição de perfis de acesso aao console com permissões granulares como: acesso de escrita, acesso de leitura, criação de usuários, alteração de configurações;

1.1.15.25. Deve suportar autenticação de administradores em base local e de modo remoto por meio de RADIUS, LDAP, TACACS+ e PKI.

1.1.15.26. Permitir criar na solução de gerência templates de configuração dos dispositivos com informações de DNS, SNMP, Configurações de LOG e Administração;

1.1.15.27. Permitir criar scripts personalizados, que sejam executados de forma centralizada em um ou mais dispositivos gerenciados com comandos de CLI dos mesmos;

1.1.15.28. Permitir criar, a partir da solução de gerência, VPNs entre os dispositivos gerenciados de forma centralizada, incluindo topologia (hub, spoke, dial-up), autenticações, chaves e métodos de criptografia;

1.1.16. **Dos requisitos de assistência técnica:**

1.1.16.1. Este serviço compreende o apoio técnico à distância dada pela assistência técnica da fabricante dos equipamentos e da CONTRATADA para solucionar problemas de ordem sistêmicos, problemas em equipamentos desta marca e problemas decorrentes de mau funcionamento de software.

1.1.16.2. Deverá existir acesso ao serviço de assistência técnica do fabricante e da CONTRATADA por telefone gratuito, email ou acesso seguro ao site, 24 (vinte e quatro) horas por dia, 7 (sete) dias por semana;

1.1.16.3. Os chamados junto ao fabricante deverão ser atendidos por engenheiros certificados e especializados do quadro de funcionários do fabricante, em inglês ou português;

1.1.16.4. No site do fabricante deverá existir ferramentas de auto-serviço que permitam o diagnóstico e sugestões de solução do problema quando possível;

1.1.16.5. Deverá existir acesso ao serviço de assistência técnica da CONTRATADA, por telefone gratuito, e-mail ou acesso ao site, 24 (vinte e quatro) horas por dia, 7 (sete) dias por semana;

1.1.16.6. Os chamados junto à CONTRATADA deverão ser atendidos por profissionais da CONTRATADA, em português e serão usados para abrir solicitações de informações, reportar incidentes ou esclarecer dúvidas quanto à utilização dos produtos e soluções fornecidos;

1.1.17. **Dos requisitos de atualização de software:**

1.1.17.1. Este serviço compreende também o acesso por parte do CONTRATANTE, às atualizações (versões e releases) de software dos equipamentos de rede disponibilizadas pelo fabricante;

1.1.17.2. Deverá ser garantida ao CONTRATANTE o direito para atualização dos firmwares, durante o período de garantia da solução, prestado pelo próprio fabricante, incluindo versões maiores (major releases), versões menores (minor releases), versões de manutenção (maintenance releases) e atualizações (updates) que forem disponibilizadas, tradicionalmente por meio de download automáticos a partir do site internet do fabricante.

1.1.18. **Dos requisitos de acesso à documentação:**

1.1.18.1. Este serviço compreende o acesso remoto por parte da CONTRATANTE às documentações técnicas dos equipamentos do fabricante;

1.1.18.2. A CONTRATANTE deverá ter acesso direto à base de dados de conhecimento do fabricante dos equipamentos que contenham especificações técnicas, informações, assistência e orientação para instalação, desinstalação, configuração e atualização de firmware e software, aplicação de correções (patches), diagnósticos, avaliações e resolução de problemas e demais atividades relacionadas à correta operação e funcionamento dos equipamentos;

1.1.19. **Garantia técnica do fabricante**

1.1.19.1. A CONTRATADA deverá descrever, em sua proposta, os termos da garantia técnica oferecida pelo fabricante, incluindo o Part Number da garantia ofertada e fornecendo também, em momento oportuno, o número de contrato individual (em nome da CONTRATANTE) junto ao fabricante.

1.1.19.2. O Termo de Garantia Técnica terá duração de até 60 (sessenta) meses.

1.1.19.3. Dos requisitos de reposição de equipamento defeituoso:

1.1.19.3.1. Este serviço compreende o envio de equipamento(s), componente(s), acessório(s) e dispositivo(s) novo(s), de primeiro uso e de modelo igual ou superior ao(s) danificado(s), às expensas do fabricante, às dependências da CONTRATANTE;

1.1.19.3.2. O contrato de reposição de peças deverá ser na modalidade 24 (vinte e quatro) horas por dia, 7 (sete) dias por semana, devendo o equipamento substituto ser entregue na CONTRATADA até o próximo dia útil (Next Business Day - NBD) após a abertura do chamado;

1.1.19.3.3. Para determinação do horário de início de cada chamado referente a substituição de equipamento defeituoso devem ser levadas em consideração as seguintes condições: caso a determinação de falha do hardware pela fabricante tenha ocorrido antes das 15h, horário local da Brasília-DF, de segunda a sexta-feira (excluindo os feriados), o equipamento deverá ser enviado no mesmo dia para chegar no próximo dia útil. Para as solicitações feitas depois das 15h, o fabricante deverá entregar o equipamento substituto até o segundo dia útil após o a determinação da falha;

1.1.19.3.4. O equipamento substituto passará à propriedade da CONTRATANTE, devendo o mesmo ser imediatamente incluído no contrato de manutenção vigente em substituição ao equipamento danificado;

1.1.19.3.5. O equipamento substituído deverá ser devolvido ao fabricante às expensas do mesmo, em até 5 (cinco) dias úteis.

1.1.19.3.6. A CONTRATANTE deverá ter acesso à Central de Assistência Técnica (TAC) do fabricante para abertura dos chamados, bem como para acompanhar e gerenciar os casos quando necessário. Esse acesso deverá ser provido 24 (vinte e quatro) horas por dia, 7 (sete) dias por semana através de login/senha individual;

1.1.19.3.7. A CONTRATANTE deverá ter a opção de abrir os chamados junto a fabricante com o intermédio da CONTRATADA;

1.1.20. **Instalação e Configuração**

1.1.20.1. A instalação e configuração deverão ser executadas por técnicos da CONTRATADA, certificados pelo fabricante dos equipamentos fornecidos, sendo necessária a apresentação de documentação original que comprove a validade desta(s) certificação(ões) enquanto durar o contrato, que pode ser solicitada a qualquer momento.

1.1.20.2. A CONTRATADA deverá apresentar um Projeto Executivo que deve ser composto por um documento do tipo SOW (em tradução livre, escopo de trabalho) e que deve conter, no mínimo, as seguintes informações:

1.1.20.2.1. Objetivo;

1.1.20.2.2. Plano de gerenciamento de mudanças, detalhando passo-a-passo o escopo da migração;

1.1.20.2.3. Cronograma das atividades que serão realizadas, com os prazos estimados e as diretrizes para cada atividade;

1.1.20.2.4. Projeto lógico de configuração e diagrama de interconexão dos equipamentos;

1.1.20.2.5. Nome(s) do(s) gerente(s) de projetos e do(s) técnico(s) responsável(is) pela execução;

1.1.20.2.6. Lista de todos os elementos instalados contendo:

1.1.20.2.6.1. Nome e endereço(s) IP do equipamento;

1.1.20.2.6.2. Equipamento e porta na qual o equipamento foi conectado;

1.1.20.2.6.3. Local de instalação (prédio, andar, sala);

1.1.20.2.6.4. Número de série do equipamento.

1.1.20.3. A instalação refere-se à instalação física e lógica, nos locais expostos pela contratante, também abrangendo:

1.1.20.3.1. Sua disposição e conectorização no rack de telecomunicações;

1.1.20.3.2. A instalação dos transceivers em seus módulos/slots;

1.1.20.3.3. Sua interconexão aos switches, roteadores, ADCs e servidores de rede, entre outros;

1.1.20.3.4. Suas configurações de interfaces, endereçamento e serviços de rede, além de outras configurações necessárias ou constantes no Projeto de Instalação;

1.1.20.3.5. Sua identificação e a identificação de todas as suas conexões.

1.1.20.4. O SOW deverá ser entregue pela CONTRATADA em até 10 (dez) dias úteis após a assinatura contrato, o qual deverá ser aprovado pela CONTRATANTE; os serviços não poderão ser iniciados antes da apresentação e assinatura de concordância de ambas as partes.

1.1.20.5. Todos os parâmetros a serem configurados deverão ser alinhados entre as partes em reuniões de pré-projeto, podendo estas ser realizadas presencialmente, por telefone ou via conferência web, devendo a CONTRATADA sugerir as configurações de acordo com normas e boas práticas, cabendo à CONTRATANTE a sua aceitação expressa ou recusa nos casos de não atendimento das condições estabelecidas;

1.1.20.6. As configurações deverão seguir fielmente a padronização previamente estabelecida pela CONTRATANTE;

1.1.20.7. A CONTRATADA deverá fazer análise do ambiente tecnológico atual, devendo a CONTRATANTE fornecer todas as informações necessárias sobre a infraestrutura instalada, de modo que se possa garantir a continuidade dos serviços prestados pelo órgão durante a migração, mantendo a disponibilidade dos serviços básicos e dos demais serviços de retaguarda (aplicativos, correio eletrônico, banco de dados, Internet, etc.);

1.1.20.8. A substituição da infraestrutura de firewall instalada no local deve ser planejada e executada de modo que não cause interrupções e paralisações não programadas, ou qualquer outro tipo de transtorno ao correto funcionamento do ambiente operacional da CONTRATANTE.

1.1.20.9. Caso não seja possível manter a disponibilidade dos serviços básicos no momento da instalação, as manobras de implantação deverão ser realizadas durante janela de manutenção agendada previamente, em horários que não comprometam o funcionamento das atividades do órgão, inclusive aos sábados, domingos e feriados;

1.1.21. Ao término da instalação deverá ser fornecido um relatório detalhado (as-built) contendo todas as configurações realizadas, com comentários sobre os principais comandos e as justificativas das opções de parametrização de modo a facilitar a posterior administração da solução e a continuidade de seu funcionamento; a critério da CONTRATANTE, poderá ser elaborado um único as-built contendo todas as informações de todos os equipamentos e softwares instalados/configurados.

ANEXO I - B - PROPOSTA DE PREÇOS

(EMITIR EM PAPEL TIMBRADO DA EMPRESA)

PROPOSTA DE PREÇOS

Objeto: Contratação de solução de firewall contemplando serviços de instalação e suporte técnico com garantia pelo período de 60 meses, com vistas a atender às necessidades do Ministério da Justiça e Segurança Pública - MJSP.

Os dados da nossa empresa são:

a) Razão Social: _____;

b) CNPJ (MF) nº: _____;[

c) Representante (s) legal (is) com poderes para assinar o contrato: _____;

d) CPF: _____ RG: _____ _____-_____;

e) Inscrição Estadual nº: _____;

f) Endereço: _____;

g) Fone: _____ Fax: _____ E-mail: _____;

h) CEP: _____; e

i) Cidade: _____ Estado: _____.

j) Banco:_____Conta Corrente:_____Agência:_____;

k) Contato: _____ Fone/Ramal: _____.

À

SUBSECRETARIA DE TECNOLOGIA DA INFORMAÇÃO E COMUNICAÇÕES/SE/MJSP

Esplanada dos Ministérios, Bloco "T", sala 308, Sede

Brasília – DF

CEP 70064-900.

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

Grupo	Item	Descrição	Unidade	QTDE	Valor unitário máximo (R$)	Valor total máximo (R$)
1	1	FIREWALL TIPO I - APPLIANCE FÍSICO	Unitário	04	R$	R$
	2	FIREWALL TIPO II - APPLIANCE FÍSICO	Unitário	05	R$	R$
	3	APPLIANCE FÍSICO PARA ANÁLISE DO TRÁFEGO DE DADOS	Unitário	01	R$	R$
	4	APPLIANCE VIRTUAL DE GERENCIAMENTO CENTRALIZADO	Unitário	01	R$	R$
	VALOR TOTAL DA CONTRATAÇÃO				**R$**	

Dados da Empresa
Endereço completo (com CEP):
Telefones:
E-mail:
Dados Bancários(nº Banco, nº agência, nº cc):
Declarações
Validade da Proposta (mínimo 60 dias), conforme o artigo 64, § 3° da Lei 8.666/93.:
Declaramos que nos preços propostos estão incluídos todos os custos e despesas de qualquer natureza, incidentes sobre os objetos desta proposta.
Declaramos total conhecimento e concordância dos termos do edital do pregão e dos seus anexos.
Assinatura
Local e data:
Nome do Representante Legal:
Identidade do Representante Legal:

_____

Assinatura do Representante Legal

ANEXO I - C - MODELO DE ORDEM DE SERVIÇO – O.S.

ORDEM DE SERVIÇO N°		DATA:	
		HORA:	
1. IDENTIFICAÇÃO DO SOLICITANTE			
Nome:	E-mail:		
Fone/Ramal:	Assinatura do Solicitante:		
2. SERVIÇO A EXECUTAR			

EMPRESA RESPONSÁVEL:	
LOCAL/REFERÊNCIA:	
HORÁRIO/DIA P/ EXECUÇÃO:	
OBS.:	

3. AUTORIZAÇÃO P/ EXECUÇÃO DOS SERVIÇOS SEM ACOMPANHAMENTO DO SETOR SOLICITANTE			
Autorizo o pessoal abaixo a realizar os serviços acima nos termos definidos em Contrato.			
Data ___/__/___	Hora ___:___ hs	Ass. e carimbo solicitante:	

4. FUNCIONÁRIO (S) RESPONSÁVEL (IS) PELO SERVIÇO A SEREM EXECUTADOS		
	Nome do funcionário	Cargo/função
1		
2		
3		

5. MATERIAL EMPREGADO			
Item	Descrição	Unidade/Tipo	Quantidade
1			
2			
3			
4			

6. DATA E HORÁRIO DO INÍCIO E TÉRMINO DOS SERVIÇOS (desconsiderar intervalos)			
Data de início do serviço	Hora	Data de término do serviço	Hora
___/__/___	___:___ hs	___/__/___	___:___ hs

7. ACEITE DO SERVIÇO		
Declaro que o serviço acima solicitado, foi executado, considerando aceito o serviço		
Data ___/__/___	Hora ___:___ hs	Ass. e carimbo solicitante:

ANEXO I - D - MODELO DE DECLARAÇÃO DE VISTORIA

DECLARAÇÃO DE VISTORIA

(EMITIR EM PAPEL TIMBRADO DA EMPRESA)

Pela presente, declaramos conhecer e compreender por inteiro o teor do PREGÃO ELETRÔNICO nº ___/2023, cujo objeto é a Contratação de solução de firewall contemplando serviços de instalação e suporte técnico com garantia pelo período de 60 meses, com vistas a atender às necessidades do Ministério da Justiça e Segurança Pública - MJSP.

Empresa:_____

C.N.P.J.(MF):_____Tel/Fax:_____

Endereço:_____

Nome do Representante: _____

Endereço Eletrônico (e-mail): _____

Brasília-DF, ...de.....de 20...

_____

Representante da Empresa

Carteira de Identidade - Órgão Emissor

Declaro que o Representante da empresa acima identificada visitou os locais de execução dos serviços.

Brasília-DF, ...de.....de 20....

_____

Nome

Carteira de Identidade - Órgão Emissor

ANEXO I - E - TERMO DE CIÊNCIA

INTRODUÇÃO			
Visa obter o comprometimento formal dos empregados da CONTRATADA diretamente envolvidos no projeto sobre o conhecimento da declaração de manutenção de sigilo e das normas de segurança vigentes na Instituição.			
IDENTIFICAÇÃO			
Contrato N°:			
Objeto:			
Contratante:			
Gestor do Contrato:		Matr.:	
Contratada:		CNPJ:	
Preposto da Contratada:		CPF:	
Por este instrumento, os funcionários abaixo-assinados declaram ter ciência e conhecer o teor do Termo de Compromisso de Manutenção de Sigilo e as normas de segurança vigentes na Contratante.			
CIÊNCIA			
CONTRATADA – Funcionários			
_____	_____		
<Nome>	***<Nome>***		

Matrícula: <*Matr.*>	**Matrícula: <*Matr.*>**
_____ **<*Nome*>** **Matrícula: <*Matr.*>**	_____ **<*Nome*>** **Matrícula: <*Matr.*>**
_____ **<*Nome*>** **Matrícula: <*Matr.*>**	_____ **<*Nome*>** **Matrícula: <*Matr.*>**

ANEXO I - F - TERMO DE COMPROMISSO

O <NOME DO ÓRGÃO>, sediado em <ENDEREÇO>, CNPJ n° <CNPJ>, doravante denominado CONTRATANTE, e, de outro lado, a <NOME DA EMPRESA>, sediada em <ENDEREÇO>, CNPJ n° <CNPJ>, doravante denominada CONTRATADA;
CONSIDERANDO que, em razão do CONTRATO N.º XX/20XX 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 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:

Cláusula Primeira – DO 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, 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 18/11/2011 e os Decretos 7.724, de 16/05/2012 e 7.845, de 14/11/2012, que regulamentam os procedimentos para acesso e tratamento de informação classificada em qualquer grau de sigilo.

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

Cláusula Terceira – 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;

Cláusula Quarta – 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.

Cláusula Quinta – DOS 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 expresso e prévio 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, mesmo 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.

Cláusula Sexta – DA 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.

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

Cláusula Oitava – 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 disponibilizadas para a CONTRATADA, serão incorporados a este TERMO, passando a fazer dele parte integrante, para todos os fins e efeitos, recebendo também a mesma proteção descrita para as informações iniciais disponibilizadas, sendo necessário a formalização de TERMO aditivo ao CONTRATO PRINCIPAL;
VIII – Este TERMO não deve ser interpretado como criação ou envolvimento das Partes, ou suas filiadas, nem em obrigação de divulgar INFORMAÇÕES para a outra Parte, nem como obrigação de celebrarem qualquer outro acordo entre si.

Cláusula Nona – DO FORO
A CONTRATANTE elege o foro da <CIDADE DA CONTRATANTE>, onde está localizada a sede da CONTRATANTE, para dirimir quaisquer dúvidas originadas do presente TERMO, com renúncia expressa a qualquer outro, por mais privilegiado que seja.

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

DE ACORDO

CONTRATANTE	**CONTRATADA**
_____ *<Nome>* Matrícula: *<Matr.>*	_____ *<Nome>* *<Qualificação>*
Testemunhas	
Testemunha 1	**Testemunha 2**
_____ *<Nome>* *<Qualificação>*	_____ *<Nome>* *<Qualificação>*

ANEXO I - G - MODELO DE DECLARAÇÃO DE RENÚNCIA À VISTORIA

DECLARAÇÃO DE RENÚNCIA À VISTORIA

(EMITIR EM PAPEL TIMBRADO DA EMPRESA)

Pela presente, declaramos RENUNCIAR a vistoria técnica aos locais e as instalações para prestação dos serviços constantes do objeto do PREGÃO ELETRÔNICO nº ___/2023, bem como seus anexos, pelo que aceitamos seus termos e comprometemo-nos a observá-los integralmente. Declaramos, outrossim, NÃO ter visitado o local dos serviços a serem executados, motivo esse que não poderei alegar o desconhecimento de fatos evidentes à época da vistoria para solicitar qualquer alteração do valor do contrato que vier a celebrar.

Empresa:_____

C.N.P.J.(MF):_____Tel/Fax:_____
Endereço:_____

Nome do Representante: _____

Endereço Eletrônico (e-mail): _____

Brasília-DF, ...de.....de 202...

_____

Representante da Empresa

Carteira de Identidade - Órgão Emissor

ANEXO I - H - MODELO DE PLANO DE INSERÇÃO

INTRODUÇÃO	
O Plano de Inserção descreverá as atividades de alocação de recursos e preparação das condições necessárias para a contratada iniciar o fornecimento da Solução de TIC.	
1 – IDENTIFICAÇÃO	
Contratada	
Nº. do Contrato	
Área Requisitante da Solução	
Gestor do Contrato	
Fiscal Requisitante	
Fiscal Técnico	
Fiscal administrativo	
2 – VISÃO GERAL DO PROJETO	
Justificativa da Contratação	
Objetivos da Contratação	
3 – METODOLOGIA DE TRABALHO	
Forma de Comunicação	
Forma de Encaminhamento das Ordens de Serviço	
Modelo de execução do contrato	
4 – EXECUÇÃO DO CONTRATO	
Ferramentas de Controle	

Id	Ferramenta	Controles	

DOCUMENTAÇÃO MÍNIMA EXIGIDA	
Documento	**Finalidade do documento**

PAPEIS E RESPONSABILIDADES			
Id	**Papel**	**Responsabilidades**	

PARTES INTERESSADAS		
Id	**Área/Órgão/Setor**	**Impacto**

FATORES CRÍTICOS DE SUCESSO	

PREMISSAS DA CONTRATAÇÃO	

RESTRIÇÕES DA CONTRATAÇÃO		

ENTREGAS PLANEJADAS				
Id	**Entrega**	**Marco**	**Duração**	**Data de Entrega**

INFRAESTRUTURA A SER DISPONIBILIZADA À CONTRATADA			
Id	**Recurso**	**Início**	**Fim**

CRITÉRIO DE ACEITAÇÃO – MÉTRICA E PERIODICIDADE	
Métrica 1	

Indicador de Qualidade	
Mínimo aceitável	
Métrica	
Ferramentas	
Periodicidade Aferição	
Métrica "N"	
Indicador de Qualidade	
Mínimo aceitável	
Métrica	
Ferramentas	
Periodicidade Aferição	

RESULTADOS ESPERADOS		
Id	**Entrega**	**Benefícios**

5 – INSTRUÇÕES COMPLEMENTARES

6 - CIÊNCIA

Fiscais do Contrato		
Fiscal Técnico	Fiscal Requisitante	Fiscal Administrativo
_____	_____	
<Nome> **Matrícula: <*Matr.*>**	***<Nome>*** **Matrícula: <*Matr.*>**	***<Nome>*** **Matrícula: <*Matr.*>**

Gestor do Contrato
_____ <Nome> Matrícula: <*Matr.*>

Contratada
_____ <Nome> CPF/CNPJ: <...>

Brasília-DF, ...de.....de 202...

ANEXO I - I - MODELO DE PLANO DE FISCALIZAÇÃO

INTRODUÇÃO	
O Plano de Fiscalização descreverá as atividades de acompanhamento e fiscalização da execução do contrato de fornecimento da Solução de TIC.	
1 – IDENTIFICAÇÃO DO CONTRATO	
Contrato nº:	
Contratante	
Área Requisitante da Solução	
Fiscal Requisitante	
Fiscal Técnico	
Fiscal Administrativo	
Gestor do Contrato	
Contratada	
CNPJ	
2 – PROCEDIMENTOS DE TESTE DE INSPEÇÃO	
CRITÉRIO DE ACEITAÇÃO – MÉTRICA E PERIODICIDADE	
Métrica 1	
Indicador de Qualidade	
Mínimo aceitável	
Métrica	
Ferramentas	
Periodicidade Aferição	
3 – CONFIGURAÇÃO/CRIAÇÃO DE FERRAMENTAS PARA IMPLANTAÇÃO E ACOMPANHAMENTO DE INDICADORES	

4 – ELABORAÇÃO/REFINAMENTO DAS LISTAS DE VERIFICAÇÃO E DOS ROTEIROS DE TESTE		
FISCAIS DO CONTRATO		
Fiscal Técnico	Fiscal Requisitante	Fiscal Administrativo
_____ ***<Nome>*** **Matrícula: <*Matr.*>**	_____ ***<Nome>*** **Matrícula: <*Matr.*>**	_____ ***<Nome>*** **Matrícula: <*Matr.*>**
GESTOR DO CONTRATO		
_____ ***<Nome>*** **Matrícula: <*Matr.*>**		
CONTRATADA		
_____ ***<Nome>*** **CPF/CNPJ: <...>**		
Brasília-DF, ...de.....de 202...		

ANEXO I - J - MODELO DE DECLARAÇÃO DE SUSTENTABILIDADE AMBIENTAL

DECLARAÇÃO DE SUSTENTABILIDADE AMBIENTAL

(EMITIR EM PAPEL TIMBRADO DA EMPRESA)

Empresa:_____

C.N.P.J.(MF):_____Tel/Fax:_____
Endereço:_____

Nome do Representante: _____

Endereço Eletrônico (e-mail): _____

Declaro, sob as penas da Lei nº 6.938/1981, na qualidade de proponente do procedimento licitatório, sob a modalidade Pregão Eletrônico nº _____, instaurado pelo Processo de nº _____, que atendemos aos critérios de qualidade ambiental e sustentabilidade socioambiental, respeitando as normas de proteção do meio ambiente.

Estou ciente da obrigatoriedade da apresentação das declarações e certidões pertinentes dos órgãos competentes quando solicitadas como requisito para habilitação e da obrigatoriedade do cumprimento integral ao que estabelece o art. 6º e seus incisos, da Instrução Normativa nº 01, de 19 de janeiro de 2010, do Ministério do Planejamento, Orçamento e Gestão – MPOG.

Por ser a expressão da verdade, firmamos a presente.

Brasília-DF, ...de.....de 20...

_____

Representante da Empresa

Carteira de Identidade - Órgão Emissor

Ministério da Justiça e Segurança Pública
Secretaria-Executiva
Coordenação de Infraestrutura de TIC

HISTÓRICO DE REVISÕES			
Data	Versão	Descrição	Autor
25/04/2023	1.0	Finalização da primeira versão do documento	Equipe de Planejamento da Contratação
22/05/2023	2.0	Finalização da segunda versão (após revisão da CGL)	Equipe de Planejamento da Contratação

ESTUDO TÉCNICO PRELIMINAR DA CONTRATAÇÃO

1. INFORMAÇÕES BÁSICAS

1.1 Número do processo: 08006.000158/2023-36

2. INTRODUÇÃO

2.1. Conforme previsto no artigo 11 da INSTRUÇÃO NORMATIVA SGD/ME Nº 01, DE 4 DE ABRIL DE 2019, a elaboração dos Estudos Técnicos Preliminares da Contratação serve essencialmente para definição e especificação das necessidades de negócio e tecnológicas, e dos requisitos necessários e suficientes à escolha da solução de TIC, contendo de forma detalhada, motivada e justificada, inclusive quanto à forma de cálculo, o quantitativo de bens e serviços necessários para a sua composição. A análise comparativa de soluções, deve considerar, além do aspecto econômico, os aspectos qualitativos em termos de benefícios para o alcance dos objetivos da contratação.

2.2. É na elaboração dos dos Estudos Técnicos Preliminares da Contratação que diversos aspectos devem ser levantados com maior profundidade para que os gestores se certifiquem, de que através de uma necessidade da área de negócio, claramente definida, há condições de atendê-la, tendo como premissa que os riscos de atendê-la são gerenciáveis e os resultados pretendidos com a contratação valem o preço estimado inicialmente, além de embasar a elaboração do Termo de Referência ou o Projeto Básico, que somente é elaborado se a contratação for considerada viável.

2.3. A presente análise tem por objetivo demonstrar a viabilidade técnica e econômica da aquisição de equipamentos de rede de dados para a modernização e expansão da capacidade, incluindo novos ativos de camada de acesso, contemplando os serviços de instalação e suporte técnico com garantia pelo período de 60 meses para atendimento das necessidades do Ministério da Justiça e Segurança Pública (MJSP).

3. DESCRIÇÃO DA NECESSIDADE

3.1. VISÃO GERAL DO MINISTÉRIO DA JUSTIÇA E SEGURANÇA PÚBLICA E SEUS OBJETIVOS ESTRATÉGICOS:

3.1.1. O Ministério da Justiça e Segurança Pública (MJSP), órgão da Administração Pública Federal, tem, dentre outras, as competências para atuar no "combate ao tráfico de drogas e crimes conexos, inclusive por meio da recuperação de ativos que financiem ou sejam resultado dessas atividades criminosas", na "prevenção e combate à corrupção, à lavagem de dinheiro e ao financiamento do terrorismo", na "coordenação de ações para combate a infrações penais em geral, com ênfase em corrupção, crime organizado e crimes violentos", na "coordenação e promoção da integração da segurança pública no território nacional, em cooperação com os entes federados", na "promoção da integração e da cooperação entre os órgãos federais, estaduais, distritais e municipais e articulação com os órgãos e as entidades de coordenação e supervisão das atividades de segurança pública" e, por fim, no "desenvolvimento de estratégia comum baseada em modelos de gestão e de tecnologia que permitam a integração e a interoperabilidade dos sistemas de tecnologia da informação dos entes federativos".

3.1.2. Atualmente o MJSP, é composto de várias unidades em sua estrutura:

- **Órgãos de assistência direta e imediata ao Ministro** (Assessorias Especiais, Gabinete do Ministro, Secretaria Executiva e Consultoria Jurídica);
- **Órgãos específicos singulares** (Secretaria Nacional de Justiça - SENAJUS, Secretaria Nacional do Consumidor - SENACON, Secretaria Nacional de Políticas sobre Drogas e Gestão de Ativos - SENAD, Secretaria Nacional de Segurança Pública - SENASP, Secretaria Nacional de Políticas Penais - SENAPPEN, Secretaria Nacional de Assuntos Legislativos - SAL, Secretaria de Acesso à Justiça - SAJU, Polícia Federal - PF, Polícia Rodoviária Federal - PRF);
- **Órgãos colegiados** (Conselho Federal Gestor do Fundo de Defesa dos Direitos Difusos - CFDD, Conselho Nacional de Combate à Pirataria e Delitos contra a Propriedade Intelectual - CNPCP, Conselho Nacional de Políticas sobre Drogas - CONAD, Conselho Nacional de Política Criminal e Penitenciária - CNPCP, Conselho Nacional de Segurança Pública e Defesa Social - CNSP, Conselho Gestor do Fundo Nacional de Segurança Pública - CFNSP, Conselho Nacional de Imigração - CNI e Comitê Nacional para os Refugiados - CNR);
- **Entidade vinculada** (Conselho Administrativo de Defesa Econômica - CADE e Autoridade Nacional de Proteção de Dados - ANPD).

3.1.3. Como pode ser observado, a estrutura do MJSP é bastante considerável e complexa, possuindo diversas áreas de atuação que merecem tratamento diferenciado e proporcional às suas especificidades, tanto do ponto de vista de suas dimensões, quanto ao grau de sensibilidade e sigilo que

as áreas necessitam para o desempenho de suas atividades.

3.1.4. Alguns temas sensíveis podem ser destacados de cada um dos Órgãos específicos singulares e de acordo com as competências do Ministério com base no decreto nº 11.348, de 01 de janeiro de 2023, como por exemplo:

Art. 14. À Secretaria Nacional de Justiça compete:

...

II - coordenar, em parceria com os órgãos da administração pública, a Estratégia Nacional de Combate à Corrupção e à Lavagem de Dinheiro - Enccla e outras ações do Ministério relacionadas com o enfrentamento da corrupção, da lavagem de dinheiro e do crime organizado transnacional;

III - coordenar a negociação de acordos e a formulação de políticas de cooperação jurídica internacional, civil e penal, e a execução dos pedidos e das cartas rogatórias relacionadas com essas matérias;

IV - coordenar as ações relativas à recuperação de ativos;

...

Art. 17. À Secretaria Nacional do Consumidor compete:

I - formular, promover, supervisionar e coordenar a política nacional de proteção e defesa do consumidor;

II - integrar, articular e coordenar o Sistema Nacional de Defesa do Consumidor;

...

X - receber e encaminhar consultas, denúncias ou sugestões apresentadas por consumidores, entidades representativas ou pessoas jurídicas de direito público ou privado;

...

Art. 20. À Secretaria Nacional de Políticas sobre Drogas e Gestão de Ativos compete:

I - assessorar e assistir o Ministro de Estado quanto às políticas sobre drogas relacionadas com a prevenção do uso indevido, a atenção e a reinserção social de usuários e dependentes de drogas, a redução da oferta e a repressão da produção não autorizada e do tráfico ilícito de drogas;

...

Art. 24. À Secretaria Nacional de Segurança Pública compete:

I - assessorar o Ministro de Estado: na articulação, na proposição, na formulação, na implementação, no acompanhamento e na avaliação de políticas, de estratégias, de planos, de programas e de projetos de segurança pública e defesa social;

II - estimular, propor, promover e coordenar a integração da segurança pública e defesa social no território nacional, em cooperação com os entes federativos, incluídas as organizações governamentais e não governamentais;

III - implementar, manter e modernizar redes de integração de banco de dados e de sistemas nacionais de informações de segurança pública e defesa social;

IV - coordenar e planejar as atividades da Força Nacional de Segurança Pública;

V - participar da elaboração de propostas de legislação em matérias relativas à segurança pública e defesa social;

VI - monitorar os riscos que possam impactar a implementação de políticas de segurança pública e defesa social e a consecução de seus objetivos;

VII - atuar no ciclo de gestão de recursos da segurança pública sob sua responsabilidade, em atividades de natureza técnica e finalística, em especial na propositura e na avaliação de políticas públicas e em seus instrumentos de implementação;

VIII - coordenar as atividades relacionadas à gestão dos recursos de segurança pública;

...

Art. 31. À Secretaria Nacional de Políticas Penais cabe exercer as competências estabelecidas nos art. 71 e art. 72 da Lei nº 7.210, de 11 de julho de 1984 - Lei de Execução Penal, e, especificamente:

I - planejar e coordenar a política nacional de serviços penais;

...

IV - prestar apoio técnico aos entes federativos quanto à implementação dos princípios e das regras da execução penal;

...

XII - promover a gestão da informação penitenciária e consolidar, em banco de dados nacional, informações sobre os sistemas penitenciários federal e dos entes federativos.

...

Art. 38. À Secretaria Nacional de Assuntos Legislativos compete:

I - promover o processo de articulação com o Congresso Nacional nos assuntos de competência do Ministério, observadas as competências dos órgãos que integram a Presidência da República;

II - providenciar o atendimento às consultas e aos requerimentos formulados, além de acompanhar a tramitação legislativa dos projetos de interesse do Ministério;

III - participar do processo de interlocução com os Governos estaduais, distrital e municipais, com as assembleias legislativas estaduais, com a Câmara Legislativa do Distrito Federal e com as câmaras municipais nos assuntos de competência do Ministério, com o objetivo de assessorá-los em suas iniciativas e de providenciar o atendimento às consultas formuladas, observadas as competências dos órgãos que integram a Presidência da República;

IV - auxiliar as comissões e grupos especiais de juristas constituídos pelo Ministro de Estado, com o objetivo de elaborar e consolidar leis; e

V - organizar e auxiliar as áreas temáticas nas consultas públicas de temas de competência do Ministério.

Art. 40. À Secretaria de Acesso à Justiça compete:

I - promover políticas públicas de modernização, aperfeiçoamento, transformação digital e democratização do acesso à justiça e à cidadania, inclusive no âmbito de plataformas digitais;

...

IV - promover ações para o aperfeiçoamento do sistema e da política de justiça, em articulação com os órgãos e as entidades dos Poderes Executivo e Judiciário e com o Ministério Público, a Defensoria Pública, a Ordem dos Advogados do Brasil, os órgãos e as agências internacionais e as organizações da sociedade civil;

...

VII - promover ações relacionadas ao Sistema de Justiça que contribuam para a redução da violência contra as mulheres, a população LGBTQIA+, os povos indígenas e as comunidades tradicionais e para o aprimoramento do Sistema de Justiça.

Art. 43. À Polícia Federal cabe exercer as competências estabelecidas no § 1º do art. 144 da Constituição, e, especificamente:

I - apurar infrações penais contra a ordem política e social ou em detrimento de bens, serviços e interesses da União ou de suas entidades autárquicas e empresas públicas, além de outras infrações cuja prática tenha repercussão interestadual ou internacional e exija repressão uniforme, conforme previsto em lei;

II - prevenir e reprimir o tráfico ilícito de entorpecentes e drogas e o contrabando e o descaminho de bens e de valores, sem prejuízo da ação fazendária e de outros órgãos públicos, nas suas áreas de competência;

...

VI - acompanhar e instaurar inquéritos relacionados com direitos humanos e conflitos agrários ou fundiários e aqueles deles decorrentes, quando se tratar de crime de competência federal, além de prevenir e reprimir esses crimes.

Art. 58. À Polícia Rodoviária Federal cabe exercer as competências estabelecidas no § 2º do art. 144 da Constituição, no art. 20 da Lei nº 9.503, de 23 de setembro de 1997 - Código de Trânsito Brasileiro, no Decreto nº 1.655, de 3 de outubro de 1995, e, especificamente:

I - planejar, coordenar e executar o policiamento, a prevenção e a repressão de crimes nas rodovias e estradas federais e nas áreas de interesse da União;

II - exercer os poderes de autoridade de trânsito nas rodovias e nas estradas federais;

III - executar o policiamento, a fiscalização e a inspeção do trânsito e do transporte de pessoas, cargas e bens;

IV - planejar, coordenar e executar os serviços de prevenção de acidentes e de salvamento de vítimas nas rodovias e estradas federais;

...

3.1.5. Merecem também ser destacados os órgãos colegiados do Ministério, que atuam em temas sensíveis, e de importância nacional, como por exemplo o Conselho Nacional de Combate à Pirataria e Delitos contra a Propriedade Intelectual (CNPCP). Esse órgão é a instância que trata do assunto pirataria no Brasil, sendo responsável pela aplicação de abordagens e metodologias inéditas para o tratamento da questão, elaborando diretrizes para a formulação e proposição de plano nacional para o combate à pirataria, à sonegação fiscal dela decorrente e aos delitos contra a propriedade intelectual.

3.1.6. Outro importante órgão colegiado é o Conselho Nacional de Políticas sobre Drogas - CONAD, sendo o órgão máximo brasileiro que regulamenta e pesquisa o uso de substâncias químicas e determina quais são drogas e quais não são e sua classificação. Este conselho também realiza campanhas de esclarecimento quanto às drogas e projetos como o de dano mínimo.

3.1.7. Destaca-se também o Conselho Nacional de Política Criminal e Penitenciária - CNPCP, que preconiza a implementação, em todo o território nacional, de uma nova política criminal e principalmente penitenciária a partir de periódicas avaliações do sistema criminal, criminológico e penitenciário, bem como a execução de planos nacionais de desenvolvimento quanto às metas e prioridades da política a ser executada.

3.1.8. O Ministério possui também em sua estrutura o Conselho Nacional de Segurança Pública e Defesa Social - CNSP, que tem o objetivo de propor diretrizes para prevenir e conter a violência e a criminalidade no País. O CNSP está previsto na lei nº 13.675, de 11 de junho de 2018, que instituiu o Sistema Único de Segurança Pública (SUSP) e a Política Nacional de Segurança Pública e Defesa Social (PNSPDS), o órgão será composto por representantes da União, dos estados, Distrito Federal, municípios e sociedade civil.

3.1.9. De acordo com o alinhamento ao plano estratégico institucional 2020-2023, o MJSP possui os seguintes objetivos estratégicos:

- **OE-PEI-01 -**Fortalecer o enfrentamento à criminalidade, com enfoque em crimes violentos, organizações criminosas, corrupção e lavagem de dinheiro, inclusive com atuação na faixa de fronteira;
- **OE-PEI-02 -** Promover o acesso à justiça e proteger os direitos do cidadão;
- **OE-PEI-03 -** Aperfeiçoar a coordenação estratégica e a integração dos órgãos de segurança pública;
- **OE-PEI-04 -** Aperfeiçoar a gestão do sistema prisional l;
- **OE-PEI-05 -** Promover a gestão e a alienação do produto de crimes;
- **OE-PEI-06 -** Ampliar a escala e a efetividade das ações de defesa da concorrência e do consumidor;
- **OE-PEI-07 -** Gerir políticas referentes aos povos indígenas;
- **OE-PEI-08 -** Aprimorar mecanismos de gestão do conhecimento e da preservação e difusão da memória arquivística nacional;
- **OE-PEI-09 -** Promover a valorização e o desenvolvimento dos servidores;
- **OE-PEI-10 -** Aprimorar e integrar a gestão e a governança institucional;
- **OE-PEI-11 -**Fortalecer e ampliar a estrutura e os serviços de TIC (Finalidade: Avaliar se os serviços de TIC considerados estratégicos estão em

operação conforme acordado, quais sejam: 1) E-mail; 2) SEI; 3) mj.gov.br; 4) Rede Local; e 5) Acesso à Internet.);

3.1.20. Para que todos os órgãos da estrutura do Ministério possam atuar de maneira eficiente e eficaz, e com os recursos necessários para o pleno desenvolvimento de suas atividades, **são necessários mecanismos tecnológicos que sejam capazes de gerar valor e entregar as informações necessárias, de forma a permitir a produção de conhecimento útil e tempestivo à tomada de decisão**, seja em nível estratégico, tático ou operacional.

3.1.21. Uma unidade crucial para que o MJSP cumpra suas funções e missão é a Subsecretaria de Tecnologia da Informação e Comunicações - STI, criada por meio do DECRETO Nº 11.348, DE 1º DE JANEIRO DE 2023, que é responsável direta pelo planejamento, coordenação e execução das atividades relacionadas com o SISP no âmbito do Ministério, além de articulação com os órgãos centrais, elaborando e consolidando planos e programas de sua competência:

> ...
>
> Art. 12. À Subsecretaria de Tecnologia da Informação e Comunicação compete:
>
> I - planejar, coordenar e supervisionar a execução das atividades relacionadas com o Sistema de Administração dos Recursos de Tecnologia da Informação no âmbito do Ministério;
>
> II - promover a articulação com os órgãos centrais do sistema federal referido no inciso I e informar e orientar os órgãos integrantes da estrutura do Ministério e da entidade a ele vinculada quanto ao cumprimento das normas estabelecidas;
>
> III - elaborar e consolidar os planos e os programas das atividades de sua área de competência e submetê-los à decisão superior; e
>
> IV - acompanhar e promover a avaliação de projetos e atividades, no âmbito de sua competência.
>
> ...

3.1.32. A busca por evolução dos serviços de informática vem resultando em mudanças no perfil de tráfego de suas aplicações internas e externas, exigindo uma revisão da arquitetura de ativos de segurança atualmente em funcionamento, requerendo dos equipamentos maiores taxas de transmissão e maior poder de processamento.

3.1.33. Tal implementação requer uma maior interatividade da parte de procedimentos de configuração, desempenho e qualidade, bem como a total interoperabilidade, visando uniformização dos recursos como um todo.

3.1.34. Nesse sentido, a adoção de tecnologias modernas e inovadoras, como solução de Firewall de alto desempenho, deixaram de ser uma tendência e passaram a ser uma realidade na Administração Pública Federal – APF, que deve estar alinhada às modernas e eficientes práticas do mercado.

3.1.35. Os Firewalls possuem funções fundamentais em uma rede de TIC, podendo evitar que pacotes indesejados e prejudiciais tenham acesso à rede interna e, portanto, às informações e recursos em posse da mesma. Assim também, os "filtros" implementados por esses equipamentos evitam que *hosts* internos tenham acesso a domínios e informações que não condizem com a política de segurança da rede.

3.1.36. Além disso, é um dos mecanismo de segurança utilizados para proteger a rede computacional contra acessos indevidos, através da identificação, análise, bloqueio, isolamento e tratamento das rotas de rede utilizadas pelo usuários e pelos sistemas computacionais sob responsabilidade do MJSP, além do gerenciamento das atividades que envolvam ameaças relacionadas à configuração de rotas. Com isso, diminui-se o risco de acessos indevidos aos sistemas do MJSP enquanto o desempenho geral da rede é otimizado através do gerenciamento mais eficaz do roteamento dos ativos de TI do órgão.

3.1.37. Existem muitas vantagens em manter uma solução de *Firewall* com poder de processamento robusto, com altas taxas de transmissão e em um ambiente de TIC totalmente coberto com suporte e garantia, cabendo destaque para os listados abaixo:

a) Manutenção da integridade dos dados;

b) Maior controle do acesso às informações;

c) Manutenção da integridade da rede;

d) Melhora a segurança da rede;

e) Proteção contra malwares;

3.1.41. Além dessas vantagens consideradas essenciais, deve-se observar os riscos que o MJSP correrá caso opte em não utilizar uma solução de *Firewall*:

a) **Comprometimento dos dados** - trata-se de um incidente de segurança em que dados pessoais e/ou informações privadas e sigilosas podem ser expostos publicamente ou a terceiros sem autorização.

b) **Sujeição aos ataques dos cibercriminosos** - atualmente, com o alto fluxo de informação, gera-se um aumento significativo de ataques, espionagem e roubo de dados cibernéticos. Ou seja, a maior conectividade trouxe com ela a maior exposição a risco e Malwares diversos, completamente dispersos pela rede ou tecnicamente planejados para atacar órgãos específicos.

c) **Comprometimento da integridade da rede** - acessos indevidos à rede podem ocorrer, afetando assim a garantia da integridade dos dados e informações essenciais.

d) **Descontrole da autorização de acesso às informações** - As políticas de segurança coincidem com as regras aplicadas no firewall, ditam as regras de permissões e proibições de acesso que um *firewall* deve implementar.

3.1.42. Em virtude dos aspectos abordados, é de fundamental importância a abordagem e entendimento da arquitetura atual da solução de firewall e sua topologia aplicada à rede do MJSP, assim como o entendimento do escopo dos projetos de segurança em infraestrutura realizados ao longo dos anos.

3.2. ATUAL ARQUITETURA DA SOLUÇÃO DE FIREWALL NA TOPOLOGIA DE REDE

3.2.1. Na atual conjuntura, a estrutura de Tecnologia da Informação do Ministério vem passando por mudanças de disposição física em suas unidades, o que tem provocado a necessidade de aquisição de equipamentos, processos de automatização e alta disponibilidade que suportem este dinamismo.

3.2.2. A atual plataforma de ativos de rede do MJSP, formada pela rede do núcleo central, é composta por três camadas:

- Camada Central;
- Camada de Distribuição e
- Camada de Acesso.

3.2.3. A Camada Central abriga os switches do tipo core, que são equipamentos de alto desempenho, os quais devem ser robustos para suportarem grande tráfego de pacotes. A arquitetura desta camada deve proporcionar alto grau de disponibilidade, capacidade, redundância e resiliência.

3.2.4. A Camada de Distribuição é responsável pela interconexão entre a camada Central e de Acesso, sendo responsável pela concentração dos pacotes

de dados oriundos da Camada de Acesso para encaminhamento à Camada Central. A Camada de Distribuição controla o fluxo do tráfego da rede usando políticas e determina domínios de broadcast, realizando funções de roteamento entre VLANs, além de conectar os pontos de acesso da rede sem fio (APs).

3.2.5. A Camada de Acesso é a camada de switches mais próxima das máquinas dos usuários, sendo que os equipamentos ativos desta camada captam os pacotes de dados oriundos das máquinas de usuários, impressoras, telefones VoIP e outros equipamentos da ponta, e os encaminham à Camada de Distribuição. O principal propósito da camada de acesso é fornecer um meio de conectar dispositivos à rede e controlar quais têm permissão de comunicação na rede.

3.2.6. Dentre os projetos de aquisição de equipamentos para essas camadas, o de reestruturação e modernização de ativos de rede da Camada Central (Core), se relaciona diretamente com funcionamento da solução de firewall, pois trouxe inovação para os Data Centers do MJSP (Primário e Secundário), e ainda teve por objetivo a inserção da estrutura *Spine-Leaf,* a qual consiste em uma espinha dorsal formada pelo SPINE e os LEAFs, que servem de entrada dos diversos subsistemas de rede. A arquitetura proposta forma um único *Fabric,* que funciona de forma redundante em camada 3 (três) e com a utilização de roteamento dinâmico interno ao Data Center.

3.2.7. Nesse contexto, a topologia da Camada Central (Leaf Serviços) e topologia de Firewall implantada nos Data Centers do MJSP (Primário e Secundário) são divididas conforme imagem abaixo:

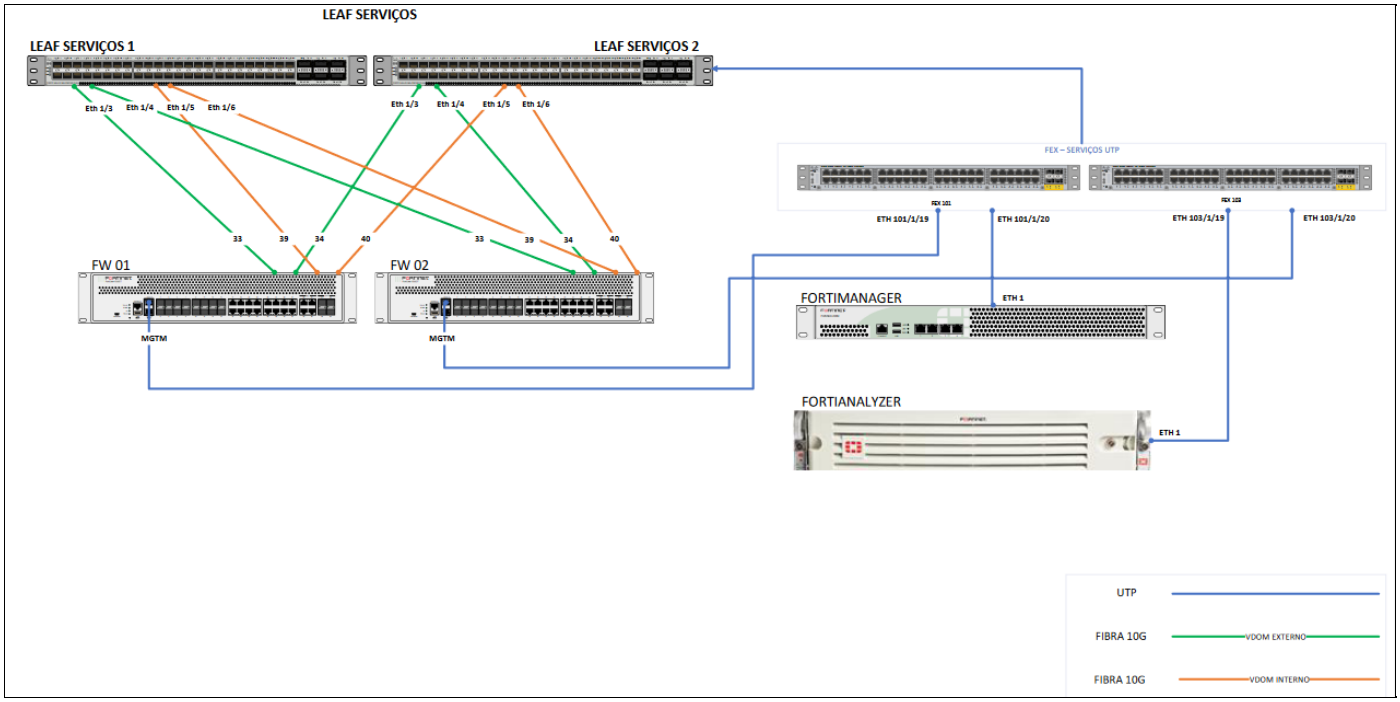

Figura 1 – Arquitetura da solução de firewall na topologia de rede

3.2.8. Na figura acima, encontra-se a solução de Firewall ligada ao Leaf de Serviços (que é a estrutura responsável por receber instalações de equipamentos relacionados aos serviços diversos de TIC, como Wireless, SERPRO, Load Balance, Videoconferência, etc.) com velocidade de link de 10 Gbps.

3.2.9. A estrutura de firewall do Ministério é composta pelos equipamentos instalados nos 2 (dois) Data Centers do MJSP, além de equipamentos localizados nas 05 (cinco) Penitenciárias Federais (Catanduvas (PR), Campo Grande (MS), Mossoró (RN), Porto Velho (RO) e Brasília (DF)). Importante salientar, que, a topologia de redes difere das implantada no MJSP e CICCN, tendo em vista que a rede de uma Penitenciária federal é menos complexa, utilizando somente switches de distribuição para ligar os equipamentos de firewall. Então, em cada Penitenciária foi instalado um Appliance Físico, contemplando assim 5 "caixas" desses ativos no total.

3.2.10. A tabela abaixo apresenta o quantitativo atual de equipamentos que atende a todo o MJSP (Data Centers Primário, Secundário e Penitenciárias):

Solução de Firewall Atual		
Descrição	**Tipo**	**Quantidade**
Appliance de Firewall para uso nos Datacenters do MJSP	Unidade	04
Appliance de Firewall para uso nas Penitenciárias Federais	Unidade	05
Appliance para análise do tráfego de dados para uso nos Datacenters do MJSP	Unidade	01
Appliance de gerenciamento centralizado para uso nos Datacenters do MJSP	Unidade	01

3.2.11. Esses equipamentos de Firewall foram adquiridos por meio do processo 08006.001190/2016-18, tendo o suporte e garantia prazos de expiração em 28/06/2023, o que requer atenção especial com a elaboração de pesquisas e análises de soluções voltadas ao atendimento da necessidade, considerando inicialmente algumas soluções como, manter a solução atual (renovando apenas o suporte e garantia), utilizar uma solução de firewall em software livre ou realizar a aquisição de uma solução por completo, sendo essas análises realizadas ainda neste estudo.

3.2.12. Outro fator importante em adquirir uma solução robusta e com alto desempenho, é a necessidade observada de utilizar links de internet redundantes em algumas unidades do MJSP, destacando-se as Penitenciárias Federais.

3.2.13. Atualmente, para a interligação das Penitenciárias Federais à infraestrutura do Ministério, é utilizada a tecnologia MPLS (Multiprotocol Label Switching, ou "Comutação de Rótulos Multiprotocolo") que é uma tecnologia de rede usada, em geral, por empresas a fim de conectar suas unidades remotas, ou por provedores de internet para a segmentação de tráfego de layer 2 e layer 3. A empresa contratada para fornecimento do MPLS é a Telebrás, sendo que o contrato prevê dupla abordagem de links, ou seja, um por fibra óptica outro por meio sem fio. Apesar disso, diversos incidentes na rede foram registrados nos anos de 2022 e agora em 2023, ocasionando que sistemas importantes para a segurança pública ficassem indisponíveis.

3.2.14. O quantitativo de incidentes foram relacionados e podem ser observados na imagem abaixo:

Incidentes TELEBRÁS			
Localidades	Anos		
Rótulos de Linha	2022	2023	Total Geral
Fortigate Forca Nacional Gama	37	35	72
PFBSB_CORE	23	31	54
Roteador_Telebras_Concentrador_MPLS_MJ_Brasilia	7	18	25
Roteador_Telebras_Concentrador_MPLS_MJ_Brasilia_Secundario	8	15	23
SW_CORE_CAMPO_GRANDE_172.22.16.10	18	34	52
SW_CORE_CATANDUVAS_172.22.80.10	31	34	65
SW_CORE_MOSSORO_172.22.144.10	63	58	121
SW_CORE_PORTO_VELHO_172.22.208.10	36	32	68
Total Geral	223	257	480

3.2.15. Sendo assim, percebe-se que foram 480 (quatrocentos e oitenta) incidentes relacionados à solução de internet/MPLS da Telebrás, contando todas as unidades do MJSP. Esta situação de recorrentes indisponibilidades traz transtornos e perdas consideráveis incalculáveis, levando em conta todos os sistemas e serviços que estão afetados e deixando de ser prestados à população. Cabe destacar que muitos dos incidentes ocorrem em decorrência da Telebrás terceirizar a última milha do link, tendo em vista a capilaridade da operadora não chegar em algumas localidades.

3.2.16. Dito isso, a equipe de planejamento da contratação está analisando a possibilidade de implementação, em um futuro próximo, da tecnologia SD-WAN (WAN definida por software), com o objetivo de aumentar a disponibilidade, a velocidade do link e diminuir os custos com links MPLS. Vários benefícios podem ser elencados da SD-WAN em comparação com o MPLS, como por exemplo:

a) As **SD-WANs não dependem de hardware especializado**. As MPLS requerem a configuração de roteadores especializados para encaminhar pacotes corretamente. As SD-WANs podem ser executadas usando qualquer hardware de rede.

b) As **SD-WANs não têm limites de largura de banda inerentes** Como as conexões MPLS são mais ou menos definidas (a menos que sejam reconfiguradas), há um limite rígido sobre quanta capacidade pode ser provisionada em uma conexão MPLS de uma só vez . As conexões SD-WAN podem adicionar capacidade conforme necessário, combinando várias conexões e aproveitando a conectividade mais rápida disponível.

c) As **SD-WANs são independentes do provedor de serviços** As MPLS exigem que as organizações usem a mesma operadora em todos os sites conectados por WAN porque as conexões MPLS precisam ser configuradas em roteadores físicos na rede adjacente. As conexões SD-WAN são executadas pela internet comum; qualquer provedor pode ser compatível com uma conexão SD-WAN.

d) O **roteamento SD-WAN é mais flexível** A SD-WAN pode aproveitar várias opções de conectividade, incluindo conexões de internet de banda larga, linhas privadas e 5G. Ela pode direcionar o tráfego e o failover entre todas as opções de conectividade disponíveis. Os serviços de MPLS normalmente exigem conexões de linha privada dedicadas do provedor de serviços.

e) As **SD-WANs se integram mais facilmente com a nuvem** Conectar-se à nuvem via MPLS é um serviço especializado oferecido por alguns provedores de serviços MPLS para alguns provedores de nuvem. Com a MPLS, a conexão com a nuvem requer a construção de uma rota direta para a infraestrutura desse provedor de nuvem.

3.2.17. Diante dos motivos expostos e das necessidades apresentadas, se faz necessário uma análise sobre as possíveis soluções no mercado para a modernização e expansão da capacidade, incluindo novos appliances físicos de firewall, além de contemplar os serviços de instalação, suporte técnico e garantia.

4. ÁREA REQUISITANTE

Área Requisitante	Responsável
Coordenação-Geral de Infraestrutura e Serviços de TIC	Rodrigo Albernaz Bezerra

5. NECESSIDADES DE NEGÓCIO

ID	Principais necessidades de negócio
1	Reestruturar e modernizar a arquitetura de firewall do Ministério, provendo aquisição de equipamentos robustos e confiáveis.
2	Suportar o aumento no número de usuários e prestação de serviços a estes de maneira rápida, segura e eficaz.
3	Suportar a crescente demanda por conectividade de rede, internet e acesso a sistemas internos que estão hospedados em nuvem.
4	Garantir a continuidade dos negócios do MJSP por meio de melhorias, apoio técnico e manutenções da solução a ser adquirida.
5	Prover a mitigação de impactos para as áreas de negócios decorrentes de problemas no funcionamento dos equipamentos de segurança
6	Aumentar a segurança por meio da ativação novas funcionalidade técnicas à nova solução
7	Prover solução de firewall eficiente com a atualização dos ativos deste Ministério.

Tabela 1 **- Necessidades de negócio**

6. NECESSIDADES TECNOLÓGICAS

ID	Principais necessidades tecnológicas
1	Manter a integridade da rede em conjunto com a integridade dos dados
2	Permitir gestão centralizada de todos dos dispositivos de segurança e borda da rede das unidades remotas (Penitenciárias), otimizando o monitoramento do uso da rede local do MJSP, agilizando a recuperação de desastres (disaster recovery).
3	Assegurar estabilidade da rede e dos sistemas frente à ampliação da infraestrutura de rede existente nas Unidades do MJSP
4	Manter a compatibilidade tecnológica do parque de ativos de segurança em funcionamento na rede do Ministério
5	Prover maior proteção contra malwares;
6	Atender prontamente ao aumento de novos serviços online e em nuvem prestados pelo MJSP e na melhoria do acesso à Internet nas Unidades Penitenciárias

7	Garantir a continuidade da conexão da VPN entre o MJSP e diversas localidades e serviços
8	Assegurar disponibilidade entre links de internet em unidades do MJSP

***Tabela 2* - Necessidades tecnológicas**

7. DEMAIS REQUISITOS NECESSÁRIOS E SUFICIENTES À ESCOLHA DA SOLUÇÃO DE TIC

ID	Demais requisitos necessários e suficientes à escolha da solução de TIC
1	Prover segurança da informação ao acessar os equipamentos e serviços do Ministério.
2	Arquitetura tecnológica de segurança compatível com a utilizada atualmente.

***Tabela 3* - Demais requisitos**

8. ESTIMATIVA DA DEMANDA – QUANTIDADE DE BENS E SERVIÇOS

Solução de Firewall		
Descrição	**Tipo**	**Quantidade**
Appliance de Firewall para uso nos Datacenters do MJSP	Unidade	04
Appliance de Firewall para uso nas Penitenciárias Federais	Unidade	05
Appliance para análise do tráfego de dados para uso nos Datacenters do MJSP	Unidade	01
Appliance de gerenciamento centralizado para uso nos Datacenters do MJSP	Unidade	01

Tabela 4 - Estimativa da Demanda

9. LEVANTAMENTO DAS SOLUÇÕES

9.1. **Solução 1 - Contratação de serviço de garantia e suporte técnico para a solução atual.**

9.1.1. O presente cenário tem o objetivo de analisar a possibilidade da contratação dos serviços de manutenção e suporte para os equipamentos existentes verificando sua viabilidade.

9.2. **Solução 2 - Contratação de toda uma solução em Software Livre.**

9.2.1. O presente cenário tem o objetivo de demonstrar a contratação por meio da instalação, configuração e mudança de todo o ambiente de firewall para uma solução de software livre.

9.3. **Solução 3 - Contratação de toda uma nova solução de firewall contemplando serviços de instalação e suporte técnico com garantia pelo período de 60 meses.**

9.3.1. O presente cenário tem o objetivo de demonstrar a solução por meio da aquisição e modernização por completo da solução de firewall dos atuais ambientes do MJSP. O objetivo principal da análise é a possibilidade de aquisição de novos appliances, expandindo e reestruturando arquitetura de segurança do MJSP, de forma a dar continuidade às melhorias com uma topologia moderna, escalável e de alto desempenho.

10. ANÁLISE COMPARATIVA DE SOLUÇÕES

10.1 **Solução 1 - Contratação de serviço de garantia e suporte técnico para a solução atual.**

10.1.1. Atualmente, o Ministério da Justiça e Segurança Pública possui uma solução de Firewall adquirida através do Processo 08006.001190/2016-18, composta por 04 (quatro) equipamentos do modelo FortiGate 1500D, sendo que 02 (dois) desses equipamentos estão instalados no datacenter primário e 02 (dois) instalados no datacenter secundário do MJSP, além de 05 (cinco) equipamentos do modelo FortiGate 500D, instalado em cada uma das cinco Penitenciárias que compõem o Sistema Penitenciário Federal, localizadas em Catanduvas (PR), Campo Grande (MS), Mossoró (RN), Porto Velho (RO) e Brasília (DF).

10.1.2. Também faz parte da solução atual, 01 (um) equipamento de Gerenciamento de Firewall, modelo FortiManager 200D, responsável por controlar todos os produtos adquiridos, permitindo o gerenciamento centralizado de todos os equipamentos de Firewall.

10.1.3. Por fim, a solução atual também possui 01 (um) equipamento de relatório de Firewall, modelo FortiAnalyzer 1000E, responsável por coletar e armazenar os dados gerados pelos equipamentos de Firewall, permitindo realizar a análise do tráfego de dados a partir de relatórios customizados.

10.1.4. O fabricante dos equipamentos já estabeleceu datas específicas para descontinuidade de todos os produtos que compõem a solução atual (*end of life*) do MJSP, conforme consta na tabela 5.

Modelo	Data de descontinuidade	Link SEI
FortiGate 1500D	31/12/2026	23806105
FortiGate 500D	08/05/2023	23806064
FortiManager 200D	03/12/2024	23806087
FortiAnalyzer 1000E	22/03/2025	23806042

Tabela 5 - Data de descontinuidade (end of life) dos equipamentos que compõem a solução de Firewall atual

10.1.5. Diante disso, observa-se que os equipamentos FortiGate 500D, FortiAnalyzer 1000E e FortiManager 200D atingirão o *end of life* em breve, estando, dessa forma, desatualizados tecnologicamente. Logo, há um comprometimento na contratação de garantia e suporte para esses equipamentos, caracterizando-se como uma solução sem sustentabilidade a médio e longo prazo.

10.1.6. Cabe destacar, que além do fato dos referidos equipamentos se encontrarem em estado de obsolescência, estando descontinuados pelo fabricante, ainda é importante considerar as Boas Práticas e Acórdãos que tratam sobre o tema para embasar de forma positiva ou negativa o cenário proposto.

10.1.7. Nessa linha, existem as BOAS PRÁTICAS, ORIENTAÇÕES E VEDAÇÕES PARA CONTRATAÇÃO DE ATIVOS DE TIC - Versão 4 (Link), do Departamento de Segurança da Informação, Serviços e Infraestrutura de Tecnologia da Informação do STI/MP, que cita a contratação de manutenção dos ativos de TIC fora de garantia como mais onerosa para a Administração Pública, assim como define o ciclo de vida para esses equipamentos:

"....

1.2.2. Tal procedimento se justifica pelo fato de que, de forma geral a contratação, a posteriori, de serviços de ***manutenção para ativos fora de garantia, usualmente é mais onerosa para a Administração*** *do que quando o bem é adquirido com garantia para toda sua vida útil. (grifo nosso)*

"....

1.4. ORIENTAÇÕES ESPECÍFICAS SOBRE CICLO DE VIDA

1.4.5. SERVIDORES DE REDE, APLICAÇÃO, EQUIPAMENTOS DE BACKUP, ARMAZENAMENTO, **SEGURANÇA**, ENTRE OUTROS

mínimo de **5 (cinco) anos** para fins de posicionamento da tecnologia e de garantia de funcionamento.*(grifo nosso)*

10.1.8. Assim como a apreciação da Egrégia Corte de Contas que exarou entendimento no sentido de condenara prática de atualizações tecnológicas em detrimento da aquisição de novos equipamentos. Para ilustrar cita-se o Acórdão TCU nº 2400/2006 que assim discorreu sobre os serviços de atualização tecnológica e suporte técnico:

"Acórdão TCU n. 2400/2006 – Plenário

"...

2.9.2.4 .... do ponto de vista técnico, o fato de existir garantia para os equipamentos que sofrerem atualização nos mesmos níveis que os prestados a equipamentos novos não garante vantagem técnica ao upgrade. Pelo contrário, não se pode esperar que um servidor em gabinete desmontado e remontado em um rack com substituição de quase todos os componentes (ver listagem dos componentes que serão substituídos à fl. 70 do anexo 2), com a permanência de alguns componentes antigos, possa ter menor probabilidade de falha que um equipamento novo que, dependendo do fornecedor, pode ser montado e testado em fábrica. A garantia não diminui o risco de falha e necessidade de substituição de componentes (mais provável no caso do upgrade do que no caso de aquisição de novos servidores), caso em que os equipamentos, mesmo que por pouco tempo, permaneceriam indisponíveis. "

"...

10.1.9. Uma observação importante também, é quanto aos equipamentos FortiGate 1500D, com data de descontinuidade em 31/12/2026, pois trata-se de equipamentos que na topologia atual (ligados nos Datacenter primário e secundário) já não atendem satisfatoriamente, conforme mencionado Nota Técnica 23657316:

"...

Diante do exposto, verifica-se que a capacidade do equipamento de Firewall do núcleo central do MJSP encontra-se próximo do seu limite máximo, representando um risco à segurança das informações sob responsabilidade do MJSP e à disponibilidade dos seus serviços.

Além disso, é possível verificar que a ferramenta FortiAnalyzer também está operando próximo ao seu limite, contribuindo para aumentar os riscos à segurança da informação do MJSP.

Cabe ressaltar que esses fatores decorrem do crescimento da rede do MJSP, que passou a disponibilizar mais serviços através da internet e do aumento de usuário que utilizam a internet para acessar tais serviços.

Ao avaliar os resultados obtidos pela presente análise, constata-se a necessidade da substituição da solução atual de Firewall por uma de maior porte, para atender tanto às necessidade atuais do MJSP, quanto às expectativas de crescimento de sua rede computacional, de modo a garantir o correto controle sobre os acessos aos dados armazenados e trafegados pelo MJSP e evitar possíveis indisponibilidade de seus serviços.

"...

10.1.10. Cabe destacar, que ao longo dos últimos anos, houve um crescimento expressivo da infraestrutura do Ministério devido à grande quantidade de projetos e aplicações que entraram em produção. Além disso, houve um aumento na utilização da nuvem e sua gama de aplicativos colaborativos, fato que sobrecarrega o tráfego, e sua capacidade de análise pelas ferramentas de segurança.

10.1.11. Essa sobrecarga nas soluções de segurança geram um consumo excessivo de recursos dos equipamentos, gerando a impossibilidade de analisar o tráfego de rede por completo, resultando em falhas de conexão à rede interna e externa do MJSP, além do risco de acessos indevidos a informações sensíveis sob a responsabilidade do MJSP. Sendo assim, os equipamentos de firewalls estão frequentemente entrando em um estado chamado de "*conserve mode*", que é uma proteção do próprio sistema pelo consumo excessivo de processamento. Importante salientar que o estado de "*conserve mode*", impacta o funcionamento geral da rede, gerando incidentes massivos para os usuários.

10.1.12. Para avaliar o desempenho destes Firewalls, foram realizadas duas medições, uma no dia 23/11/2022 às 9:00 horas (Figura 1) e outra no dia 29/11/2022 às 16:00 horas (Figura 2). Em ambas as medições, é possível verificar que o consumo médio de CPU alcança, respectivamente, 85,4% e 81,9% do limite da ferramenta.

10.1.13. Em uma situação de maior acesso aos serviços do MJSP ou no caso de um possível ataque cibernético, esse consumo pode alcançar valores que ultrapassam o limite da solução, podendo resultar em indisponibilidades de sistemas ou acesso indevido aos dados sob responsabilidade do MJSP, conforme imagens extraídas da solução:

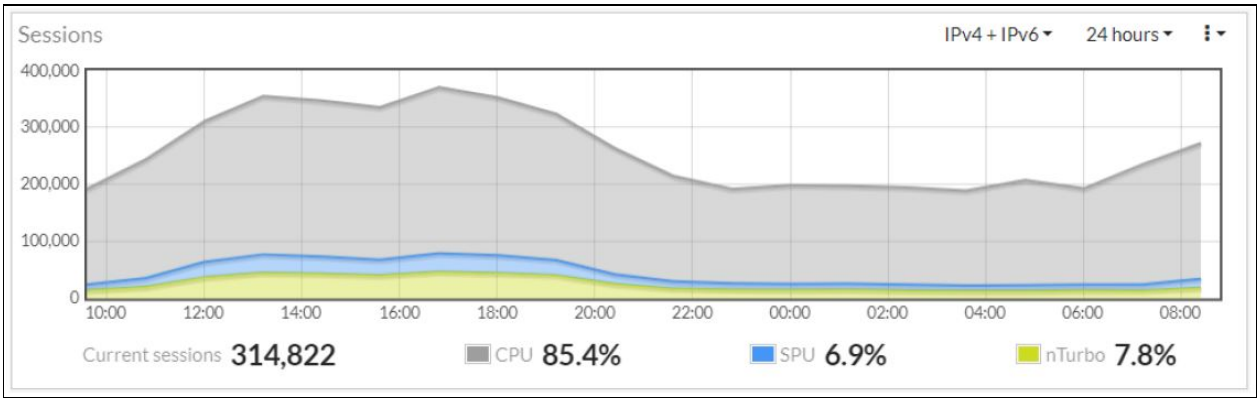

Figura 2 – Número de conexões e consumo de CPU e SPU do Firewall do núcleo central – Medição 01

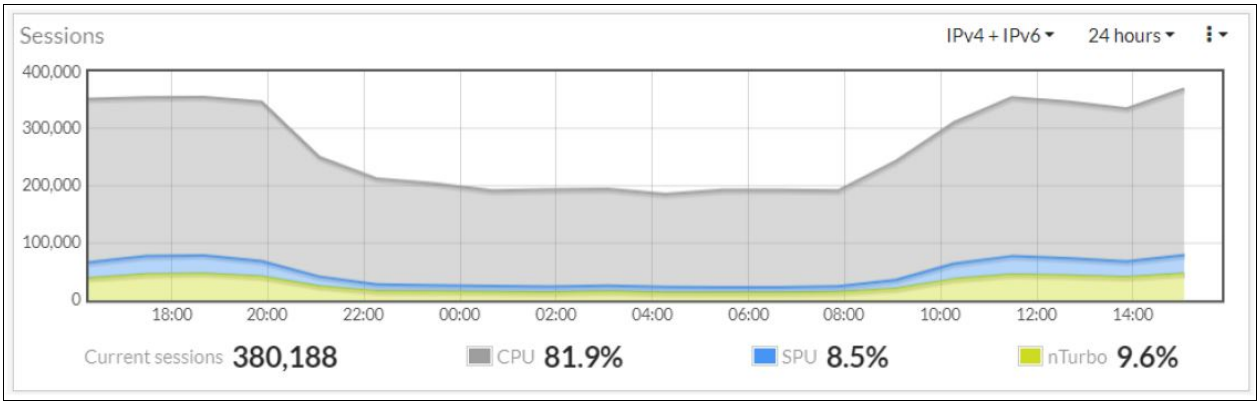

Figura 3 – Número de conexões e consumo de CPU e SPU do Firewall do núcleo central – Medição 02

10.1.14. Diante o exposto, a equipe de planejamento contratação entende que a contratação de serviço de garantia e suporte técnico para os ativos existentes, considerando a topologia atualmente implementada, o consumo elevado do tráfego de rede, as boas práticas, orientações e vedações para contratação de ativos de TIC e o acórdão TCU *n. 2400/2006,* **não é uma solução viável**, pois também implica em risco elevado para a operação dos serviços críticos de tecnologia da informação providos pelo MJSP devido à indisponibilidade de suporte aos equipamentos por parte do fabricante.

10.2. Solução 2 - Contratação de toda uma solução em Software Livre.

10.2.1. O presente cenário tem o objetivo de demonstrar uma possível utilização de solução em Software Livre nos atuais ambientes do MJSP (sede), CICCN-DF e Penitenciárias Federais . A disposição principal da análise é a viabilidade de implementação de toda uma solução de software livre, inclusive com suporte e garantia, de forma a tentar concretizar uma topologia de firewall moderna, escalável e de alto desempenho.

10.2.2. Nessa linha de soluções, destaca-se algumas forças e fraquezas observadas caso se implemente a solução em Software Livre:

Forças	Fraquezas
Open-Source	Interface não muito intuitiva
Permite a instalação de pacotes extras;	Demanda um conhecimento mais aprofundado para explorar suas funcionalidades
Execução de serviços como VPN, regras de NAT, geração de chaves RSA e monitoramento de tráfego	Suporte básico
Sistema leve	Necessário capacitação da equipe com frequência para configurações
	Funciona bem em pequenas e médias empresas
	Necessário Hardware adequado do cliente para sua instalação
	Necessário atualização e monitoramento tempestivos dos plugins por meio das comunidades

Tabela 6 - Forças e Fraquezas na Utilização de Solução em Software Livre

10.2.3. Apesar da solução possuir qualidades como ser Open Source (código projetado para ser acessado abertamente pelo público), permitir a utilização de VPN, NAT, chaves de segurança e ainda ser considerado um sistemas leve, há bastante fraquezas e necessidades específicas do MJSP que não são supridas pela solução.

10.2.4. Destaca-se nisso que a solução como um todo não possui nativamente uma empresa especializada/fabricante para manter a solução e prestar suporte especializado, sendo necessário aguardar a "comunidade" disponibilizar as atualizações sempre que considerar oportuno.

10.2.5. Além disso, a solução é disponibilizada, geralmente, em appliances virtuais, necessitando de servidores de processamento e espaço de armazenamento de dados nos nossos Datacenters e Penitenciárias para realizar a instalação e configuração. Nisso, cabe deslindar a carência desses equipamentos em nossos Datacenters e demais locais atualmente.

10.2.6. Outro fato importante é a dificuldade que poderá ser encontrada na configuração e implementação da solução de SD-WAN de forma a ter o gerenciamento centralizado, com automação do controle do caminho baseado em políticas, capacidade de segregar tráfego com base nas aplicações da camada 7 e utilizando topologia "full mesh".

10.2.7. Em virtude dos fatos mencionados, a solução de contratação de toda uma solução em Software Livre, contemplando serviços de instalação e suporte técnico, **não é uma solução viável** às áreas de negócio e técnicas do Ministério da Justiça e Segurança Pública.

10.3. Solução 3 - Contratação de uma nova solução de firewall contemplando serviços de instalação e suporte técnico com garantia pelo período de 60 meses.

10.3.1. O presente cenário tem o objetivo de demonstrar a modernização necessária da topologia da nova solução de firewall dos atuais ambientes do MJSP (sede), CICCN-DF e Penitenciárias Federais . A disposição principal da análise é a possibilidade de aquisição de ativos novos contemplando serviços de instalação e suporte técnico com garantia pelo período de 60 meses, de forma a implementar uma topologia de firewall moderna, escalável e de alto desempenho.

10.3.2. A Figura 4 demonstra a topologia de firewall implementada junto aos equipamentos de redes presentes no Datacenter MJSP (SEDE) e CICCN-DF:

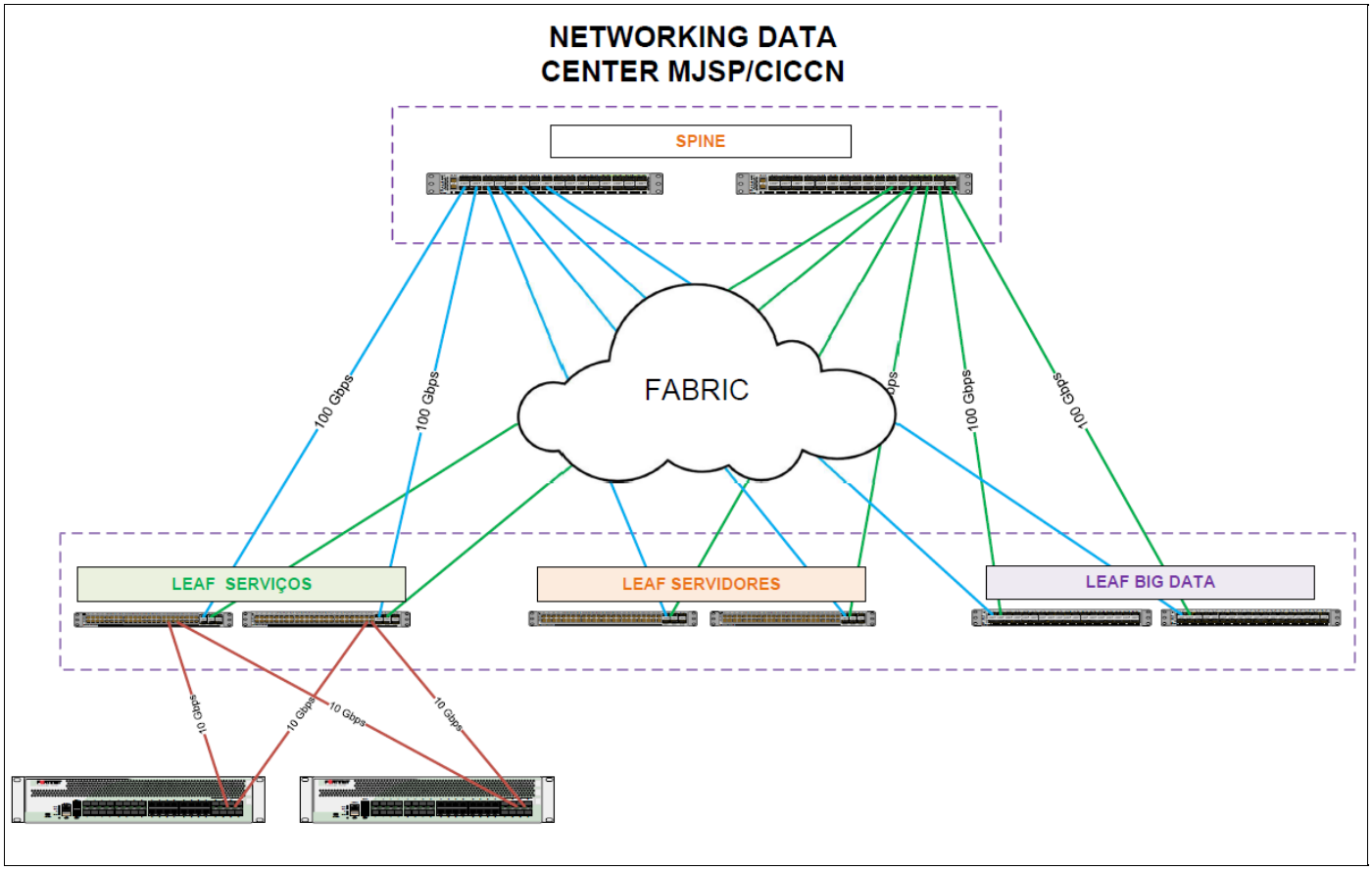

Figura 4 – Topologia MJSP e CICCN

10.3.3. De um modo geral, a topologia física não será alterada, permanecendo a nova solução também conectada aos switches Leafs de Serviços, proporcionando a padronização de topologia física, mitigando os riscos de uma parada da rede e obtendo a possibilidade de uma futura expansão tecnológica.

10.3.4. Destaca-se na nova solução, a importância em adquirir Firewalls considerados de Última Geração (inspeção profunda de pacote que vai além da inspeção e do bloqueio de portas/protocolos para adicionar uma inspeção ao nível da aplicação, uma prevenção de intrusões e obter informações fora da firewall), com a implementação da tecnologia de SD-WAN, sendo listado abaixo as principais características e vantagens, como:

10.3.4.1. Os NGFWs são a evolução e ampliação das capacidades dos firewalls tradicionais. Inspeciona os dados em um nível mais profundo para identificar e bloquear ameaças que podem estar ocultas no tráfego normal.

10.3.4.2. Os NGFWs usam inspeção profunda de pacotes (DPI), ou seja, inspeciona o corpo de cada pacote, não apenas o cabeçalho, verificando os corpos dos pacotes em busca de assinaturas de malware e de outras ameaças em potencial. Durante essa inspeção, o conteúdo de cada pacote é comparado com o conteúdo de ataques maliciosos conhecidos.

10.3.4.3. Faz o controle do aplicativo e application awareness, isto é, bloqueiam ou autorizam pacotes com base em para qual aplicativo eles estão sendo encaminhados. Os NGFWs fazem isso analisando o tráfego na camada 7, a camada de aplicativos.

10.3.4.4. Maior capacidade em prevenção de intrusões (IPSs), utilizando métodos de detecção de assinaturas (verifica as informações dentro dos pacotes recebidos e as compara com ameaças conhecidas), detecção de anomalias estatísticas (verifica o tráfego para detectar mudanças incomuns de comportamento, em comparação com uma base de referência) e detecção de análise de protocolos stateful (semelhante à detecção de anomalias estatísticas, mas com foco nos protocolos de rede em uso, comparando-os com o uso normal dos protocolos).

10.3.4.5. Inteligência contra ameaças, ou seja, são capazes de receber e agir com base em informações de inteligência contra ameaças provenientes de fontes externas, mantendo a eficácia da detecção de assinaturas do provedor ao fornecer as assinaturas de malware mais recentes, também fornecendo informações sobre a reputação de IP. "A reputação de IP" identifica os endereços de IP de onde os ataques (especialmente ataques de bot).

10.3.4.6. Os NGFWs podem processar o tráfego em várias camadas no modelo OSI, não apenas nas camadas 3 (camada de rede) e 4 (a camada de transporte). Os NGFWs podem analisar o tráfego na camada 7 HTTP e identificar quais aplicativos estão sendo utilizados.

10.3.5. A Figura 5 demonstra a topologia de firewall implementada nas Penitenciárias junto aos principais equipamentos de redes presentes nas localidades:

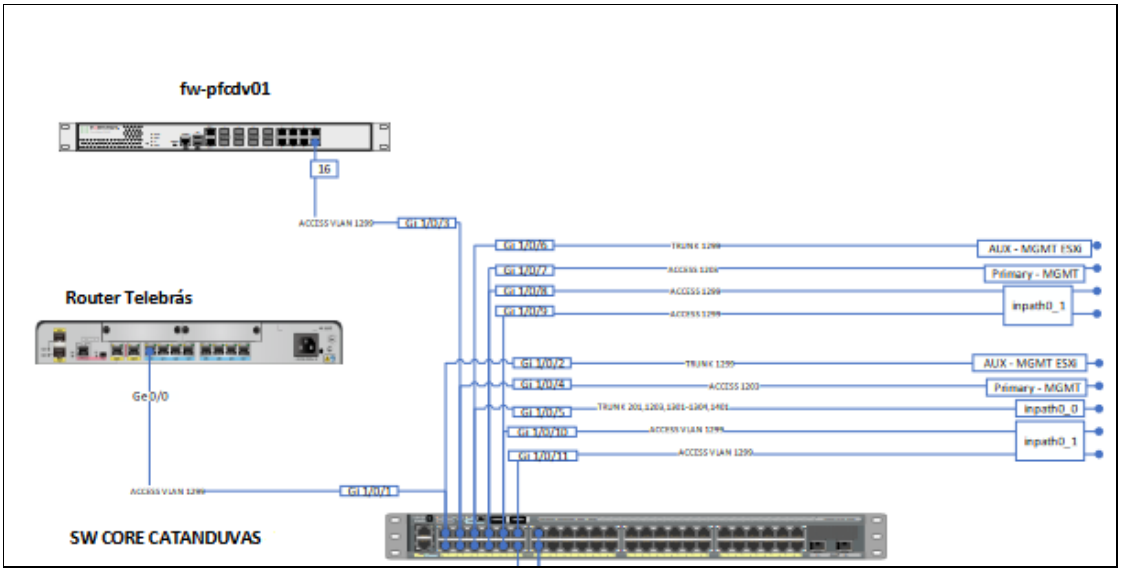

Figura 5 – Topologia de Firewall das Penitenciárias

10.3.6. A topologia de firewall implementada nas penitenciárias segue um padrão, utilizando-se de um appliance físico (de menor processamento e capacidade devido à quantidade de usuários na rede) ligado diretamente os Switch Core juntamente com outros serviços. Esta topologia física também será mantida, substituindo os atuais equipamentos por outros mais modernos, visando a utilização mais predominante da tecnologia de SD-WAN.

10.3.7. A SD-WAN pode ser entendida como uma WAN definida por software, ou seja, uma tecnologia de implantações de redes WAN baseadas em software via internet, oferecendo valor de utilidade significativo para os órgãos públicos e unidades distribuídas em termos de agilidade e capacidade de alavancar a economia da largura de banda da Internet.

10.3.8. A SD-WAN garante desempenho e resiliência consistentes de aplicativos, automatiza o direcionamento de tráfego de maneira orientada por aplicativos com base nos propósitos do MJSP, melhora a segurança da rede e simplifica a arquitetura WAN.

10.3.9. Além disso, a implantação rápida de serviços de WAN (como largura de banda e firewall) é menos complexa e muitas vezes sem a necessidade de enviar pessoal de TI no local, pois tem o gerenciamento centralizado (Centralizado no Datacenter Primário do MJSP). A largura de banda pode ser facilmente adicionada (com circuitos adicionais) ou reduzida à medida que os requisitos de negócios evoluem. A virtualização e a configuração automatizada de políticas de negócios e de segurança permitem serviços de direcionamento de tráfego automatizados, controlados centralmente com poucos cliques.

10.3.10. Sendo assim, adquirir uma nova solução de firewall (Firewall Next Generation (NGFW)), com implementação da solução de SD-WAN, vai otimizar implantações de links de dados e VPN nas unidades do MJSP, principalmente nas Penitenciárias Federais, e apresentam ainda outras funcionalidades, como:

10.3.10.1. Automatização do caminho das WANs e possibilidade de automação do controle do caminho baseado em políticas de negócios e aplicações;

10.3.10.2. Definição dinâmica de caminhos e métricas, baseadas na visibilidade em tempo real, sobre o destino desejado da aplicação, seu desempenho, a experiência do usuário final da aplicação e a qualidade das redes disponíveis no caminho;

10.3.10.3. Automação alinhada aos negócios e baseada em políticas para definir a qualidade do serviço e privilégios de acesso para todas as aplicações e todos os usuários, em combinação com a escolha automatizada do caminho;

10.3.10.4. Gerenciamento centralizado, com uma visualização integrada e topologia "full mesh" da estrutura de conectividade entre o datacenter e Unidades, tudo em uma plataforma de gerenciamento integrada e centralizada, que possibilite automatizar a implantação da VPN, com escolha do melhor link de dados e melhor caminho para a VPN, possibilitar múltiplas VPN's e continuidade do serviço de VPN em caso de falhas ou degradação de um dos links de dados, melhorando a conectividade entre redes das Unidades e a Sede;

10.3.10.5. Monitoramento de desempenho integrado de ponta a ponta e otimização da WAN de forma segura.

10.3.10.6. Suporte a VLANs, capacidade de segregar tráfego pelas WANs e entre redes LANs sem fio, e com fio e capacidade de segregar tráfego com base nas aplicações da camada 7;

10.3.10.7. Capacidade de aplicar regras de controle de acesso, desempenho e segurança com base na política definida no console de gerenciamento central;

10.3.10.8. Implantação sem configurações na unidade remota " zero-touch" via ativação automatizada e segura de todos os gateways de WAN.

10.3.11. Em virtude dos fatos mencionados, a solução de contratação de toda uma nova solução de firewall contemplando serviços de instalação e suporte técnico com garantia pelo período de 60 meses **é o cenário mais viável**, com vistas os benefícios técnicos e de padronização prestados às áreas de negócio do Ministério da Justiça e Segurança Pública.

11. REGISTRO DE SOLUÇÕES CONSIDERADAS INVIÁVEIS

11.1. Solução 1 - Contratação de serviço de garantia e suporte técnico para a solução atual.

11.1.1. Entende-se que este cenário não é viável em virtude das BOAS PRÁTICAS, ORIENTAÇÕES E VEDAÇÕES PARA CONTRATAÇÃO DE ATIVOS DE TIC - Versão 4, do Departamento de Segurança da Informação, Serviços e Infraestrutura de Tecnologia da Informação do STI/MP, o acórdão TCU *n. 2400/2006*, além da necessidade de expansão e atualização dos ativos de TIC.

11.2. Solução 2 - Contratação de toda uma solução em Software Livre.

11.2.1. Não é uma solução viável, considerando o escopo das necessidades do MJSP e por não se enquadrar nos aspectos técnicos de TIC do MJSP necessários para está contratação.

12. ANÁLISE COMPARATIVA DE CUSTOS (TCO)

12.1.Não se aplica, pois apenas a **Solução 3 - contratação de toda uma nova solução de firewall contemplando serviços de instalação e suporte técnico com garantia pelo período de 60 meses** encontra-se viável no momento, não sendo possível realizar comparação com outra, conforme previsto no art. 11, § 1º da INSTRUÇÃO NORMATIVA SGD/ME Nº 01, DE 4 DE ABRIL DE 2019.

13. DESCRIÇÃO DA SOLUÇÃO DE TIC A SER CONTRATADA

13.1 **Solução 3** - Trata-se da solução de **contratação de toda uma nova solução de firewall contemplando serviços de instalação e suporte técnico com garantia pelo período de 60 meses**, que contempla plano de atualização, expansão tecnológica e contingência constituídos por uma série de ações e procedimentos.

13.2. A tabela abaixo traz o item e a localidade de instalação de cada equipamento:

Item	Descrição	Quantidade Total	Quantidade por localidade	Local de Instalação
1	Appliance de Firewall para uso nos Datacenters do MJSP	04	02	Datacenter Primário - SEDE do MJSP
			02	Datacenter Secundário - CICCN
2	Appliance de Firewall para uso nas Penitenciárias Federais	05	01	Penitenciária Federal Catanduvas (PR)
			01	Penitenciária Federal Campo Grande (MS)
			01	Penitenciária Federal Mossoró (RN)
			01	Penitenciária Federal Porto Velho (RO)
			01	Penitenciária Federal Brasília (DF)
3	Appliance para análise do tráfego de dados	01	01	Datacenter Primário - SEDE do MJSP
4	Appliance de gerenciamento centralizado	01	01	Datacenter Primário - SEDE do MJSP

Tabela 7 - Quantidade e localização para instalação

13.3. As principais especificações e requisitos da solução serão destacados nesta etapa do planejamento, as demais serão incluídas no Termo de Referência, em seu anexo.

13.3.1. **Appliance Físico de Firewall para uso nos Datacenters do MJSP.**

13.3.1. 1. Throughput de no mínimo, 15 (quinze) Gbps, com as funcionalidades de firewall, controle de aplicação, IPS, anti-malware e prevenção contra ameaças avançadas de dia-zero habilitadas e atuantes;

13.3.1. 2. O Throughput é a quantidade de tráfego que um único equipamento écapaz de encaminhar, não havendo soma entre os membros do cluster;

13.3.1. 3. Suporte a, no mínimo, 12.000.000 (doze milhões) de conexões simultâneas;

13.3.1. 4. Suporte a, no mínimo, 500.000 (quinhentos mil) novas conexões por segundo;

13.3.1. 5. Armazenamento de, no mínimo, 480GB SSD;

13.3.1. 6. Deve possuir fontes de alimentação AC 100-240VAC redundantes e hot-swappable;

13.3.1. 7. No mínimo, 16 (Dezesseis) interfaces de rede de 1GbE RJ-45;

13.3.1. 8. No mínimo, 02 (duas) interfaces de rede de 10 Gbps SFP+;

13.3.1. 9. No mínimo, 01 (uma) interface Gigabit dedicada para alta disponibilidade;

13.3.1. 10. 01 (uma) interface do tipo console ou similar;

13.3.1. 11. Deverão ser licenciados para suportar, pelo menos, 5.000 (cinco mil) usuários de VPN SSL;

13.3.1. 12. VPN com capacidade de, pelo menos, 40 (quarenta) Gbps de tráfego IPSec;

13.3.1. 13. Suportar, no mínimo, 2 instâncias de firewall (cluster) e permitir a expansão, através de aquisição futura de licenças;

13.3.1. 14. O Throughput e as interfaces solicitados neste item deverão ser comprovados através de datasheet público na internet. Não serão aceitas declarações de fabricantes informando números de performance e interfaces;

13.3.1. 15. Todas as interfaces fornecidas nos appliances devem estar licenciadas e habilitadas para uso imediato, incluindo seus transceivers/transceptores do tipo SR.

13.3.1. 16. Não serão aceitos appliances virtualizados para os firewalls, somente equipamentos físicos.

13.3.2. **Appliance Físico de Firewall para uso nas Penitenciárias Federais**

13.3.2.1. Throughput de, no mínimo, 1Gbps com a funcionalidade de Threat Prevention, ou seja, com funcionalidades de Firewall, IPS, Controle de Aplicação e Antivírus habilitadas;

13.3.2.2. Throughput de, no mínimo, 8 Gbps de VPN IPSec para ser utilizado no SD-WAN;

13.3.2.3. Estar licenciado para, ou suportar sem o uso de licença, 500 túneis de VPN IPSEC Site-to-Site simultâneos;

13.3.2.4. Suporte a, no mínimo, 55 mil novas conexões por segundo;

13.3.2.5. Suportar no mínimo 1 Gbps de throughput de Inspeção SSL;

13.3.2.6. Possuir ao menos 16 interfaces 1 GE RJ45;

13.3.2.7. Possuir ao menos 4interfaces 1 GE SFP com transceivers inclusos;

13.3.2.8. Possuir ao menos 2 interfaces 10 GE SFP+ com transceivers inclusos;

13.3.2.9. Suportar a criação de no mínimo 5 instâncias virtuais;

13.3.2.10. Deve incluir porta USB compatível com modem 3G/4G, permitindo ainda que este link WAN seja utilizado nas regras de SD-WAN;

13.3.2.11. Possuir armazenamento de no mínimo de 480GB;

13.3.2.12. Possuir fonte de alimentação interna redundante;

13.3.2.13. Deve suportar a instalação em rack padrão 19";

13.3.3. **SD-WAN**

13.3.3.1. Deve possuir capacidade para utilizar, pelo menos 3 (três) links de WAN, sendo no mínimo 2 (dois) links simultâneos.

13.3.3.2. Permitir que a escolha do link WAN de saída seja influenciada por regras definidas pelo administrador de rede da CONTRATANTE e dinamicamente. As regras devem permitir ao menos um dos parâmetros a seguir ou combinação destes:

13.3.3.2.1. Endereço IP de origem e/ou destino;

13.3.3.2.2. Subredes de origem e/ou destino;

13.3.3.2.3. Métricas de Jitter, latência e perda de pacotes por aplicação;

13.3.3.2.4. Status da porta de WAN primários (UP ou DOWN);

13.3.3.2.5. Toda a comunicação Wan deve trafegar em um túnel VPN ponto-a-ponto estabelecido dinamicamente entre os PONTOS DE PRESENÇA da CONTRATANTE;

13.3.3.2.6. Suportar o protocolo de tunelamento GRE (General Routing Encapsulation - RFC 2784);

13.3.3.2.7. A solução deve ter um tempo máximo de failover e failback de 300 segundos;

13.3.3.2.8. A topologia da rede WAN deve ser dentre outras possíveis, a de malha completa (full mesh);

13.3.3.2.9. O estabelecimento do túnel VPN entre os pontos de presença pode inicialmente ser orientado pelo concentrador, mas o tráfego de dados após o estabelecimento do túnel deve ser realizado diretamente entre os integrantes do túnel, sem consumir throughput do concentrador;

13.3.3.2.10. A solução de SD-WAN deverá ser integrada no próprio appliance de NGFW.

14. ESTIMATIVA DE CUSTO TOTAL DA CONTRATAÇÃO

14.1. Conforme o "Guia de Boas Práticas em Contratação de Soluções de Tecnologia da Informação" V 3.0 do SISP, o orçamento informado nesse momento é preliminar. Ele deverá ser suficiente na análise de custo total de propriedade para a escolha da solução. **O orçamento detalhado será realizado na confecção do Termo de Referência.**

Grupo	Item	Descrição	Unidade	QTDE	Estimativo unitário (R$)	Estimativo total (R$)
1	1	FIREWALL TIPO I - APPLIANCE FÍSICO	Unitário	04	R$ 1.195.000,00	R$ 4.780.000,00
	2	FIREWALL TIPO II - APPLIANCE FÍSICO	Unitário	05	R$ 93.000,00	R$ 465.000,00
	3	APPLIANCE FÍSICO PARA ANÁLISE DO TRÁFEGO DE DADOS	Unitário	01	R$ 210.000,00	R$ 210.000,00
	4	APPLIANCE VIRTUAL DE GERENCIAMENTO CENTRALIZADO	Unitário	01	R$ 300.00,00	R$ 300.00,00
	ESTIMATIVA DO CUSTO TOTAL DA CONTRATAÇÃO *(Art. 11, Inciso IV, da IN 01/2019 SGD/ME)* *				**R$ 5.755.000,00**	
	* Conforme o "Guia de Boas Práticas em Contratação de Soluções de Tecnologia da Informação" V 3.0 do SISP (pág. 39), o orçamento estimado informado nesse momento é preliminar. **O orçamento detalhado será realizado na confecção do Termo de Referência.**					

Tabela 8 - Descrição dos itens

15. JUSTIFICATIVA TÉCNICA DA ESCOLHA DA SOLUÇÃO

15.1. A escolha da solução de contratação de toda uma nova solução de firewall contemplando serviços de instalação e suporte técnico com garantia pelo período de 60 meses se deu foi por vários motivos, podendo destacar os de âmbito técnico como fator importante dessa escolha.

15.2. De fato, para chegar a escolha da solução mais viável, foi necessário realizar a segmentação dos requisitos por localidade, o que remete a necessidades específicas para cada ambiente de TIC administrado pelo MJSP, sendo essas localidades os Datacenters primário e secundário e as Penitenciárias Federais (Catanduvas (PR), Campo Grande (MS), Mossoró (RN), Porto Velho (RO) e Brasília (DF)).

15.3. Os Datacenters primário e secundário e todas as penitenciárias possuem necessidades claras, a primeira é a substituição dos ativos da solução de firewall atuais, desatualizados tecnologicamente e que estão próximos do fim de vida ficando sem suporte e garantia, Já a segunda, trata-se da necessidade de expansão da capacidade da solução de Firewall do núcleo central do MJSP, pois encontra-se próximo do seu limite máximo, representando um risco à segurança das informações sob responsabilidade do MJSP e à disponibilidade dos seus serviços.

15.4. Além disso, soma-se a necessidade de ativação da tecnologia de SD-WAN nas localidades onde há indisponibilidades de links constantemente, ou ainda nos locais que possuem sistemas e serviços sensíveis que precisem de uma maior mitigação de riscos.

15.5. Sendo assim, tecnicamente, ficou comprovado que a melhor solução para os Datacenters primário e secundário é a aquisição de ativos novos, levando em consideração, para a escolha das especificações dos equipamentos, o aumento de usuários na rede, serviços disponibilizados e acessos externos aos sistemas ofertados pelo MJSP.

15.6. Por fim, conclui-se que o benefício da aquisição de uma nova solução de firewall contemplando serviços de instalação e suporte técnico foi evidenciado e comprovado, uma vez que foram realizadas análises do ponto de vista técnico, trazendo com isso melhor administração e acompanhamento da equipe de fiscalização dos contratos.

15.7. Em vista dos argumentos técnicos levantados em todo este Estudo Técnico, contratação de toda uma nova solução de firewall contemplando serviços de instalação e suporte técnico com garantia pelo período de 60 meses **foi considerado o cenário mais viável**, com vistas os benefícios técnicos e de atendimento da necessidades das áreas de negócio do Ministério da Justiça e Segurança Pública.

16. JUSTIFICATIVA ECONÔMICA DA ESCOLHA DA SOLUÇÃO

16.1. O aspecto econômico da solução escolhida (**contratação de toda uma nova solução de firewall contemplando serviços de instalação e suporte técnico com garantia pelo período de 60 meses**) foi considerado no sentido do minucioso estudo da quantidade exata ou o mais próximo da realidade necessária, com requisitos, análises e comparações técnicas consideradas essenciais para os ativos de firewall em cada localidade, já que não foi possível realizar a comparação econômica com as demais soluções devido à singularidade atual do ambiente de TIC, dispensando a necessidade de

cálculos comparativos entre soluções, conforme previsto no art. 11, § 1º da INSTRUÇÃO NORMATIVA SGD/ME Nº 01, DE 4 DE ABRIL DE 2019: *"§ 1º As soluções identificadas no inciso II consideradas inviáveis deverão ser registradas no Estudo Técnico Preliminar da Contratação, dispensando-se a realização dos respectivos cálculos de custo total de propriedade."*

17. BENEFÍCIOS A SEREM ALCANÇADOS COM A CONTRATAÇÃO

17.1. Os benefícios buscados com a substituição, expansão e atualização de equipamentos com o objetivo de mitigar os riscos, evitar impactos na segurança e na rotina dos usuários da rede do MJSP, se traduzem nas listadas abaixo:

a) Manter parque de ativos de segurança (Firewalls) com suporte, manutenção e garantia;

b) Prover a infra-estrutura de Firewalls necessária para suportar, de forma otimizada e flexível, as demandas de informações e serviços das áreas finalísticas;

c) Manter e aprimorar o método de gestão centralizada e comunicação de toda a infra-estrutura de Firewalls de forma a agilizar a sua operação;

d) Suportar a demanda futura por largura de banda e balanceamento de links nas Penitenciárias com a utilização da tecnologia SD-WAN;

e) Garantir soluções voltadas à segurança em redes de computadores;

18. PROVIDÊNCIAS A SEREM ADOTADAS

18.1. As próximas providências estão relacionadas as etapas referentes à contratação da solução escolhida, levando em consideração outras áreas envolvidas neste projeto.

18.2. Com isso, as demais etapas que envolvem diretamente a área técnica e requisitante são:

1. A Aprovação e Assinatura do Estudo Técnico Preliminar (ETP) pelos Integrantes Técnico e Requisitante da Equipe de Planejamento da Contratação e pela autoridade máxima da Área de TIC, conforme previsto no art. 11, § 2º da INSTRUÇÃO NORMATIVA SGD/ME Nº 01, DE 4 DE ABRIL DE 2019.
2. Elaboração do Termo de Referência pela Equipe de Planejamento da Contratação a partir do Estudo Técnico Preliminar da Contratação, que será assinado pela Equipe de Planejamento da Contratação e pela autoridade máxima da Área de TIC e aprovado pela autoridade competente.
3. Em paralelo a elaboração do Termo de Referência, realizar a pesquisa de mercado, que trará os esclarecimentos necessários sobre os parâmetros utilizados para a mensuração do preço médio de licitações realizadas e de mercado.
4. A composição do Mapa de Gerenciamento de Riscos (instrumento de registro e comunicação da atividade de gerenciamento de riscos ao longo de todas as fases da contratação).

19. DECLARAÇÃO DE VIABILIDADE

19.1. O presente Estudo Técnico Preliminar da Contratação evidencia que a forma de contratação que maximiza a probabilidade do alcance dos resultados pretendidos com a mitigação dos riscos e observância dos princípios da economicidade, eficácia e eficiência, seria a realização de processo de **contratação de toda uma nova solução de firewall contemplando serviços de instalação e suporte técnico com garantia pelo período de 60 meses**, para atendimento das necessidades do Ministério da Justiça e Segurança Pública.

19.2. Como principais objetivos a serem alcançados, entre outros, podem ser citados:

- Alinhamento estratégico com as iniciativas do MJSP, garantindo a entrega de valor para que as áreas finalísticas consigam atingir seus objetivos específicos;
- Melhoria da qualidade dos serviços prestados pela STIC a sua população cliente, com adoção das melhores práticas de mercado incorporadas à solução tecnológica que se pretende adquirir.
- Manter parque de ativos de segurança com suporte, manutenção e garantia;
- Prover a infraestrutura de firewall necessária para suportar, de forma otimizada e flexível, as demandas de informações e serviços das áreas finalísticas;
- Suportar a demanda futura por por maior proteção contra malwares;

19.3. Diante do exposto, a equipe de planejamento declara ser **viável** a contratação da solução pretendida.

Documento assinado eletronicamente por **Bruno Alves de Lima**, **Integrante Técnico(a)**, em 23/06/2023, às 14:46, com fundamento no § 3º do art. 4º do Decreto nº 10.543, de 13 de novembro de 2020.

Documento assinado eletronicamente por **RODRIGO ALBERNAZ BEZERRA**, **Coordenador(a)-Geral de Infraestrutura e Serviços**, em 23/06/2023, às 15:34, com fundamento no § 3º do art. 4º do Decreto nº 10.543, de 13 de novembro de 2020.

A autenticidade do documento pode ser conferida no site http://sei.autentica.mj.gov.br informando o código verificador **24328235** e o código CRC **4070E751**
O trâmite deste documento pode ser acompanhado pelo site http://www.justica.gov.br/acesso-a-sistemas/protocolo e tem validade de prova de registro de protocolo no Ministério da Justiça e Segurança Pública.

MINUTA

Ministério da Justiça e Segurança Pública
Secretaria-Executiva

Esplanada dos Ministérios, Bloco T, Anexo II, - Bairro Zona Cívico Administrativa, Brasília/DF, CEP 70064-900
Telefone: (61) 2025-7645 - - www.justica.gov.br

Minuta de Contrato Nº 9048696/2019-DICON/CCONT/CGL/SAA/SE

* MINUTA DE DOCUMENTO

TERMO DE CONTRATO Nº ...../20XX

TERMO DE CONTRATO DE PRESTAÇÃO DE SERVIÇOS Nº ___/20XX QU FAZEM ENTRE SI A UNIÃO, REPRESENTADA PELO MINISTÉRIO DA JUSTIÇA SEGURANÇA PÚBLICA, POR INTERMÉDIO DA SUBSECRETARIA DE TECNOLOGIA DA INFORMAÇÃO E DA COORDENAÇÃO-GERAL DE LICITAÇÕES E CONTRATOS E A EMPRESA xxxxxxxxxxxxxxxxxxx.

PROCESSO Nº 08006.000158/2023-36

A União, representada pelo **MINISTÉRIO DA JUSTIÇA E SEGURANÇA PÚBLICA**, com sede na Esplanada dos Ministérios, CEP 70064-900, Brasília/DF, inscrito no CNPJ sob o n° 00.394.494/0013-70, neste ato representado pelo Subsecretário de Tecnologia da Informação e Comunicação, **Senhor NEY RÊGO BARROS JUNIOR**, nomeado pela Portaria n° 2.606 de 28 de junho de 2023, publicada no D.O.U. de 29 de junho de 2023, com delegação de competência fixada pela Portaria SE n° 1.411, de 25 de novembro de 2021, publicada no D.O.U. de 25 de novembro de 2021 - Edição Extra, e pela Coordenadora-Geral de Licitações e Contratos, **Senhora ANA PAULA DE OLIVEIRA SILVA**, nomeada pela Portaria n° 641, de 10 de fevereiro de 2023, publicada no D.O.U. de 13 de fevereiro de 2023 e com delegação de competência fixada pela Portaria SAA nº 76, de 25 de novembro de 2021, publicada no D.O.U. de 29 de novembro de 2021, doravante denominada **CONTRATANTE**, e a Empresa **XXXXXXXXXXXXXXXXX.**, inscrita no CNPJ n° XXXXXXXXXX e inscrição estadual n° XXXXXXXX, estabelecida XXXXXXXXXXX - CEP XXXXXXX, neste ato representada pelo Senhor **xxxxxxx**, doravante denominada **CONTRATADA**, tendo em vista o que consta no Processo nº 08006.000158/2023-36 e em observância às disposições da Lei nº 8.666, de 21 de junho de 1993, da Lei nº 10.520, de 17 de julho de 2002, da Lei nº 8.248, de 22 de outubro de 1991, do Decreto nº 9.507, de 21 de setembro de 2018, do Decreto nº 7.174, de 12 de maio de 2010, da Instrução Normativa SGD/ME nº 1, de 4 de Abril de 2019 e da Instrução Normativa SEGES/MPDG nº 5, de 26 de maio de 2017 e suas alterações, resolvem celebrar o presente Termo de Contrato, decorrente do Pregão nº ...../20...., mediante as cláusulas e condições a seguir enunciadas.

1. CLÁUSULA PRIMEIRA – OBJETO

1.1. O objeto do presente instrumento é o fornecimento de solução de firewall contemplando serviços de instalação e suporte técnico com garantia pelo período de 60 meses, com vistas a atender às necessidades do Ministério da Justiça e Segurança Pública - MJSP, conforme as especificações e demais condições de execução contidas no Termo de Referência, anexo do Edital.

1.2. Este Termo de Contrato vincula-se ao Edital do Pregão, identificado no preâmbulo e à proposta vencedora da CONTRATADA, independentemente de transcrição.

1.3. Objeto da contratação:

GRUPO	ITEM	DESCRIÇÃO DO BEM OU SERVIÇO	CÓDIGO CATMAT/CATSER	QUANTIDADE	MÉTRICA OU UNIDADE	VALOR UNITÁRIO
1	1	FIREWALL TIPO I - APPLIANCE FÍSICO	484747	04	Unidade	
	2	FIREWALL TIPO II - APPLIANCE FÍSICO	484747	05	Unidade	
	3	APPLIANCE FÍSICO PARA ANÁLISE DO TRÁFEGO DE DADOS	481647	01	Unidade	
	4	APPLIANCE VIRTUAL DE GERENCIAMENTO CENTRALIZADO	27472	01	Unidade	

Planilha adaptada conforme previsão do Termo de Referência.

2. CLÁUSULA SEGUNDA - VIGÊNCIA

2.1. O prazo de vigência deste Termo de Contrato é aquele fixado no Edital, de 12 (doze) meses, com início na data de ...../...../..... e encerramento em ...../...../....., prorrogáveis conforme art. 57, §1º, da Lei nº 8.666/93.

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

Adaptada conforme previsão do Termo de Referência.

3. CLÁUSULA TERCEIRA – PREÇO

3.1. O valor total da contratação é de R$ ..... (.....).

3.2. No valor acima estão incluídas todas as despesas ordinárias diretas e indiretas decorrentes da execução do objeto, inclusive tributos e/ou impostos, encargos sociais, trabalhistas, previdenciários, fiscais e comerciais incidentes, taxa de administração, frete, seguro e outros necessários ao cumprimento integral do objeto da contratação.

4. CLÁUSULA QUARTA – DOTAÇÃO ORÇAMENTÁRIA

4.1. As despesas decorrentes desta contratação estão programadas em dotação orçamentária própria, prevista no orçamento da União, para o exercício de 20XX, na classificação abaixo:

Programa de Trabalho: 04122003220000000001

Plano de Trabalho Resumido (PTRES): 172184

Fonte: 1000

Ação: 2000

Plano Orçamentário (PO): 000C

Plano Interno (PI): GL67OTCGLTI

Naturezas de despesas: 449052 e 449040

4.2. No(s) exercício(s) seguinte(s), as despesas correspondentes correrão à conta dos recursos próprios para atender às despesas da mesma natureza, cuja alocação será feita no início de cada exercício financeiro.

5. CLÁUSULA QUINTA – PAGAMENTO

5.1. O prazo para pagamento à CONTRATADA e demais condições a ele referentes encontram-se definidos no Termo de Referência e no Anexo XI da IN SEGES/MP n. 5/2017.

6. CLÁUSULA SEXTA – REAJUSTAMENTO DE PREÇOS EM SENTIDO AMPLO

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

7. CLÁUSULA SÉTIMA – GARANTIA DE EXECUÇÃO

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

8. CLÁUSULA OITAVA – MODELO DE EXECUÇÃO DOS SERVIÇOS E FISCALIZAÇÃO

8.1. O modelo de execução do Contrato, os materiais que serão empregados, a disciplina do recebimento do objeto e a fiscalização pela CONTRATANTE são aqueles previstos no Termo de Referência, anexo do Edital.

9. CLÁUSULA NONA – OBRIGAÇÕES DA CONTRATANTE E DA CONTRATADA

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

10. CLÁUSULA DÉCIMA - SANÇÕES ADMINISTRATIVAS

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

11. CLÁUSULA DÉCIMA PRIMEIRA - RESCISÃO

11.1. O presente Termo de Contrato poderá ser rescindido:

11.1.1. por ato unilateral e escrito da Administração, nas situações previstas nos incisos I a XII e XVII do art. 78 da Lei nº 8.666, de 1993, e com as consequências indicadas no art. 80 da mesma Lei, sem prejuízo da aplicação das sanções previstas no Termo de Referência, anexo do Edital;

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

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

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

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

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

11.4.2. relação dos pagamentos já efetuados e ainda devidos;

11.4.3. indenizações e multas.

12. CLÁUSULA DÉCIMA SEGUNDA – VEDAÇÕES E PERMISSÕES

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

12.2. É permitido à CONTRATADA caucionar ou utilizar este Termo de Contrato para qualquer operação financeira, nos termos e de acordo com os procedimentos previstos na Instrução Normativa SEGES/ME nº 53, de 8 de Julho de 2020.

12.2.1. A cessão de crédito, a ser feita mediante celebração de termo aditivo, dependerá de comprovação da regularidade fiscal e trabalhista da cessionária, bem como da certificação de que a cessionária não se encontra impedida de licitar e contratar com o Poder Público, conforme a legislação em vigor, nos termos do Parecer JL-01, de 18 de maio de 2020.

12.2.2. O crédito a ser pago à cessionária é exatamente aquele que seria destinado à cedente (contratada) pela execução do objeto contratual, com o desconto de eventuais multas, glosas e prejuízos causados à Administração, sem prejuízo da utilização de institutos tais como os da conta vinculada e do pagamento direto previstos na IN SEGES/ME nº 5, de 2017, caso aplicáveis.

13. CLÁUSULA DÉCIMA TERCEIRA – ALTERAÇÕES

13.1. Eventuais alterações contratuais reger-se-ão pela disciplina do art. 65 da Lei nº 8.666, de 1993, bem como do Anexo X da IN/SEGES/MPDG nº 05, de 2017.

13.2. A CONTRATADA é obrigada a aceitar, nas mesmas condições contratuais, os acréscimos ou supressões que se fizerem necessários, até o limite de 25% (vinte e cinco por cento) do valor inicial atualizado do Contrato.

13.3. As supressões resultantes de acordo celebrado entre as partes contratantes poderão exceder o limite de 25% (vinte e cinco por cento) do valor inicial atualizado do Contrato.

14. CLÁUSULA DÉCIMA QUARTA – DOS CASOS OMISSOS

14.1. Os casos omissos serão decididos pela CONTRATANTE, segundo as disposições contidas na Lei nº 8.666, de 1993, na Lei nº 10.520, de 2002 e demais normas federais aplicáveis e, subsidiariamente, segundo as disposições contidas na Lei nº 8.078, de 1990 – Código de Defesa do Consumidor – e normas e princípios gerais dos contratos.

15. CLÁUSULA DÉCIMA QUINTA – PUBLICAÇÃO

15.1. Incumbirá à CONTRATANTE providenciar a publicação deste instrumento, por extrato, no Diário Oficial da União, de acordo com o prescrito no artigo 61, parágrafo único, da Lei nº 8.666, de 1993, bem como divulgá-lo no respectivo sítio oficial na Internet, em atenção ao art. 8º, § 2º, da Lei nº 12.527, de 2011, c/c art. 7º, § 3º, inciso V, do Decreto nº 7.724, de 2012.

16. CLÁUSULA DÉCIMA SEXTA - FORO

16.1. É 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 possam ser compostos pela conciliação, conforme art. 55, §2º da Lei nº 8.666/93.

17. CLÁUSULA DÉCIMA SÉTIMA – DA ASSINATURA ELETRÔNICA E/OU DIGITAL

17.1. O presente instrumento será firmado através de assinatura eletrônica e/ou digital, certificada pelo Sistema Eletrônico de Informações - SEI do Ministério da Justiça e Segurança Pública - MJSP, garantida a eficácia das Cláusulas.

17.2. Em conformidade com o disposto no § 2º, art. 10, da Medida Provisória nº 2.200-2, de 24 de agosto de 2001, a assinatura deste termo pelo representante oficial da CONTRATADA, pressupõe declarada, de forma inequívoca, a sua concordância, bem como o reconhecimento da validade e do aceite ao presente documento.

17.3. A respectiva autenticidade poderá ser atestada a qualquer tempo, seguindo os procedimentos impressos na nota de rodapé, não podendo, desta forma, as partes se oporem a sua utilização.

ANA PAULA DE OLIVEIRA SILVA
Coordenadora-Geral de Licitações e Contratos
Ministério da Justiça e Segurança Pública

NEY RÊGO BARROS JUNIOR
Subsecretário de Tecnologia da Informação e Comunicação
Ministério da Justiça e Segurança Pública

xxxxxxxxxxxxxxxxxxxxxxx
Representante da Contratada

TESTEMUNHAS:

1. NOME:

CPF:

2. NOME:

CPF:

Documento assinado eletronicamente por **LORENNA AYRES LEAL LIMA**, **Coordenador(a) de Contratos**, em 31/08/2023, às 14:44, com fundamento no § 3º do art. 4º do Decreto nº 10.543, de 13 de novembro de 2020.

A autenticidade do documento pode ser conferida no site http://sei.autentica.mj.gov.br

Ministério da Justiça e Segurança Pública
Secretaria-Executiva
Divisão de Licitações

ANEXO IV DO EDITAL

VALORES MÁXIMOS ADMISSÍVEIS

Grupo	Item	Descrição do Bem ou Serviço	Código CATMAT/CATSER	Quantidade	Métrica ou Unidade	Valor Unitário	Valor Total
1	1	FIREWALL TIPO I - APPLIANCE FÍSICO	484747	04	Unidade	R$ 1.276.800,00	R$ 5.107.200,00
	2	FIREWALL TIPO II - APPLIANCE FÍSICO	484747	05	Unidade	R$ 102.067,50	R$ 510.337,50
	3	APPLIANCE FÍSICO PARA ANÁLISE DO TRÁFEGO DE DADOS	481647	01	Unidade	R$ 210.030,00	R$ 210.030,00
	4	APPLIANCE VIRTUAL DE GERENCIAMENTO CENTRALIZADO	27472	01	Unidade	R$ 179.500,00	R$ 179.500,00
VALOR GLOBAL MÁXIMO ESTIMADO						**R$ 6.007.067,50**	

Documento assinado eletronicamente por **EDUARDO DE OLIVEIRA DA ROSA**, **Analista Técnico(a) Administrativo(a)**, em 31/08/2023, às 15:19, com fundamento no § 3º do art. 4º do Decreto nº 10.543, de 13 de novembro de 2020.

A autenticidade do documento pode ser conferida no site http://sei.autentica.mj.gov.br informando o código verificador **25110173** e o código CRC **48DC1C99**
O trâmite deste documento pode ser acompanhado pelo site http://www.justica.gov.br/acesso-a-sistemas/protocolo e tem validade de prova de registro de protocolo no Ministério da Justiça e Segurança Pública.

Referência: Processo nº 08006.000158/2023-36 SEI nº 25110173