MINISTÉRIO DA JUSTIÇA E SEGURANÇA PÚBLICA

EDITAL DE LICITAÇÃO

PREGÃO ELETRÔNICO Nº 26/2020

08006.000602/2020-71

Torna-se público, para conhecimento dos interessados, que a União, por intermédio do Ministério da Justiça e Segurança Pública, por meio da Pregoeira designada pela Portaria nº 64 de 02 de março de 2020, da Coordenação-Geral de Licitações e Contratos da Subsecretaria de Administração, publicada no D.O.U. de 04 de março de 2020, realizará licitação, na modalidade PREGÃO, na forma ELETRÔNICA, com critério de julgamento menor preço por grupo, sob a forma de execução indireta, no regime de empreitada por preço unitário, 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, da Instrução Normativa SGD/ME nº 1, de 4 de abril de 2019, das Instruções Normativas SEGES/MP nº 05, de 26 de maio de 2017 e nº 03, de 26 de abril de 2018 e da Instrução Normativa SLTI/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: 06/11/2020

Horário: 9h

Local: Portal de Compras do Governo Federal – www.comprasgovernamentais.gov.br

1. DO OBJETO

1.1. O objeto da presente licitação é a escolha da proposta mais vantajosa para a contratação de serviços de tecnologia da informação e comunicação de empresa especializada no fornecimento de solução de ativos de rede e balanceamento de carga para os Data Centers, incluindo serviços especializados, aquisição de equipamentos e softwares, modernização e expansão da capacidade atual para atendimento das necessidades do Ministério da Justiça e Segurança Pública, conforme condições, quantidades e exigências estabelecidas neste Edital e seus anexos.

1.2. A licitação será dividida em grupos, formados por um ou mais itens, conforme tabela constante do Termo de Referência, facultando-se ao licitante a participação em quantos grupos forem de seu interesse, devendo oferecer proposta para todos os itens que os compõem.

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

1.4. Cada serviço ou produto do lote deverá estar discriminado em itens separados nas

propostas de preços, de modo a permitir a identificação do seu preço individual na composição do preço global, e a eventual incidência sobre cada item das margens de preferência para produtos e serviços que atendam às Normas Técnicas Brasileiras - NTB.

2. DOS RECURSOS ORÇAMENTÁRIOS

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

2.1.1. Programa de Trabalho: 0412200322000000001

2.1.2. Plano de Trabalho Resumido (PTRES): 172184

2.1.3. Fonte: 0100

2.1.4. Ação: 2000

2.1.5. Plano Orçamentário (PO): 000C

2.1.6. Plano Interno (PI): GL67PTCGLTI

3. DO CREDENCIAMENTO

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

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

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

3.4. O licitante responsabiliza-se exclusiva e formalmente pelas transações efetuadas em seu nome, 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

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

4.2.8.1. É admissível a participação de organizações sociais, qualificadas na forma dos arts. 5º a 7º da Lei 9.637/1998, desde que os serviços objeto desta licitação se insiram entre as atividades previstas no contrato de gestão firmado entre o Poder Público e a organização social (Acórdão nº 1.406/2017- TCU-Plenário), mediante apresentação do Contrato de Gestão e dos respectivos atos constitutivos.

4.2.9. 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 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, nos termos da Instrução Normativa SLTI/MP nº 2, de 16 de setembro de 2009.

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

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

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

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

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

5. DA APRESENTAÇÃO DA PROPOSTA E DOS DOCUMENTOS DE HABILITAÇÃO

5.1. Os licitantes encaminharão, exclusivamente por meio do sistema, concomitantemente com os documentos de habilitação exigidos no edital, proposta com a descrição do objeto ofertado e o preço, até a data e o horário estabelecidos para 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.

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

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

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

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

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

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

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

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

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

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

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

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

7. DA ABERTURA DA SESSÃO, CLASSIFICAÇÃO DAS PROPOSTAS E FORMULAÇÃO 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 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. Só poderá haver empate entre propostas iguais (não seguidas de lances), ou entre lances finais da fase fechada do modo de disputa aberto e fechado.

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

7.26.1. prestados por empresas brasileiras;

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

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

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

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

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

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

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

7.30. Será assegurado o direito de preferência previsto no seu artigo 3º, conforme procedimento estabelecido nos artigos 5° e 8° do Decreto n° 7.174, de 2010.

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

8. DA ACEITABILIDADE DA PROPOSTA VENCEDORA.

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

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

8.2.2. contenha vício insanável ou ilegalidade;

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

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

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

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

8.2.4.1.2. 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.

8.3. Se houver indícios de inexequibilidade da proposta de preço, ou em caso da necessidade de esclarecimentos complementares, poderão ser efetuadas diligências, na forma do § 3° do artigo 43 da Lei n° 8.666, de 1993 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.

8.4. Quando o licitante apresentar preço final inferior a 30% (trinta por cento) da média dos preços ofertados para o mesmo item, e a inexequibilidade da proposta não for flagrante e evidente pela análise 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.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.

8.4.1. 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.

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

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

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

8.6. 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.

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

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

8.9. 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.

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

9. DA HABILITAÇÃO

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

a) SICAF;

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

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

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

d) Lista de Inidôneos e o Cadastro Integrado de Condenações por Ilícitos Administrativos - CADICON, mantidos pelo Tribunal de Contas da União - TCU;

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

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

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

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

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

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

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

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

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

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

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

9.3. Havendo a necessidade de envio de documentos de habilitação complementares, necessários à confirmação daqueles exigidos neste Edital e já apresentados, o licitante será convocado a encaminhá-los, em formato digital, via sistema, no prazo de 2 (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 aqueles documentos que, pela própria natureza, comprovadamente, forem emitidos somente em nome da matriz.

9.6.1. Serão aceitos registros de CNPJ de licitante matriz e filial com 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. no caso de empresário individual, inscrição no Registro Público de Empresas Mercantis, a cargo da Junta Comercial da respectiva sede;

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;

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

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

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

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

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

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

9.10. **Qualificação Econômico-Financeira:**

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

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

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

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

9.10.3. 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 =	Ativo Circulante + Realizável a Longo Prazo / Passivo Circulante + Passivo Não Circulante
SG =	Ativo Total / Passivo Circulante + Passivo Não Circulante
LC =	Ativo Circulante / Passivo Circulante

9.10.4. As empresas, cadastradas ou não no SICAF, 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 estimado da contratação ou do item pertinente.

9.11. **Qualificação Técnica:**

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

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

Grupo I:

a) Fornecimento de 50% do quantitativo de cada item de Switches (Spine e Leaf - itens 1, 2 e 3) de Data Center com características compatíveis com as especificadas nesse Termo de Referência, contendo especificamente as seguintes funcionalidades:

b) Suporte a topologias Spine-and-Leaf;

c) Suporte à Multichassis Link Etherchannel;

d) Suporte à Fabric IP L3 com VXLAN;

e) Fornecimento de 50% da quantidade de Switches de Agregação (item 4) com características compatíveis com as especificadas nesse Termo de Referência;

f) Comprovar a instalação e configuração de equipamentos semelhantes utilizando a topologia Spine-and-Leaf.

Grupo II:

a) Fornecimento de 50% do quantitativo da Solução de Segurança e Balanceamento de Carga (item 14) com características compatíveis com as especificadas nesse Termo de Referência, contendo especificamente as seguintes funcionalidades:

b) Suporte a SLB e GLSB;

c) Suporte à WAF;

d) Suporte à SSL Offload, visibilidade e orquestração de tráfego SSL.

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

9.11.1.1.2. 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 CONTRATANTE deseja implementar. Além disso, conforme exposto na justificativa da contratação, pretende-se realizar modificações de criticidade alta na topologia de redes do MJSP, o que torna essencial, para garantir a correta implementação do projeto, que configurações adequadas, desempenho, qualidade, além da disponibilidade, cofiabilidade e integridade das informações, sejam garantidas pela LICITANTE, sendo isso exposto pelas qualificações técnicas solicitadas.

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

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

9.11.4. 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/MP n. 5/2017.

9.11.5. 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/MP n. 5/2017.

9.11.6. As empresas, cadastradas ou não no SICAF, deverão apresentar atestado de vistoria assinado pelo servidor responsável, nos termos do item 12.3.1 do Termo de Referência.

9.11.6.1. 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 (a) da prova de inscrição nos cadastros de contribuintes estadual e municipal e (b) da apresentação do balanço patrimonial e das demonstrações contábeis do último exercício.

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

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

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

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

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

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

9.18. Nos itens não exclusivos a microempresas e empresas de pequeno porte, em havendo inabilitação, haverá nova verificação, pelo sistema, da eventual ocorrência do empate ficto, previsto nos artigos 44 e 45 da LC nº 123, de 2006, seguindo-se a disciplina antes estabelecida para aceitação da proposta subsequente.

9.19. O licitante provisoriamente vencedor em um item, que estiver concorrendo em outro item, ficará obrigado a comprovar os requisitos de habilitação cumulativamente, isto é, somando as exigências do item em que venceu às do item em que estiver concorrendo, e assim sucessivamente, sob pena de inabilitação, além da aplicação das sanções cabíveis.

9.19.1. Não havendo a comprovação cumulativa dos requisitos de habilitação, a inabilitação recairá sobre o(s) item(ns) de menor(es) valor(es), cuja retirada(s) seja(m) suficiente(s) para a habilitação do licitante nos remanescentes.

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

10. DO ENCAMINHAMENTO DA PROPOSTA VENCEDORA

10.1. A proposta final do licitante declarado vencedor deverá ser encaminhada no prazo de 2 (duas) horas, a contar da solicitação do Pregoeiro no sistema eletrônico e deverá:

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

10.1.2. apresentar a proposta devidamente ajustada ao lance vencedor;

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.

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

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

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

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

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

proposta de outro licitante.

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

11. DOS RECURSOS

11.1. O Pregoeiro declarará o vencedor e, depois de decorrida a fase de regularização fiscal e trabalhista de microempresa ou empresa de pequeno porte, se for o caso, concederá o prazo de no mínimo trinta minutos, para que qualquer licitante manifeste a intenção de recorrer, de forma motivada, isto é, indicando contra quais decisões 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

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 ou aceitar instrumento equivalente, conforme o caso (Nota de Empenho/Carta Contrato/Autorização), sob pena de decair do direito à contratação, sem prejuízo das sanções previstas neste Edital.

15.2.1. 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 anterior poderá ser prorrogado, por igual período, por solicitação justificada do adjudicatário e aceita pela Administração.

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

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

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

15.3.3. a contratada reconhece que as hipóteses de rescisão são aquelas previstas nos artigos 77 e 78 da Lei nº 8.666/93 e reconhece os direitos da Administração previstos nos artigos 79 e 80 da mesma Lei.

15.4. O prazo de vigência da contratação é de 12 (doze) meses prorrogável conforme previsão no termo de referência.

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

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

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

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

15.7. Na hipótese de o vencedor da licitação não comprovar as condições de habilitação consignadas no edital ou se recusar a assinar o contrato ou a ata de registro de preços, a Administração, sem prejuízo da aplicação das sanções das demais cominações legais cabíveis a esse licitante, poderá convocar outro licitante, respeitada a ordem de classificação, para, após a

comprovação dos requisitos para habilitação, analisada a proposta e eventuais documentos complementares e, feita a negociação, assinar o contrato.

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 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. 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.

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

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

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

20.3.3. 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;

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

20.3.4.1. A Sanção de impedimento de licitar e contratar prevista neste subitem também é aplicável em quaisquer das hipóteses previstas como infração administrativa no subitem 20.1 deste Edital.

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

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

20.5. 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.

20.6. 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.

20.7. 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.

20.8. 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.

20.9. 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.

20.10. 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.

20.11. As penalidades serão obrigatoriamente registradas no SICAF.

20.12. 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 621, 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.

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

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

22. DAS DISPOSIÇÕES GERAIS

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

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

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

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

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

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

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

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

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

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

22.11. O Edital está disponibilizado, na íntegra, no endereço eletrônico https://www.gov.br/compras/pt-br/ e www.justica.gov.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

22.12.2. ANEXO I - A - ESPECIFICAÇÕES TÉCNICAS

22.12.3. ANEXO I - B - PROPOSTA DE PREÇOS

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

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

22.12.6. ANEXO I - E - TERMO DE CIÊNCIA

22.12.7. ANEXO I - F - TERMO DE COMPROMISSO

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

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

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

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

22.12.12. ANEXO II – Valores Máximos Admissíveis

22.12.13. ANEXO III – Minuta de Termo de Contrato 1

22.12.14. ANEXO IV - Minuta de Termo de Contrato 2

ALEXANDRA LACERDA FERREIRA RIOS

PREGOEIRA

Documento assinado eletronicamente por **ALEXANDRA LACERDA FERREIRA RIOS**, **Chefe da Divisão de Licitações**, em 22/10/2020, às 09:12, conforme o § 1º do art. 6º e art. 10 do Decreto nº 8.539/2015.

A autenticidade do documento pode ser conferida no site http://sei.autentica.mj.gov.br informando o código verificador **12962938** e o código CRC **04ED998C**
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.

Ministério da Justiça e Segurança Pública
Secretaria-Executiva
Divisão de Licitações

ANEXO I DO EDITAL

TERMO DE REFERÊNCIA

Histórico de Revisões

Data	Versão	Descrição	Autor
18/08/2020	1.0	Finalização da primeira versão do documento	Equipe de Planejamento da Contratação
11/09/2020	2.0	Finalização da segunda versão do documento	Equipe de Planejamento da Contratação
15/09/2020	3.0	Finalização da terceira versão do documento	Equipe de Planejamento da Contratação
15/10/2020	4.0	Revisão após Parecer da CONJUR	Equipe de Planejamento da Contratação

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

1. OBJETO DA CONTRATAÇÃO

1.1. Contratação de solução de ativos de rede e balanceamento de carga para os Data Centers, incluindo serviços especializados, aquisição de equipamentos e softwares, modernização e expansão da capacidade atual para atendimento das necessidades do Ministério da Justiça e Segurança Pública.

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	Switch Spine	**122971**	04	Unidade
	2	Switch Leaf- Tipo A	**122971**	06	Unidade
	3	Switch Leaf- Tipo B	**122971**	04	Unidade
	4	Switch de Agregação	**122971**	02	Unidade
	5	Sistema de Gerenciamento de Equipamentos de Data Center	**27464**	01	Unidade
	6	Solução de Controle de Acesso – Virtual Machine	**27464**	01	Unidade
	7	Licenciamento Switches existentes	**27464**	02	Unidade
	8	Transceiver 10G Multimodo (LC)	**150812**	70	Unidade
	9	Transceiver 25G Multimodo (LC)	**150812**	16	Unidade
	10	Cordão Óptico Duplex, 10G Multimodo,(LC/LC) (10 metros)	**41521**	62	Unidade
	11	Cabo de Conexão Direta 100G – (10 metros)	**150812**	20	Unidade
	12	Cabo de Conexão Direta 40G – (10 metros)	**150812**	08	Unidade
	13	Operação Assistida	**27340**	01	Unidade
Grupo	**Item**	**Descrição do Bem ou Serviço**	**Código CATMAT/CATSER**	**Quantidade**	**Métrica ou Unidade**
		Solução de segurança e balanceamento			

2	14	Solução de segurança e balanceamento de carga - Appliance Físico - Tipo A	**150100**	02	Unidade
	15	Transceiver 10G Multimodo - para item 14 (Appliance Físico - Tipo A)	**150812**	16	Unidade
	16	Solução de segurança e balanceamento de carga - Tipo B (Ambiente Virtual) para 36 meses	**27502**	01	Unidade
	17	Operação Assistida	**27340**	01	Unidade

2.2. Como pode ser observado, a presente contratação será dividida em dois grupos:

2.2.1. **Grupo 1** será responsável pelo fornecimento dos Ativos de Redes, com todos os componentes necessários, para a reestruturação e modernização dos Data Centers do núcleo central do Ministério e CICCN-DF.

2.2.2. **Grupo 2** será responsável pelo fornecimento de Balanceamento de Carga e Segurança, também para os dois Data Centers.

2.2.2.1. Importante destacar que o Grupo 2 é composto por equipamentos e componentes físicos que serão instalados no Data Center do núcleo central do Ministério e também por solução de software (item 16 do grupo 2) que atuará como redundância no Data Center do CICCN-DF.

2.2.2.2. Para tanto, tendo em vista que o item 16 do Grupo 2 se trata de uma solução de software de balanceamento e segurança, e que será contratada no modelo de subscrição, será firmado um contrato separado para esse item.

2.2.3. **Grupo 1**

2.2.3.1. A aquisição de todos os Ativos do Grupo 1 terão contrato de 12 (doze) meses, tendo garantia de 60 meses, contados do aceite definitivo da solução.

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

2.2.4. **Grupo 2**

2.2.4.1. A aquisição de todos Ativos de Balanceamento do grupo 2 terão contrato de 12 (doze) meses, tendo garantia de 60 meses, contados do aceite definitivo da solução.

2.2.4.2. O item 16 terá contrato de 36 (trinta e seis) meses com pagamento único, conforme inciso IV, do art. 57, da Leinº 8.666/93. Para esse item será firmado contrato separado, cuja vigência está prevista para iniciar após o Termo de Recebimento Definitivo (TRD).

2.2.4.3. 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 3.555/2000: Regulamenta a modalidade de licitação denominada pregão, para aquisição de bens e serviços comuns.

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

3.1.6. 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.

3.1.7. 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.

3.1.8. Instrução Normativa nº 73/2020: 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.

3.1.9. Instrução normativa nº 1, de 4 de abril de 2019: 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.

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

3.1.11. 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.

3.1.12. Guias, manuais e modelos publicados pelo Órgão Central do SISP (art. 8º, §2, da IN SGD/ME nº 1/2019).

4. JUSTIFICATIVA PARA A CONTRATAÇÃO

4.1. *Contextualização e Justificativa da Contratação*

4.1.1. A Diretoria de Tecnologia da Informação e Comunicação do Ministério da Justiça e Segurança Pública (DTIC/MJSP) passou por mudanças estruturais e regimentais no de 2019/20, 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 rede atualmente em funcionamento, requerendo dos equipamentos ativos maiores taxas de transmissão e maior poder de processamento.

4.1.3. Tal implementação requer uma maior interatividade da parte de gerência entre os sistemas, procedimentos de configuração, desempenho, qualidade e recuperação da informação, 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 switches de alto desempenho e disponibilidade, equipamentos balanceadores de carga e segurança da informação aplicada às camadas superiores, 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. **Atual arquitetura e topologia de rede, balanceamento e segurança**

4.1.5.1. Seguindo as boas práticas de mercado, a implementação do modelo de arquitetura de redes em camadas é amplamente difundida no mundo todo. Existem diversos benefícios na adoção da arquitetura de rede em camadas, como por exemplo:

- Escalabilidade - facilmente expandidas;
- Redundância - aumentar drasticamente a disponibilidade por meio de implementações redundantes simples com redes hierárquicas;
- Desempenho - taxas de transmissão próximas ao máximo suportado em toda a rede;
- Segurança - segurança de porta do nível de acesso e políticas no nível de distribuição tornam a rede mais segura;
- Gerenciamento - relativamente simples em uma rede hierárquica;
- Sustentabilidade - permite a escala da rede sem que haja muitas complicações.

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

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

4.1.5.3. 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.

4.1.5.4. 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).

4.1.5.5. 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.

4.1.5.6. Cabe destacar que a manutenção de todas as camadas apresentadas é fundamental para o perfeito funcionamento da rede do MJSP, tendo em vista que a ocorrência de um incidente ou problema em um dos equipamentos da estrutura de rede em questão, impacta diretamente no trabalho dos usuários, tornando indisponível todos os meios de TIC, como internet, impressoras,

acesso ao correio eletrônico, entre outros.

4.1.5.7. Salienta-se que no ano de 2016, através do processo (08006.001634/2016-15), foram adquiridos novos equipamentos de Acesso para substituição somente para o 3º e 4º andares do Edifício Sede, onde encontram-se a Secretaria Executiva e Gabinete do Ministro. No mesmo processo, também foram adquiridos equipamentos para interconexão dos servidores de rede do Datacenter do INFOSEG, e substituição de switches nas então quatro Penitenciárias Federais.

4.1.5.8. Na época, uma das motivações para a troca desses equipamentos, era a ocorrência constante de incidentes em alguns switches de acesso, fato que gerou transtornos às áreas de negócio, impossibilitando a comunicação de dados e telefonia e que levou a DTIC a adotar soluções paliativas de contorno como reinicialização dos equipamentos.

4.1.5.9. Além disso, naquele período, cerca de 80% dos equipamentos de acesso, e 100% dos equipamentos de distribuição, encontravam-se sem contrato de garantia e suporte, necessitando de atualização tecnológica, garantia e serviço de suporte do fabricante.

4.1.5.10. Salienta-se que, no ano de 2018, por meio do processo de aquisição (08006.001282/2018-51), foram adquiridos switches de distribuição e acesso contemplando a troca em cerca de 80% de todo o nosso parque desses ativos, tendo o final de suporte e garantia em março de 2024. A referida aquisição teve como principal objetivo suprir a necessidade de switches que não foram adquiridos no ano de 2016.

4.1.5.11. Cabe ainda ressaltar, que no ano de 2014, por meio do processo 08006.001074/2014-29, foram adquiridos switches da Camada Central (Core) em substituição aos equipamentos defasados naquele período, além de solução de controle de acesso à rede e dispositivos e solução de rede sem fio, todos instalados no Data Center do edifício sede, 2° andar, sala 201.

4.1.5.12. Os referidos equipamentos foram adquiridos em dezembro de 2014, com 48 meses de garantia e suporte, os quais tiveram sua expiração em dezembro de 2018.

4.1.5.13. Atualmente, os equipamentos da Camada Central já atingiram seu tempo de vida útil e estão desatualizados tecnologicamente, além de terem sua sustentação e disponibilidade comprometidas pela falta de contrato de suporte, manutenção e garantia.

4.1.5.14. A atual estrutura de Data Centers do MJSP é formada pelos Data Centers do núcleo central e pelo Data Center do Centro Integrado de Comando e Controle Nacional de Brasília – CICCN-DF, que está sob responsabilidade tecnológica da DTIC/MJSP, após a extinção da Secretaria Extraordinária de Segurança para Grandes Eventos – SESGE, cuja data de extinção ocorreu no dia 31 de julho de 2017.

4.1.5.15. Atualmente o Ministério possui no núcleo central dois CPD's, e uma sala técnica que abriga a solução de telefonia do MJSP (T5 do edifício Sede).

4.1.5.16. No primeiro CPD, mais antigo, localizado no segundo andar do Edifício Sede, sala 201, estão concentrados todos os equipamentos que formam o núcleo de rede do MJSP, como Switch Core, convergência de todas as fibras ópticas dos andares do Edifício Sede, Anexo I e Anexo II. Salienta-se que atualmente existe uma limitação de velocidade na conexão entre os andares e o núcleo da rede, tendo em vista que os cabos de fibra óptica são do padrão monomodo e ainda funcionam com transeivers antigos, também monomodo.

4.1.5.17. Os atuais switches Core da rede estão configurados para formarem dois VSS (*Virtual Switching System*): VSS-LAN e VSS-DC. No VSS-LAN são configuradas todas as interfaces de rede que recebem as fibras dos andares, já no VSS-DC, são concentradas as fibras ópticas de interligação do outro Data center que fica localizado no térreo do Anexo II.

4.1.5.18. Ligados ao switch Core da rede, estão os equipamentos de firewall da rede do MJSP, que fazem a segmentação e proteção externa e interna da rede, sendo que os equipamentos estão cobertos por contrato de suporte e garantia do fabricante, e além das funções de firewall, executam também funções de IPS/IDS e filtro de conteúdo.

4.1.5.19. A rede sem fio do órgão também possui equipamentos instalados nesse Data Center, quais sejam duas controladoras e appliances ISE que fazem o gerenciamento da autenticação da rede sem fio de visitantes, bem como o controle de acesso à rede e usuários.

4.1.5.20. Também estão concentrados no Data Center, os equipamentos de videoconferência do MJSP, que foram substituídos por equipamentos adquiridos pelo DEPEN através do processo (08016.000044/2015-67).

4.1.5.21. Por último, tem-se a chegada da operadora SERPRO, que atualmente é responsável pela interligação das unidades do MJSP, via INFOVIA, e também pelo link principal de Internet.

4.1.5.22. No segundo CPD, localizado no térreo do Anexo II, antiga sala do INFOSEG, concentra-se todo o ambiente de processamento e armazenamento da rede MJSP, como sistemas de Virtualização, Sistema de CFTV, Controle de Acesso do órgão, Storages e Backup. Também estão instalados no referido Data Center, os concentradores MPLS, link de Internet redundante da TELEBRAS, e solução de aceleradores de WAN, que otimizam o tráfego das cinco Penitenciárias Federais, as quais são suportadas pela DTIC/MJSP.

4.1.5.23. Destaca-se que para interconexão de todos os equipamentos listados no Data Center em questão, o MJSP dispõe de uma estrutura de *switches* de alto desempenho capazes de interligar a altas velocidades, os servidores do ambiente de processamento, os quais formam a base para todo o ambiente de virtualização, aos demais *switches* cores da rede e também ao *firewalls* da rede, que estão instalados fisicamente no Data Center do edifício Sede, sala 201.

4.1.5.24. Historicamente, este Data Center era utilizado pela rede INFOSEG, que possuía servidores, aplicações e banco de dados dedicados para aquela estrutura. No decorrer dos anos, a rede INFOSEG foi migrada para o SERPRO e o espaço foi ocupado pela então CGTI para instalação de equipamentos da rede do Ministério, tendo em vista que o Data Center do edifício sede estava com infiltrações que gerava risco para os equipamentos de processamento e armazenamento, que lá estavam instalados. Com isso, houve uma separação dos equipamentos de Data Center do órgão, que com o passar do tempo foi crescendo, não havendo espaço físico em nenhum dos locais para concentração em um único local, equipamentos de rede, segurança, processamento, armazenamento e backup. Foi a partir daí, que os equipamentos começaram a operar separadamente, gerando-se gargalos e diversos pontos de falhas.

4.1.5.25. O atual cenário não se deu a curto prazo, mas sim ao longo dos anos, onde mudanças naturais da conjuntura política, de gestão e de empresas que apoiavam na administração dos ambientes, resultaram no atual panorama. Outro fator que levou a este cenário, foi a falta de recursos financeiros e priorização para realização de projetos de infraestrutura com o objetivo de proporcionar a concentração dos ativos do órgão em um único local físico com a segurança e a proteção adequada.

4.1.5.26. Importante esclarecer que o fato de os equipamentos de *firewalls* estarem instalados em outro Data Center gera um *delay* na comunicação entre as aplicações e os servidores de banco de dados.

4.1.5.27. Salienta-se que o fato de a infraestrutura de Data Center do MJSP ser composta por locais separados fisicamente para acomodação de seus equipamentos gera uma fragilidade nos sistemas, pois os locais funcionam de forma complementar e gerando uma dependência mútua, sendo que um suporta as soluções de rede e segurança e o outro a parte de processamento, armazenamento e backup. Para a interconexão entre as duas partes, são necessários links de fibra óptica de forma a manter a maior taxa de transferência possível entre os dois locais.

4.1.5.28. Cabe destacar que atualmente o Ministério possui appliances ISE, que fazem o gerenciamento da autenticação da rede sem fio de visitantes, bem como o controle de acesso à rede e usuários. Essa ferramenta foi adquirida no ano de 2014, por meio do contrato 74/2014, que já encontra-se expirado. Na época, como não havia licença para todos os equipamentos da rede de acesso, o escopo da contratação consistiu em utilizar a solução para o controle de acesso da rede sem fio visitante.

4.1.5.29. É oportuno mencionar que foram adquiridos novos equipamentos de Acesso para substituição somente para o 3º e 4º andares do Edifício Sede, os quais possuem licenças que permitem a implementação de controle de acesso. Assim como, no ano de 2018, por meio do processo de aquisição (08006.001282/2018-51), foram adquiridos switches de distribuição e acesso contemplando a troca em cerca de 80% de todo o parque desses ativos, os quais também contemplam licenças para utilização nesse projeto. Com isso, atualmente todos os switches da rede possuem licenciamento para funcionamento com solução de controle de acesso.

4.1.5.30. Para modernizar o controle de acesso da rede de computadores do Órgão é necessário que o funcionamento da referida solução seja revisto de forma que sejam integrados e todos os switches, provendo o controle de acesso de todas as portas do equipamentos da rede acesso, bem como seja reativado o suporte do fabricante.

4.1.5.31. Além da estrutura de Data Centers do núcleo central do Ministério, a DTIC é responsável pela gestão do Data Center do Centro Integrado de Comando e Controle Nacional de Brasília – CICCN-DF (sala cofre), que também possui ativos de rede, responsáveis pela interconexão dos equipamentos internos o Data Center e também interligação com a sala técnica da pétala H do complexo do Departamento de Polícia Rodoviária Federal.

4.1.5.32. Atualmente a estrutura de switches do Data Center do CICCN-DF é composta por 2 (dois) switches Extreme Networks, modelo Black Diammond 8810 (RACK 02) interligados para atender às camadas de distribuição e as de acesso do edifício e 2 (dois) switches Extreme Networks Summit X440-24t para realizarem conexão com os servidores e *firewalls* da sala cofre. Os equipamentos foram adquiridos em 2013, Contrato 18/2013, 08131.000437/2013.92, e estão sem contrato de garantia e suporte.

4.1.5.33. Com o objetivo de prover a alta disponibilidade entre os dois Data centers (MJSP e CICCN-DF), a DTIC, no ano de 2018, iniciou projetos para este fim, sendo um deles a modernização das ferramentas de virtualização, por meio do contrato 30/2018 (7794421) com novas ferramentas de virtualização, como *Vmware vSphere Enteprise Plus With Operations Management (vSOM), Software de Gerenciamento Vcenter Server Standard e Software NSX - ENTERPRISE PLUS*, as quais estão em fase final de implantação e irão modernizar o ambiente de virtualização e implementar alta disponibilidade com o Data Center do CICCN-DF, também de responsabilidade desta DTIC.

4.1.5.34. Cabe destacar ainda que, além das ferramentas possibilitarem alta disponibilidade entre os Data centers, ainda será possível a implantação do recursos de microssegmentação para máquinas virtuais e containers, assim como monitoramento e detecção de problemas para aplicativos tradicionais e nativos em nuvem. Com o NSX, as funções de rede, como switch, roteamento e firewall, são incorporadas ao hypervisor e distribuídas em todo o ambiente. Isso possibilita a implantação de um “hypervisor de rede” que funciona como uma plataforma para sistemas de redes virtuais e serviços de segurança. De maneira semelhante ao modelo operacional de máquinas virtuais, as redes virtuais são aprovisionadas programaticamente e gerenciadas sem depender do hardware subjacente.

4.1.5.35. Importante destacar que para que dois Data Centers funcionem em alta disponibilidade de forma plena, várias ações precisam ser consideradas em todos os níveis, desde a camada física até a camada de aplicações. Nesse sentido, é necessário uma solução que tenha a capacidade de balancear carga entre servidores (Server Load Balancing – SLB), utilizando para isso funções de *Global Server Load Balancing* (GSLB), que proporciona a hospedagem de serviços em mais de um data center, permitindo alta disponibilidade e serviço de balanceamento de links.

4.1.5.36. Esses balanceadores são importantes para momentos de pico de tráfego de acesso. Algoritmos inteligentes dedicam-se à distribuição de tarefas entre os processadores disponíveis para que usuário não se depare com situações inconvenientes em seu acesso à internet e aplicações no MJSP.

4.1.5.37. O balanceamento na utilização da rede passa, sobretudo, por reencaminhar o tráfego por caminhos alternativos a fim de descongestionar os acessos aos servidores.

4.1.5.38. Sendo assim, também neste projeto, torna-se imprescindível uma análise de solução com dispositivos que são responsáveis pelo balanceamento e que possuam funções de *Global Server Load Balancing* (GSLB) e sincronização dos dados de forma automática.

4.1.5.39. Outro fator importante, que merece ser tratado como requisito essencial em um projeto comunicação entre os dois Data centers, é a capacidade realizar a abertura de conexões criptografadas, ou seja, uma visibilidade e inspeção de SSL. Além disso, há também necessidade de prover segurança nas camadas superiores (aplicação).

4.1.5.40. Soluções voltadas à segurança em redes de computadores são amplamente difundidas e necessárias em um ambiente com constantes atualizações e propenso a situações de volatilidade, que são constantes e recorrentes em qualquer ambiente de TI.

4.1.5.41. Nessa linha, a criptografia é uma forma de garantir a confidencialidade das informações, protegendo a privacidade e a integridade de dados. Segundo o Gartner, mais de 80% do tráfego atual já utiliza criptografia para garantir maior segurança das informações (https://www.gartner.com/en/documents/3869861/encrypted-web-traffic0). Por outro lado, sua utilização também cria um ponto cego que os invasores conseguem explorar para escapar dos controles de segurança.

4.1.5.42. A partir de resultados recentes de testes do NSS Labs, concluiu-se que os dispositivos tradicionais de rede e segurança, ao inspecionar o tráfego criptografado, tem seu desempenho afetado gravemente. Em média, o impacto no desempenho da inspeção profunda de pacotes é de 60%, com a média de queda nas taxas de conexão de 92% e aumento no tempo de resposta de 672% (https://www.nsslabs.com/press/2018/7/24/nss-labs-expands-2018-ngfw-group-test-with-ssl-tls-security-and-performance-test-reports/), número que representa uma taxa impressionante.

4.1.5.43. A grande diferença entre a funcionalidade de SSL Offload e Orquestração SSL é que enquanto a funcionalidade de SSL Offload se concentra em reduzir o impacto de tratamento SSL nos servidores, tem-se na orquestração um recurso que se destina a abrir, de forma centralizada e seletiva, as conexões criptografadas, com o intuito de a aliviar a exigência de processamento dos dispositivos clássicos de Segurança (Firewall, Sistemas IPS, WAF, web proxy, DLP, dentre outros).

4.1.5.44. Com tal abordagem, os elementos especializados em Segurança podem direcionar seus recursos computacionais para as tarefas de inspeção de tráfego para as quais são otimizados. Além de proteger o investimento nas soluções existentes no que concerne a desempenho, tal mecanismo contribui para ampliar a segurança da rede, pois opera no sentido de eliminar os “pontos cegos” que decorrem do significativo volume de canais SSL criptografados.

4.1.5.45. Cabe citar que o Ministério sempre buscou por soluções que atendam aos requisitos e melhores práticas disseminadas nesse mercado voltado à segurança, implementando ações e adquirindo equipamentos robustos e capazes de mitigar ações mal intencionadas.

4.1.5.46. Alguns equipamentos foram adquiridos em dezembro de 2017 por meio do processo 08006.001190/2016-18 (Contratação de empresa especializada para o fornecimento de serviços de aquisição de Solução de Segurança de Perímetro, incluindo suporte técnico, manutenção e garantia de funcionamento, para o atendimento das necessidades do Ministério da Justiça e Segurança Pública).

4.1.5.47. Essa solução (Firewall) é importante e essencial para proteção de ataques cibernéticos, sendo um dispositivo de segurança de rede que monitora o tráfego, tanto da entrada, quanto de saída. Além disso, age de acordo com o conjunto de regras estabelecidas, ou seja, decide o que pode entrar e qual tráfego específico será bloqueado. O seu principal objetivo é proteger a integridade dos dados, bem como a confidencialidade deles.

4.1.5.48. As funções de Inspeção SSL podem ser habilitadas nos firewalls atuais (Fortigate). Contudo, não são *hardwares* dedicados somente a essa atividade, pois realizam também a Filtragem de pacotes, Web Filter, IDS e IPS e QOS. Além disso, os Firewalls do Ministério trabalham em cluster em modo ativo-passivo, o que quer dizer que em cada momento um deles está responsável pelo tráfego do ambiente.

4.1.5.49. Observa-se que, em certo momento, o device FG1K5D3I17802261 ultrapassou 12 GBPs de throughput e a memória do FG1K5D3I17802243 ultrapassou 82% (ao alcançar o limite de 80% de consumo de memória o equipamento começa a desabilitar funções até que o consumo abaixe novamente a um nível seguro).

4.1.5.50. Ao avaliar as especificações técnicas dos firewalls (Fortigate), atualmente instalados no

ambiente, observou-se que o limite máximo dos equipamentos quando se habilitada a função *SSL-Inspection* atinge capacidade máxima de 5.7GBPs.

4.1.5.51. Sendo assim, caso a função de Inspeção SSL seja utilizada junto ao firewall existente, além de não ter capacidade de throughput necessária para o atual momento, corre-se o risco de afetar os demais serviços existentes. Por fim, torna-se fundamental uma análise dos cenários e soluções viáveis para esta necessidade.

4.1.5.52. Para tanto é requisito fundamental que a nova solução tenha a capacidade de classificar o tráfego que passa pela solução e coordenar para que seja enviado somente aos dispositivos que realmente necessitam inspecioná-lo, tendo em vista melhor combinação das políticas definidas pelo administrador, que determinam o que deve ser interceptado e enviado para um conjunto de serviços de segurança com base no contexto. Este direcionamento de tráfego norteado por políticas permite melhor utilização de investimentos em segurança existentes. A solução de visibilidade SSL deve permitir classificar os diferentes cadeias de serviços baseadas em contextos, considerando, por exemplo: IP de origem e destino, porta de destino, Geolocalização, entre outros.

4.1.5.53. Salienta-se que o Ministério está em fase de implantação e prospecção de diversas aplicações de Segurança Pública, as quais são essenciais na implementação de políticas públicas nos estados. Portanto, é necessário que o Ministério garanta a alta disponibilidade e balanceamento de carga das camadas de serviços de maneira que seja feita a distribuição de tráfego entre os dispositivos ativos mantendo a resiliência dos ambientes em caso de falha da solução.

4.1.5.54. Já quando se trata de proteção nas camadas superiores (camada aplicação), apesar de serem equipamentos modernos e seguros, eles não são dedicados para proteção efetiva na camada de aplicação, que necessita de uma proteção de seus aplicativos com análises comportamentais, defesa proativa contra bots e criptografia na camada de aplicativos de dados confidenciais.

4.1.5.55. Essa proteção pode ser aperfeiçoada com um Web Application Firewall (Firewall de Aplicação Web - WAF), que monitora, filtra e bloqueia pacotes de dados conforme eles viajam de e para um aplicativo da Web. Ele pode ser baseado em rede, host ou em nuvem e é frequentemente implantado através de um proxy.

4.1.5.56. O MJSP possui diversas aplicações e dados sensíveis, os quais devem possuir mecanismos para proteção das credenciais do usuário, sendo que uma delas é o uso de conexões criptografadas (TLS) para impedir que as mesmas sejam interceptadas e o atacante consiga informações sensíveis.

4.1.5.57. Atualmente, um dos principais tipos de ataques do OWASP TOP 10 é baseado na identidade de usuários, tentando explorar dados sensíveis e após isso conseguir dados importantes da aplicação se passando por um usuário válido. Diante disso, visando proteger os dados dos usuários, a solução deve suportar a criptografia de sessões HTTP desde o browser do usuário, provendo proteção contra interceptação por terceiros e evitando ataques do tipo Man in the Browser e Keyloggers.

4.1.5.58. Sendo assim, um Web Application Firewall (Firewall de Aplicação Web - WAF) fornece segurança na Web para serviços on-line contra ataques de segurança mal-intencionados, como injeção SQL, XSS (cross-site scripting). Os WAFs detectam e filtram ameaças que podem degradar, comprometer ou expor aplicativos online a ataques de negação de serviço (DoS). WAFs examinam o tráfego HTTP antes que ele atinja o servidor de aplicativos. Eles também protegem contra a transferência não autorizada de dados do servidor.

4.1.5.59. Diante o exposto sobre segurança em aplicações, torna-se fundamental uma análise, neste projeto, de uma solução de Web Application Firewall (Firewall de Aplicação Web - WAF) sendo dedicado para proteção efetiva da camada de aplicação.

4.1.5.60. É oportuno também destacar o cenário atual do balanceamento de carga entre aplicações. O Ministério possui mais de 200 aplicações sustentadas em produção, as quais são sustentadas por meio de clusters de máquinas virtuais divididos por tecnologias, tanto para servidores de aplicação, como para bancos de dados. As tecnologias de servidores de aplicação atualmente sustentadas pela DTIC/MJSP estão concentradas basicamente em: Jboss, Wildfly, Tomcat, PHP, IIS e Zope Plone, e para Sistemas Gerenciadores de Banco de Dados são divididas em: Microsoft SQL Server, MySQL, PostgreSQL e Oracle.

4.1.5.61. Seguindo as melhores práticas de mercado, a DTIC/MJSP vem desenvolvendo, ao longo dos últimos anos, um trabalho de padronização e automatização em todas as trilhas de desenvolvimento, testes, homologação, produção e treinamento. Como padrão, para cada aplicação em produção, e sempre que necessário, a aplicação é replicada em todas as demais trilhas, de forma que se tenha um processo de integração contínua no desenvolvimento e sustentação das aplicações. Destaca-se que a DTIC/MJSP está preparando o ambiente de infraestrutura, bem como iniciando o desenvolvimento de novas aplicações, no conceito de containers, fato que exigirá ambientes confiáveis e escaláveis.

4.1.5.62. Ainda como um dos projetos a serem implementados pelo MJSP, a solução tecnológica de Big Data Analytics e de plataforma para captura, curadoria, descoberta, análise, mineração e integração de grande volume de dados, tem por objetivo também o Ministério e suas Secretarias, no contexto da execução das políticas públicas, no processo de tomada de decisão em nível estratégico, tático e operacional.

4.1.5.63. Nessa linha, a Nota Técnica n.º 1/2019/CGISE/DTIC/SE/MJ (9159487), elaborada pela Coordenação-Geral de Infraestrutura e Serviços, e que teve como objetivo relacionar as necessidades de contratações para a área de Tecnologia da Informação e Comunicações visando a

evolução e sustentação dos projetos estratégicos do Ministério da Justiça e Segurança Pública, que tratam de sistemas capazes de realizar o processamento e a análise de grandes volumes de dados, denominados "Projetos de Big Data", traz alguns pontos essenciais à execução do projeto, como:

- Principais desafios no processamento de grandes volumes de dados;
- Necessidade de segurança das informações;
- Necessidades tecnológicas e independência de fornecedor;
- Necessidade de expansão da infraestrutura para os projetos de Big Data;
- Arquitetura tecnológica de armazenamento e processamento de dados;
- Arquitetura tecnológica de rede de dados;
- Estrutura física do Data Center do Ministério da Justiça e Segurança Pública.

4.1.5.64. Essa Nota Técnica também reforça, em seu item 4.2, a necessidade de uma arquitetura tecnológica de rede de dados capaz de prover sustentação ao projeto de Big Data Analytics:

> ...
> *A implantação da nova infraestrutura de equipamentos dedicados ao projeto Big Data implicará também na necessidade de expansão da infraestrutura de rede atualmente disponível nos datacenters do MJSP. A intensidade de tráfego que é característica de aplicações que realizam processamento e armazenamento de dados de maneira distribuída demanda que sejam providos equipamentos de rede de garantir a conectividade e a largura de banda entre todos os nós componentes da arquitetura com baixíssima latência e inexistência de oversubscription (ou seja, a capacidade de cursar tráfego dos switches de rede deve ser igual ou superior a somatória da taxa de transferência de todas as suas interfaces somadas).*
> ...

4.1.5.65. Cabe destacar que, em 17/12/2019, não sendo possível continuar com o projeto descrito e planejado no processo 08006.000621/2019-63, foi instituído o processo SEI 08006.001367/2019-11 com a finalidade de materializar o novo planejamento de contratação considerando a demanda existente, conforme Despacho nº 709/2019/CGISE/DTIC/SE/MJ (10421490):

> ...
> *Restando mantida a necessidade detalhada no Documento de Oficialização da Demanda 8740327 e não tendo sido possível atendê-la por meio da contratação planejada no processo atual, deverá ser iniciado novo processo de contratação com a mesma finalidade, havendo, no entanto, espaço para amadurecimento e redefinição das necessidades de acordo com eventual alteração do cenário.*
>
> *Foi instituído o processo SEI08006.001367/2019-11 com a finalidade de materializar o novo planejamento de contratação considerando a demanda existente.*
> ...

4.1.5.66. Diante disso, e tendo como perspectiva a continuidade da contratação de solução de Big Data Analytics, a prevenção de eventuais falhas no ambiente de TI do MJSP, a prospecção de um ambiente seguro com suporte e garantia dos ativos de redes, a garantia dos requisitos de expansibilidade, assim como a reestruturação necessária para atender ao projeto de Big Data Analytics e as futuras demandas e projetos, se faz necessária a aquisição de equipamentos ativos de rede para a Camada Central do MJSP, que contemplem planos de redundância e contingência constituídos por uma série de ações e procedimentos que visam soluções e dispositivos de recuperação relacionados com essas falhas.

4.1.5.67. Diante dos motivos expostos, se faz necessária a contratação de solução de ativos de rede, balanceamento de carga e segurança para os Data Centers, incluindo serviços especializados, aquisição de equipamentos e softwares, modernização e expansão da capacidade atual para atendimento das necessidades do Ministério da Justiça e Segurança Pública.

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

ALINHAMENTO AOS PLANOS ESTRATÉGICOS	
ID	**Objetivos Estratégicos**
ON17	Fortalecer e ampliar a estrutura e os serviços de TI

ALINHAMENTO AO PDTIC 2016-2019		
ID	**Ação do PDTIC**	**Meta do PDTIC associada**
NI14	Atender as Necessidades de dados e informações das áreas meio e finalísticas do MJSP	Aquisição de Solução para prover alta

	[illegible]	disponibilidade do Data Center

ALINHAMENTO AO PAC 2019	
Item	**Descrição**
93	EQUIPAMENTOS BALANCEADORES DE CARGA PARA APLICAÇÕES E LINKS DE DADOS, ANEXO I À RESOLUÇÃO Nº 01, DE 24 DE ABRIL DE 2019 (8645718).
162	REESTRUTURAÇÃO DE INFRAESTRUTURA DE DATACENTER, ANEXO I À RESOLUÇÃO Nº 01, DE 24 DE ABRIL DE 2019 (8645718)

4.3. ***Estimativa da demanda***

4.3.1. **Ativos de redes - Detalhamento de topologias e equipamentos para o site do núcleo central do MJSP.**

4.3.1.1. **Topologia SPINE-LEAF:**

4.3.1.1.1. A topologia é composta por equipamentos que compõem as camadas de SPINE e LEAF (LEAF SERVIÇOS, LEAF SERVIDORES e LEAF BIG DATA).

4.3.1.1.2. Como pode ser observado na Figura 1, são detalhados, de forma meramente ilustrativa, os equipamentos com suas respectivas quantidades de portas, velocidades e conectividade, formando assim o *Fabric*.

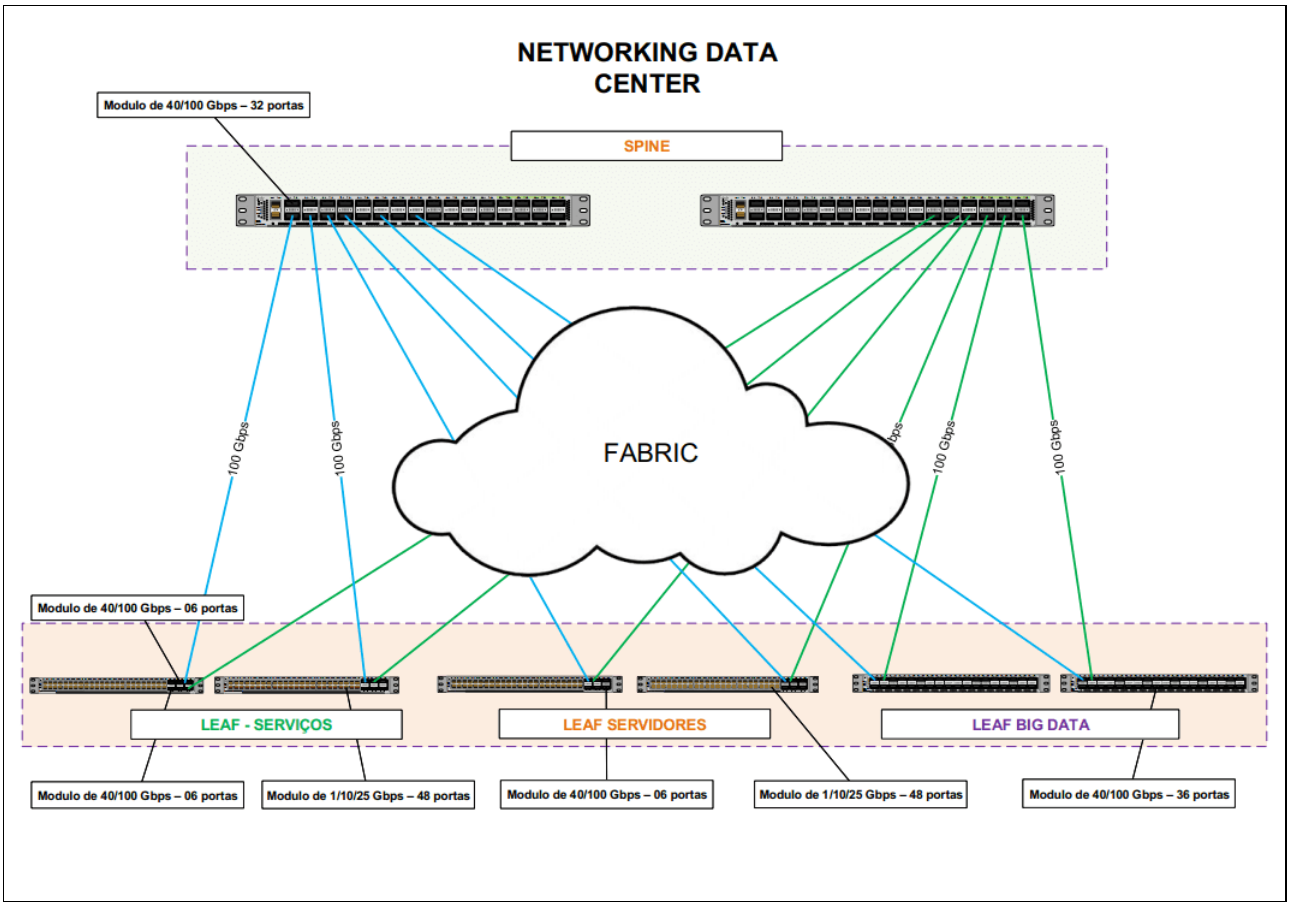

Figura 1- Topologia SPINE-LEAF

4.3.1.1.3. Para os equipamentos na camada SPINE, há a previsão de switches de 32 portas 40/100 Gigabit Ethernet, cujas modularidades foram definidas tomando como base aspectos técnicos considerados como essenciais pela área técnica responsável, assim como características de escalabilidade para uso estimado de 05 (cinco) anos.

4.3.1.1.4. Os switches do SPINE, inicialmente, se conectam com os switches LEAFS (LEAF SERVIÇOS, LEAF SERVIDORES e LEAF BIG DATA) a uma velocidade de conexão de 100 Gbps em cada porta. Para interconexão entre os switches do SPINE e os switches LEAFS estão sendo previstos Cabos de Conexão Direta de 100 Gbps.

4.3.1.1.5. O quantitativo de equipamentos para a camada SPINE, bem como os Cabos de Conexão Direta para conexão dos LEAF, são:

CAMADA SPINE	
Quantidade	**Descrição**
02	Switches de Núcleo (Core Switch), composto por 32 (trinta e duas) portas 40/100 Gigabit Ethernet, em cada switch, para interconexão com os switches Leafs (LEAF SERVIÇOS, LEAF SERVIDORES e LEAF BIG DATA)
12	Cabos de Conexão Direta 100G – (10 metros, mínimo)

Tabela 01 - quantitativos camada Spine

4.3.1.2. **Topologia LEAF SERVIÇOS:**

4.3.1.2.1. O LEAF SERVIÇOS irá concentrar toda a parte de conectividade externa e interna da rede, bem como serviços acessórios que não estarão diretamente conectados nos LEAF SERVIDORES e LEAF BIG DATA. Inicialmente estarão conectados no referido LEAF os seguintes serviços:

a) Controladoras Wi-fi;

b) Roteador Telebras (internet e MPLS);

c) Switch SERPRO (Internet e INFOVIA);

d) Firewalls (interno e externo);

e) Switches de agregação dos andares;

4.3.1.2.2. Além disso, para o provisionamento de portas UTPs, serão reaproveitados dois equipamentos existentes no Data Center, Extensor de fabric Cisco Nexus 2348 com 48 portas 1/10G, 6 portas de uplink 40G QSFP (PART NUMBER N2K-C2348TQ), que foram adquiridos por meio do Processo Administrativo nº (08006.001634/2016-15). Inicialmente estarão conectados aos Extensor de fabric Cisco Nexus 2348 os seguintes serviços:

a) Gateway SIP;

b) Aceleradores de WAN;

c) Videoconferência

d) Thalles

4.3.1.2.3. Para conexão entre os novos equipamentos, e os existentes, serão reaproveitados cabos de Conexão Direta de 40 Gbps que acompanham o Extensor de fabric Cisco Nexus 2348.

4.3.1.2.4. Conforme ilustrado na Figura 2, a topologia LEAF SERVIÇOS é composta por equipamentos de alta disponibilidade de banda, baixa latência e expansíveis:

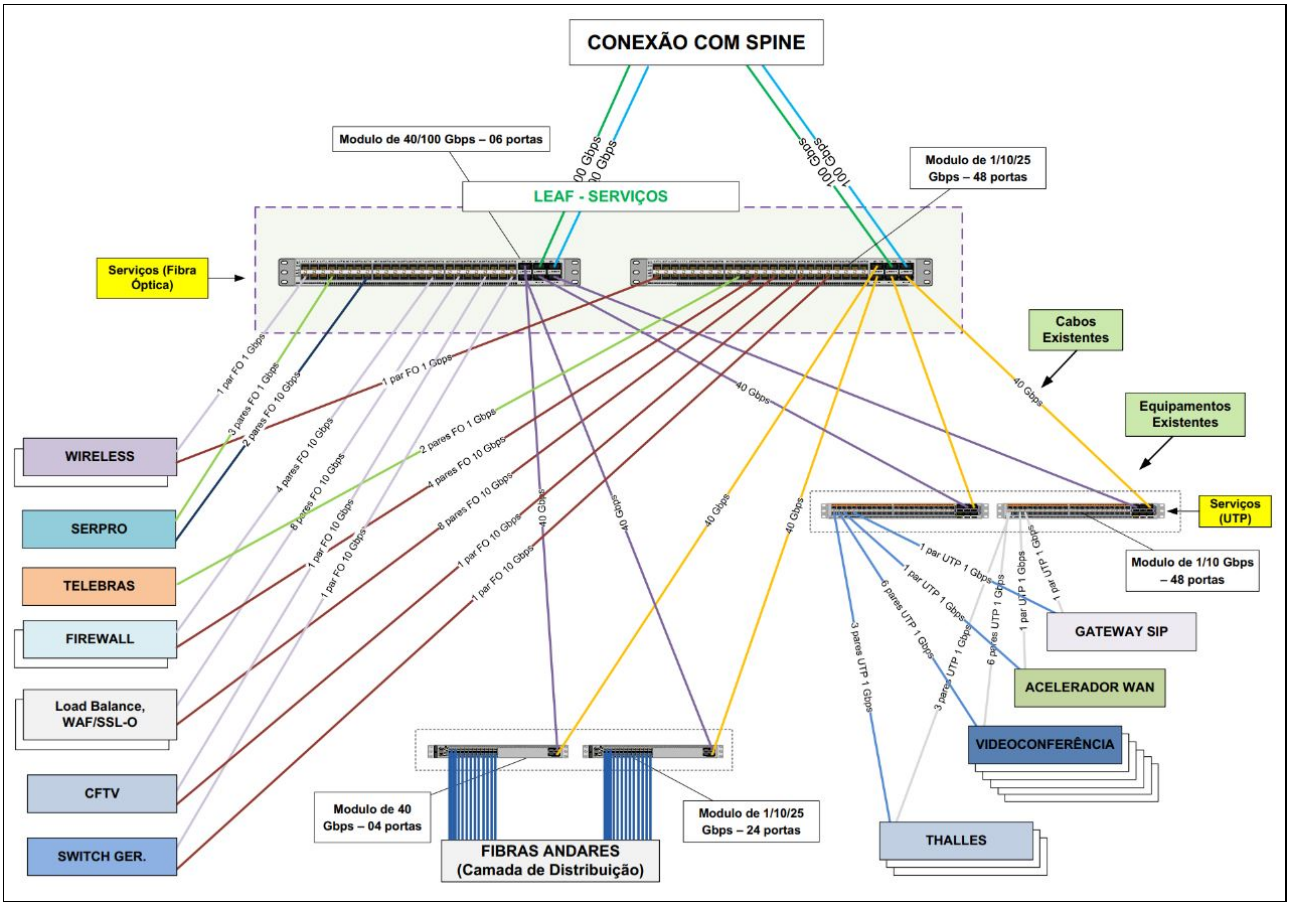

Figura 2- LEAF - SERVIÇOS

4.3.1.2.5. Para os equipamentos do LEAF SERVIÇOS, há a previsão de switches com no mínimo de 48 portas 1/10/25 Gbps, com no mínimo 6 portas de 40/100 Gigabit Ethernet, cujos os aspectos foram

definidos tomando como base requisitos técnicos considerados como primordiais pela área técnica responsável, assim como características de crescimento para uso estimado de 05 (cinco) anos. Deverão ser previstos transceivers, totalmente compatíveis tecnologicamente com os equipamentos, para interconexão dos demais equipamentos (*Firewalls,* controladoras *Wi-fi*, Aceleradores de WAN e Roteador Telebras, Switch SERPRO e gateway SIP).

4.3.1.2.6. Para os equipamentos de agregação dos andares, há a previsão de switches com no mínimo 24 portas 1/10/25 Gbps, contendo no mínimo 4 portas de 40G, que serão ligados às fibras dos andares, assim como há previsão de Transceivers para interconexão dos andares, tanto para o lado do Data Center, quanto para as 16 (dezesseis) salas técnicas. Os equipamento atualmente existentes nas 16 salas técnicas e que fazem a distribuição são do modelo WSC3650-24PD (PART NUMER C1-WS3650-24PD/K9). Aqui, cabe destacar a necessidade dos transceivers serem totalmente compatíveis tecnologicamente com os equipamentos que fazem a distribuição nos andares (Modelo de transceivers atualmente instalados: SFP-10G-SR), pois qualquer modificação necessária por incompatibilidade pode causar impacto no acesso dos usuários à rede MJSP.

4.3.1.2.7. É importante também prever conectividade para soluções que serão renovadas em um futuro próximo, como é o caso da Solução de Segurança de Perímetro (Firewall - Processo 08006.001190/2016-18), e que necessitam de conexões junto ao LEAF SERVIÇOS, sendo um requisito fundamental que essas ligações promovam maiores capacidades de tráfego, largura de banda e densidade.

4.3.1.2.8. Nessa linha, após análise técnica, se faz necessário para nova Solução de Segurança de Perímetro (Firewall) que este projeto contemple Transceivers, 25G Multimodo, LC, totalmente compatível com os switches de 48.

4.3.1.2.9. Para interligação dos equipamentos do LEAF SERVIÇOS com o Switches de agregação dos andares, deverão ser previstos Cabos de Conexão Direta de 40 Gbps.

4.3.1.2.10. Sendo assim, projeta-se que esses switches supram os requisitos expostos, com eficiência na comunicação, alta disponibilidade de banda e baixa latência entre os nós.

4.3.1.2.11. Abaixo são expostos os quantitativos necessários para o dimensionamento do LEAF SERVIÇOS:

LEAF - SERVIÇOS	
Quantidade	**Descrição**
02	Switches de Agregação, composto por, no mínimo, 48 (quarenta e oito) portas, 1/10/25, com no mínimo 06 portas de 40/100, em cada switch;
02	Switches de Agregação composto por, no mínimo, 24 (vinte e quatro) portas 1/10/25, com no mínimo 04 portas de 40G, em cada switch;
04	Cabos de Conexão Direta 40G, 10 metros, mínimo
90	Transceivers, 10G Multimodo, LC, totalmente compatível com os switches de 48 e 24 portas
16	Transceivers, 25G Multimodo, LC, totalmente compatível com os switches de 48.
30	Cordões Óptico, 10G Multimodo, LCxLC, 10 metros, mínimo

***Tabela 02 - quantitativos* LEAF SERVIÇOS**

4.3.1.3. **<u>Topologia LEAF SERVIDORES</u>**

4.3.1.3.1. O LEAF SERVIDORES, como o próprio nome já diz, irá concentrar todos os servidores do Data Center.

4.3.1.3.2. Conforme descrito na Figura 3, a topologia LEAF SERVIDORES também será composta por equipamentos de alta disponibilidade de banda, baixa latência e expansíveis:

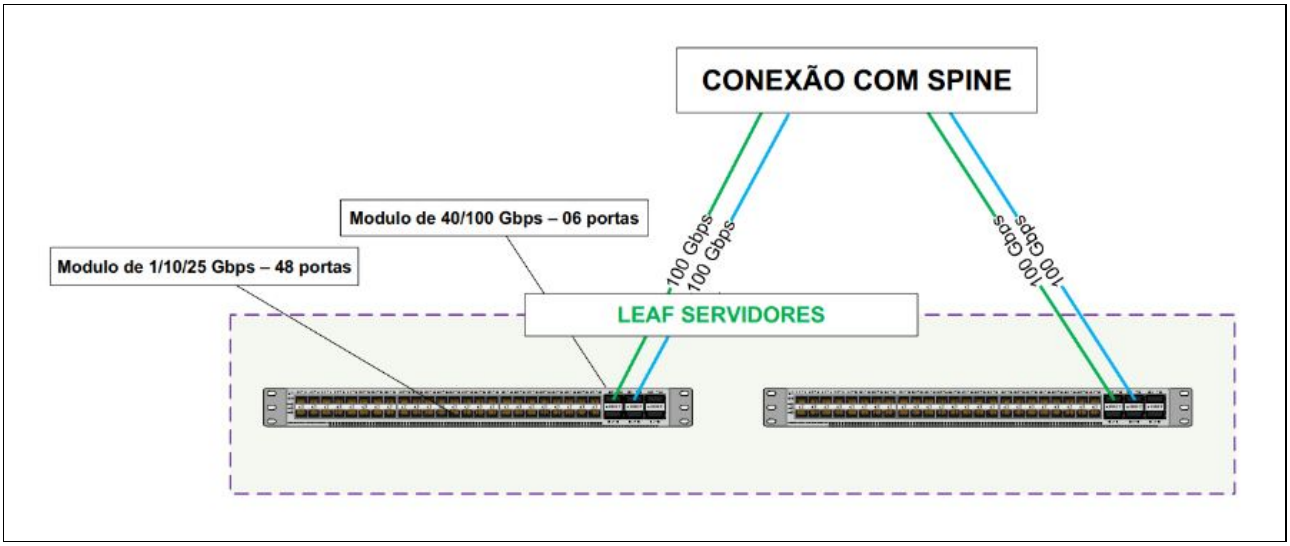

Figura 3 - LEAF SERVIDORES

4.3.1.3.3. Para os equipamentos do LEAF SERVIDORES, há a previsão de switches com no mínimo de 48 portas 1/10/25 Gbps, com no mínimo 6 portas de 40/100 Gigabit Ethernet, os quais foram determinados com base nos requisitos técnicos considerados fundamentais pela área técnica, assim como características de ampliação para uso estimado de 05 (cinco) anos. Deverão ser previstos

transceivers, totalmente compatíveis tecnologicamente com os equipamentos, para interconexão dos servidores aos switches do LEAF SERVIDORES.

4.3.1.3.4. Com isso, entende-se que esses switches supram as exigências apresentadas, com aprimoramento de tráfego leste-oeste, eficiência na comunicação, alta disponibilidade de banda e baixa latência entre os nós.

4.3.1.3.5. Abaixo são expostos os quantitativos necessários para o dimensionamento do LEAF de SERVIDORES:

LEAF SERVIDORES	
Quantidade	**Descrição**
02	Switches de Agregação, composto por, no mínimo, 48 portas, 1/10/25, com no mínimo 6 portas 40/100, em cada switch;
20	Cordão Óptico,10/40G Multimodo, LCxLC, 10 metros, mínimo;
20	Cordão Óptico,10G Multimodo, LCxLC, 05 metros, mínimo;
04	Cabos de Conexão Direta 40G, 10 metros, mínimo.

***Tabela 03 - quantitativos* LEAF SERVIDORES**

4.3.1.4. **Topologia LEAF BIG DATA**

4.3.1.4.1. O LEAF BIG DATA, como o próprio nome já diz, irá concentrar todos os equipamentos da solução Big Data que está sendo prospectada pela CGISE.

4.3.1.4.2. Destaca-se que por meio do processo 08006.000621/2019-63 foi inciada a aquisição de uma solução de Big Data. No decorrer do processo vislumbrou-se a possibilidade de adesão da ARP do Pregão nº 11/2018 - CML/MD. No entanto, após a análise mais aprofundada da equipe de planejamento da contratação, optou-se por iniciar uma nova contratação (08006.001367/2019-11), que ainda está sendo prospectada.

4.3.1.4.3. Tendo em vista que o projeto de Big Data é estratégico para o Ministério, e necessitará de conectividade com o restante da rede, quando implantada, será previsto um LEAF exclusivo para a referida solução. Entretanto a equipe de planejamento do projeto de Big Data deverá incluir em seu escopo equipamentos de rede, transceivers e cabos necessários, com total compatibilidade com o LEAF BIG DATA que está sendo adquirido no presente processo.

4.3.1.4.4. Sendo assim, projeta-se que esses switches (LEAF BIG DATA) supram a necessidade da solução de Big Data, que demandam otimização de tráfego leste-oeste e eficiência na comunicação, dependendo de uma alta disponibilidade de banda e baixa latência entre os nós.

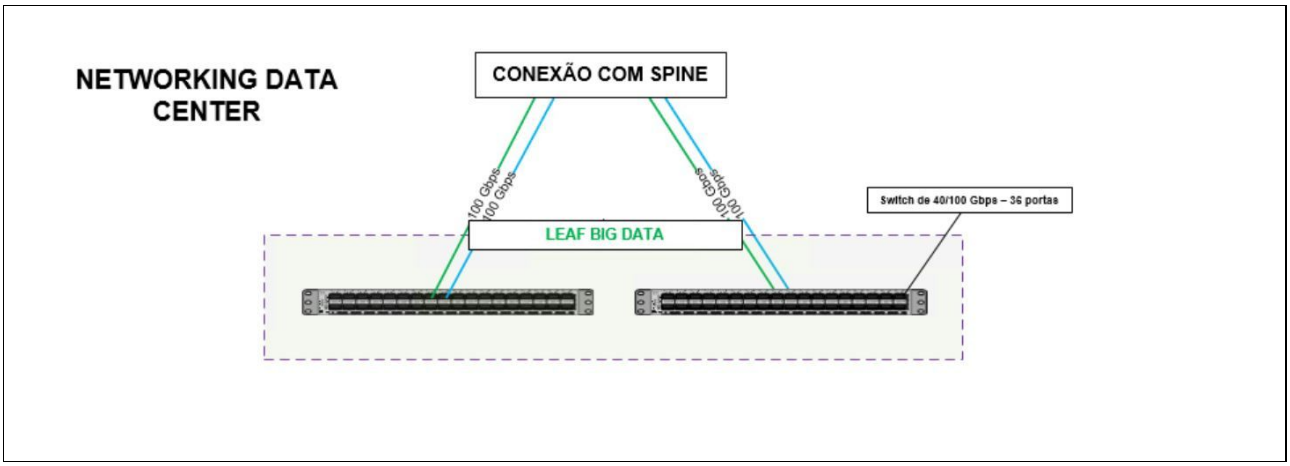

Figura 4 - LEAF BIG DATA

4.3.1.4.5. Conforme detalhado na Figura 4, a topologia LEAF BIG DATA, assim como as demais camadas LEAF, é composta por equipamentos de alta disponibilidade de banda, baixa latência e expansíveis.

4.3.1.4.6. Para os equipamentos da LEAF BIG DATA, há a previsão de switches com no mínimo de 36 portas 40/100 Gigabit Ethernet, cujas modularidades foram definidas tomando como base aspectos técnicos considerados como essenciais pela área técnica responsável, assim como características de expansibilidade para uso estimado de 05 (cinco) anos.

4.3.1.4.7. Cabe frisar que não há previsão de Switches (topo de rack) para atendimento da solução Big Data, como já exposto, pois isso ficará a cargo da equipe que fará o projeto de Big Data.

4.3.1.4.8. Abaixo são expostos os quantitativos necessários para o dimensionamento do LEAF BIG DATA:

LEAF BIG DATA	
Quantidade	**Descrição**
02	Switches de Agregação composto por, no mínimo, 36 (trinta e seis) portas 40/100 Gigabit Ethernet, em cada switch;

***Tabela 04 - quantitativos* LEAF BIG DATA**

4.3.2. **Ativos de redes - Detalhamento de topologias e equipamentos para o site do CICCN-DF.**

4.3.2.1. **Topologia SPINE-LEAF**

4.3.2.1.1. Como pode ser observado na Figura 5, a topologia SPINE-LEAF CICCN-DF é semelhante a do Site Principal (Figura 1), sendo composta por equipamentos das camadas de SPINE e LEAF (LEAF SERVIÇOS, LEAF SERVIDORES e LEAF BIG DATA).

4.3.2.1.2. Destaca-se que serão detalhados, de forma meramente ilustrativa, os equipamentos com suas respectivas quantidades de portas, velocidades e conectividade, formando assim o *Fabric*.

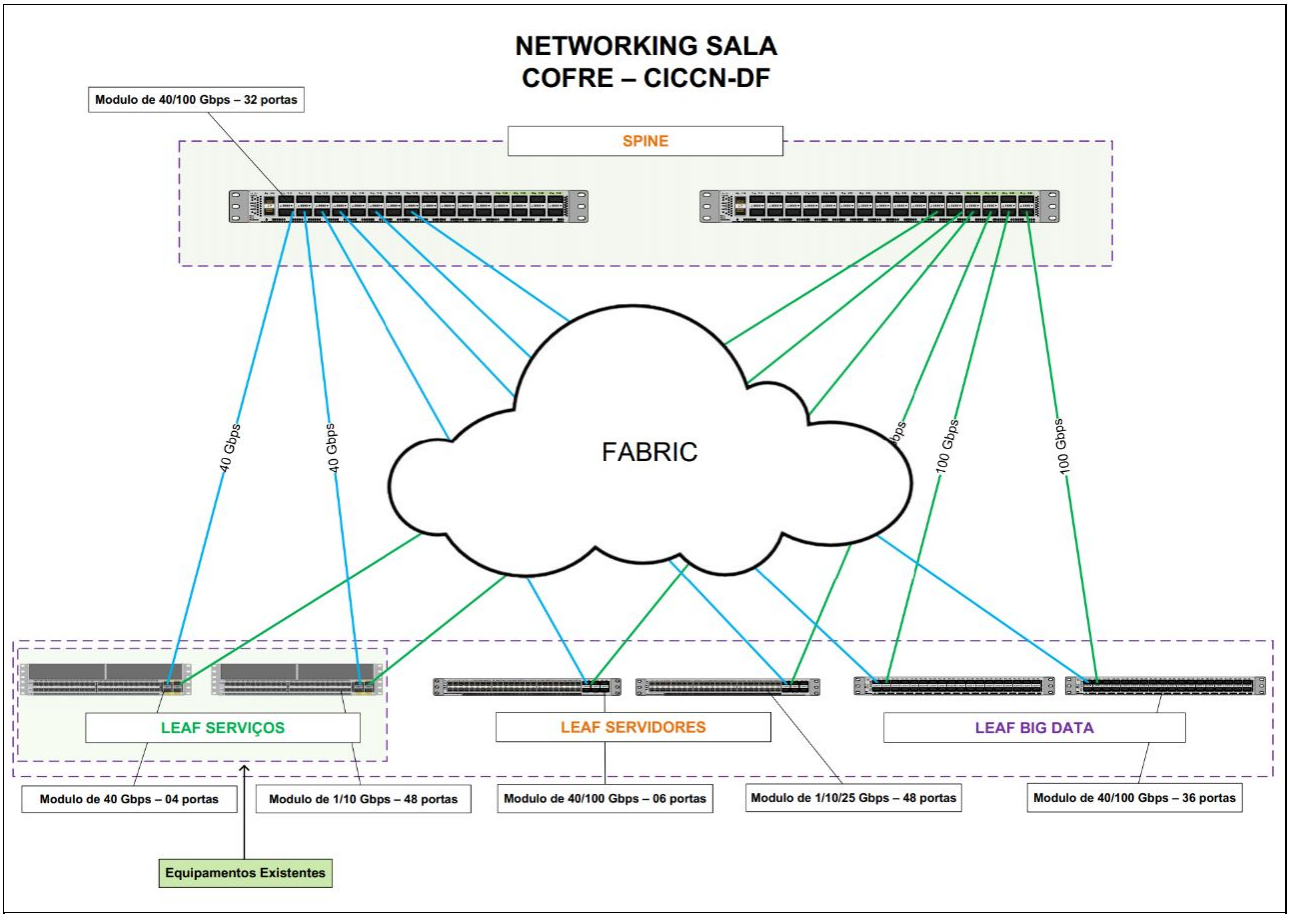

Figura 5 - SPINE LEAF CICCN-DF

4.3.2.1.3. Para os equipamentos na camada SPINE, há a previsão de switches de 32 portas 40/100 Gigabit Ethernet, cujas modularidades foram definidas tomando como base aspectos técnicos considerados como essenciais pela área técnica responsável, assim como características de escalabilidade para uso estimado de 05 (cinco) anos.

4.3.2.1.4. Os switches do SPINE, inicialmente, se conectam com os switches LEAFS (LEAF SERVIDORES e LEAF BIG DATA) a uma velocidade de conexão de 100 Gbps em cada porta, e no caso do LEAF SERVIÇOS, será feita a conexão a uma velocidade de 40 Gbps. Para interconexão entre os switches do SPINE e os switches LEAFS estão sendo previstos Cabos de Conexão Direta de 100 Gbps, com exceção do LEAF SERVIÇOS que necessitará de Cabos de Conexão Direta de 40 Gbps.

4.3.2.1.5. Por fim, da mesma forma que na definição da arquitetura de rede do núcleo central do MJSP, foi levado em consideração na definição dos quantitativos de switches e portas de cada equipamento a relação entre Spine x Leaf x servidores, de forma a minimizar o *oversubscription* na rede, inclusive considerando alguns cenários de múltiplas falhas dos equipamentos e de suas conexões, de modo que se possa escoar todo o tráfego (ou grande parte dele) entre as referidas camadas.

4.3.2.1.6. O quantitativo de equipamentos para a camada SPINE, bem como os Cabos de Conexão Direta para conexão dos LEAF, são:

SPINE LEAF CICCN-DF	
Quantidade	**Descrição**
02	Switches de Núcleo (Core Switch), composto por 32 (trinta e duas) portas 40/100 Gigabit Ethernet, em cada switch, para interconexão com os switches LEAFS (LEAF SERVIÇOS, LEAF SERVIDORES e LEAF BIG DATA)
08	Cabos de Conexão Direta 100 Gbps – (10 metros, mínimo)
04	Cabos de Conexão Direta 40 Gbps – (10 metros, mínimo)

Tabela 05 - quantitativos camada Spine CICCN

4.3.2.2. **Topologia LEAF SERVIÇOS**

4.3.2.2.1. Importante salientar, que pelo fato do Data Center do CICCN-DF estar sendo projetado para redundância do Data Center do núcleo central, além do fato de existir somente uma sala técnica (pétala H do complexo da DPRF), alguns equipamentos estão sendo reduzidos ou adaptados nos LEAFES.

4.3.2.2.2. O LEAF SERVIÇOS da Sala Cofre do CICCN-DF, como pode ser observado na Figura 6, possui menor quantidade de equipamentos que o mesmo LEAF no Data Center do MJ, tendo em vista menor quantidade de serviços a serem atendidos. Inicialmente estarão conectados no referido LEAF os seguintes serviços:

a) Switch SERPRO (INFOVIA);

b) Firewalls (interno e externo);

c) Interligação com a sala técnica a pétala H do complexo da DPRF (DIOP);

4.3.2.2.3. Conforme ilustrado na Figura 6, a topologia LEAF SERVIÇOS é composta por equipamentos de alta disponibilidade de banda, baixa latência e expansíveis:

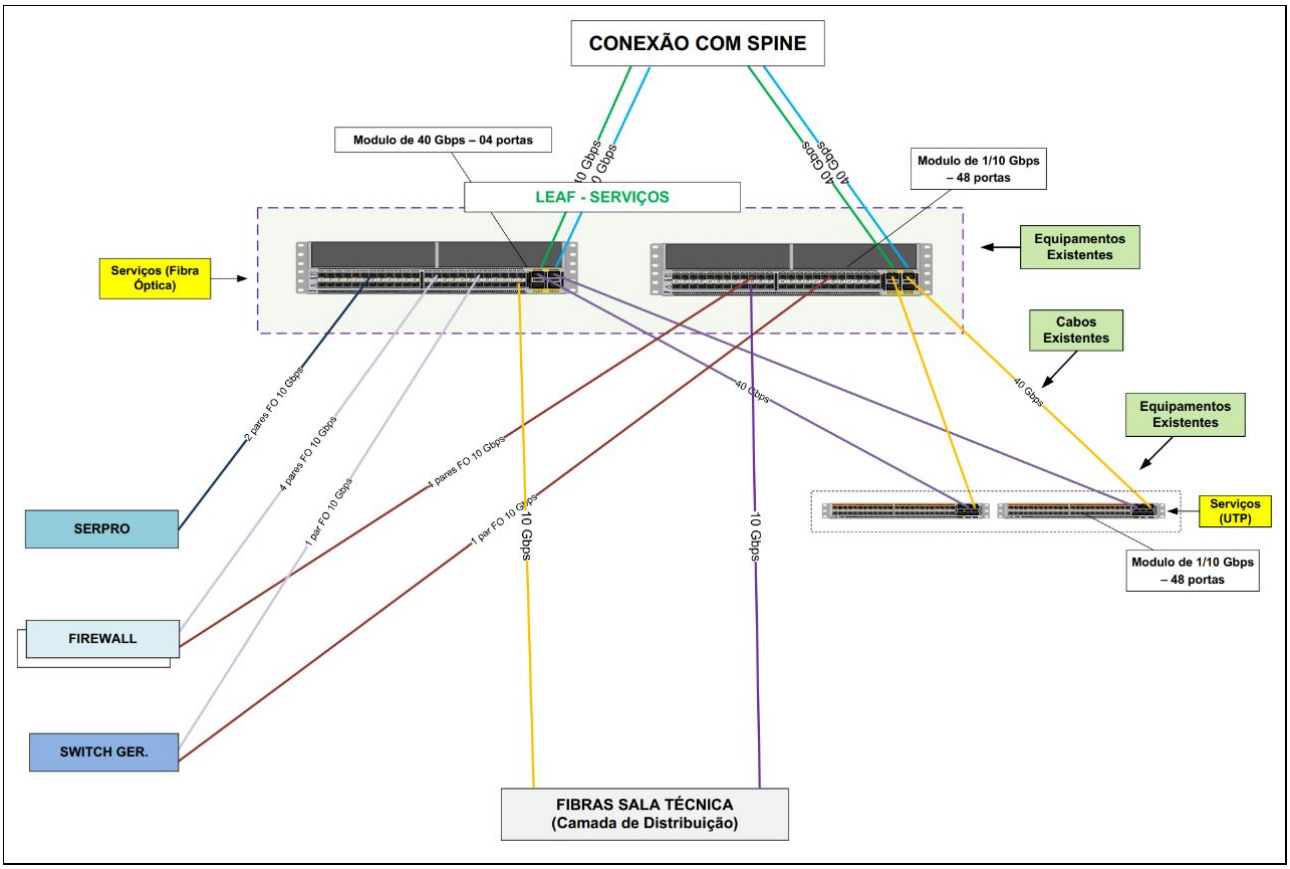

Figura 6 - LEAF SERVIÇOS CICCN-DF

4.3.2.2.4. Destaca-se que os equipamentos que compõe o LEAF SERVIÇOS do CICCN (Switches Cisco Nexus 56128P 48 portas 10G SFP Ethernet - PART NUMBER N5K-C56128P) e Extensor de fabric Cisco Nexus 2348 com 48 portas 1/10G, 6 portas de uplink 40G QSFP (PART NUMBER N2K-C2348TQ), equipamentos adquiridos por meio do Processo Administrativo nº (08006.001634/2016-15), serão reaproveitados, pois atualmente encontram-se instalados no Data Center do INFOSEG e ainda com suporte e garantia do fabricante.

4.3.2.2.5. Para os dois Switches Cisco Nexus 56128P será necessária a aquisição licenciamento para que possam permitir a configuração do protocolo Virtual Extensible LAN (VXLAN) – que permite a criação de segmentos de redes virtuais e sua extensão através da camada de redes (nível 3) ao encapsular quadros Ethernet em pacotes IP através de UDP. Além disso, deve propiciar a configuração do protocolo de roteamento dinâmico BGPv4 para IPv4 e IPv6.

4.3.2.2.6. Abaixo são expostos os quantitativos necessários para o dimensionamento do LEAF SERVIÇOS:

LEAF SERVIÇOS	
Quantidade	**Descrição**
12	Transceivers, 10G Multimodo, LC, totalmente compatível com os switches de 48 portas
12	Cordões Óptico, 10G Multimodo, LCxLC, 10 metros, mínimo

***Tabela 06 - quantitativos* LEAF SERVIÇOS**

4.3.2.3. **Topologia LEAF SERVIDORES**

4.3.2.3.1. O LEAF SERVIDORES da Sala Cofre do CICCN, possui exatamente a mesma topologia (Figura 3), e equipamentos que o LEAF correspondente no Data Center do MJ.

4.3.2.3.2. Abaixo são expostos os quantitativos necessários para o dimensionamento do LEAF de SERVIDORES:

LEAF SERVIDORES	
Quantidade	**Descrição**
02	Switches de Agregação, composto por, no mínimo, 48 portas, 1/10/25, com no mínimo 6 portas 40/100, em cada switch;
20	Transceivers, 10G Multimodo, LC, totalmente compatível com os switches de 48 portas
20	Cordões Óptico, 10G Multimodo, LCxLC, 10 metros, mínimo

***Tabela 07 - quantitativos* LEAF SERVIDORES**

4.3.2.4. **Topologia LEAF BIG DATA**

4.3.2.4.1. O LEAF BIG DATA da Sala Cofre do CICCN, possui exatamente a mesma topologia (Figura 22), e equipamentos que o LEAF correspondente no Data Center do MJ.

4.3.2.4.2. Abaixo são expostos os quantitativos necessários para o dimensionamento do LEAF BIG DATA:

LEAF BIG DATA	
Quantidade	**Descrição**
02	Switches de Agregação composto por, no mínimo, 36 (trinta e seis) portas 40/100 Gigabit Ethernet, em cada switch

Tabela 08 - quantitativos LEAF BIG DATA

4.3.3. **Detalhamento de topologias e equipamentos de balanceamento de carga para o site do núcleo central do MJSP.**

4.3.3.1. Abaixo encontram-se as topologias, meramente ilustrativas, que detalham cada conexão:

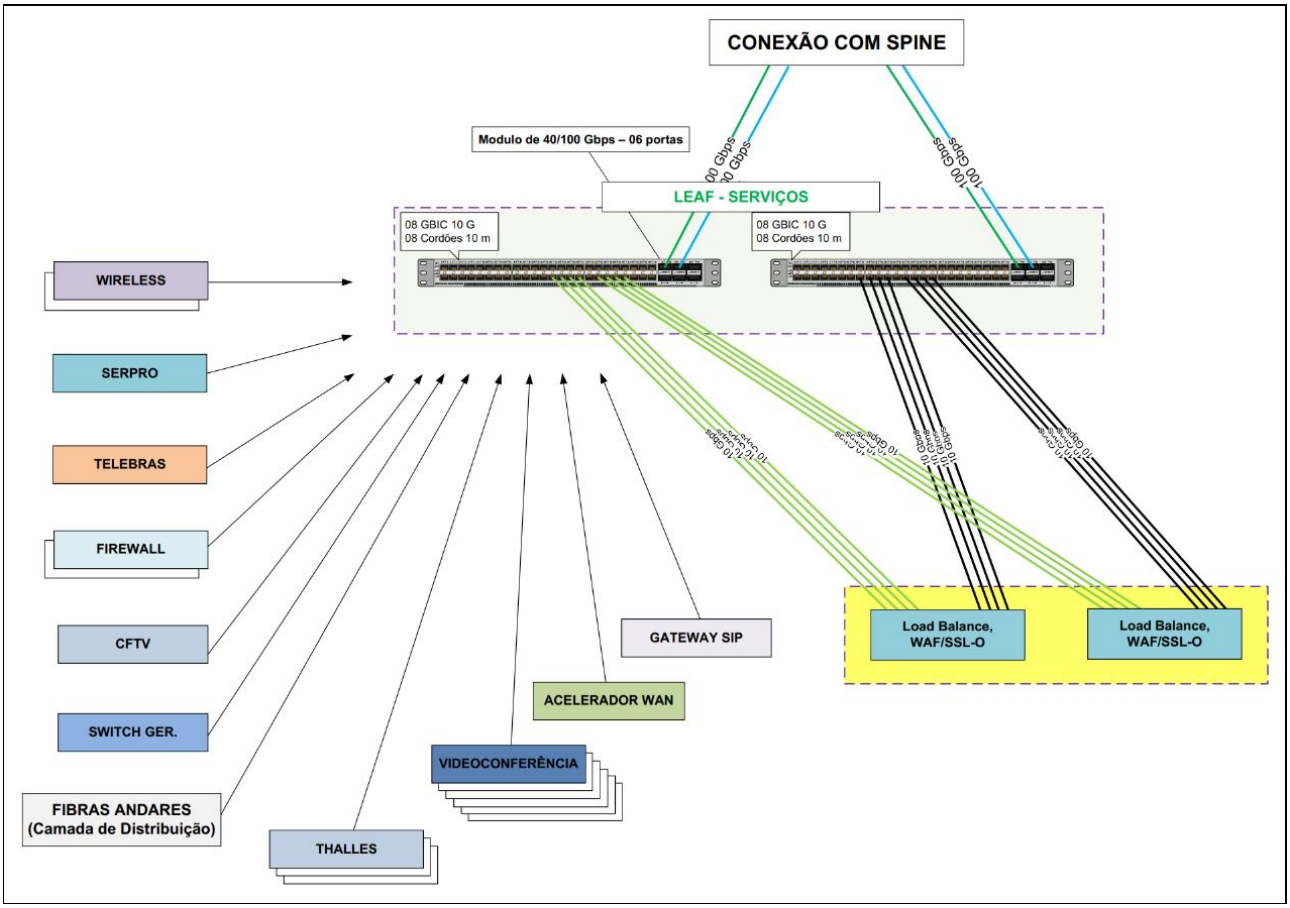

Figura 7 - Balanceamento de carga, SSL-O, WAF

4.3.3.1.1. Conforme visto na Figura 7, os equipamentos, uma parte da solução de balanceamento de carga e segurança serão instalados no LEAF SERVIÇOS.

4.3.3.1.2. Com o objetivo de suportar altas cargas de processamento (tratamento de tráfego SSL), vislumbra-se a implementação de solução física (*appliances* físicos).

4.3.3.1.3. Para funcionalidades não triviais, que demandam pouco processamento e recursos de hardware (CPU, memória e interfaces de rede), optou-se pela implementação de uma solução virtualizada.

4.3.3.1.4. Com o objetivo de solucionar a demanda de um Web Application Firewall (Firewall de Aplicação Web - WAF), a melhor solução escolhida foi a aquisição de Licença para solução de segurança e balanceamento de carga (GSLB, WAF, DDoS, MFA/SSO), sendo dedicado para proteção efetiva da camada de aplicação.

4.3.3.1.5. Para realizar as conexões junto ao LEAF SERVIÇOS, serão utilizados Transceiver 10G Multimodo (LC), bem como os respectivos cabos de conexão, com no mínimo 10 metros.

4.3.3.1.6. Será necessário também treinamento na solução e Operação Assistida.

4.3.3.1.7. Abaixo são expostos os quantitativos necessários para o dimensionamento da solução de segurança e balanceamento de carga e segurança:

SOLUÇÃO DE BALANCEAMENTO DE CARGA E SEGURANÇA - LEAF SERVIÇOS - NÚCLEO CENTRAL	
Quantidade	**Descrição**
02	Solução de segurança e balanceamento de carga - Appliance Físico - Tipo A
16	Transceiver 10G Multimodo LC
01	Operação Assistida

Tabela 09 - quantitativos SOLUÇÃO DE BALANCEAMENTO DE CARGA E SEGURANÇA - NÚCLEO CENTRAL

4.3.4. **Detalhamento de topologias de balanceamento de carga e segurança para o site do CICCN-DF.**

4.3.4.1. A solução de balanceamento de carga e segurança no Data Center do CICCN-DF, será implementada de forma virtualizada, tendo em vista que demandam menor processamento e recursos de hardware (CPU, memória e interfaces de rede).

4.3.4.2. Esta solução deve ser baseada em um serviço de subscrição, com direito de uso pelo período de 36 (trinta e seis meses), tendo como volume máximo contratado de *throughput* 20 (vinte) Gbps.

4.3.4.3. Além disso, é requisito fundamental que a solução ofereça suporte técnico especializado no ambiente configurado, sendo esses de forma **corretiva, preventiva e evolutiv**a.

4.3.4.4. Os serviços de **natureza corretiva** são aqueles efetuados com objetivo de solucionar problemas de funcionamento e disponibilidade da solução e de esclarecer dúvidas relacionadas à instalação, configuração, uso e atualização dos produtos;

4.3.4.5. Os serviços de **natureza preventiva** são aqueles nas quais a CONTRATADA, mediante visita trimestral (on-site), realiza uma checagem da saúde e funcionamento da solução já implementada, permitindo um diagnóstico preciso do status atual da rede;

4.3.4.6. Os serviços de **natureza evolutiva** são aqueles em que a CONTRATADA, mediante solicitação da CONTRATANTE, implementará atualizações de software para os equipamentos, mantendo a solução em pleno funcionamento e na versão desejada pela CONTRATANTE.

4.3.4.7. Além de serviços de implementação de melhorias da solução implementada, os serviços especializados também poderão ser utilizados para:

- Desinstalação/reinstalação da solução;
- Consultoria Especializada;
- Repasse adicional de conhecimento.

4.3.4.8. Com isso, temos o serviço da Solução de Segurança e Balanceamento de carga – aaS que traz como principal benefício a flexibilidade e dinamicidade que o modelo de *Enterprise Agreement* oferece, assim como, ao adquirir um pacote de *throughput* (20 Gbps, por exemplo), passa a poder utilizar tal capacidade na mesma medida de suas necessidades, podendo serem aprovisionadas quantas e em quaisquer tamanhos de máquinas sejam necessárias desde que somadas utilizem o *throughput* total contratado.

4.3.4.9. Com base no mencionado, temos o seguinte dimensionamento:

SOLUÇÃO DE BALANCEAMENTO DE CARGA E SEGURANÇA - CICCN-DF	
Quantidade	**Descrição**
01	Solução de segurança e balanceamento de carga - Tipo B (Ambiente Virtual) para 36 meses

***Tabela 10 - quantitativos* SOLUÇÃO DE BALANCEAMENTO DE CARGA E SEGURANÇA - CICCN-DF**

4.3.5. **Tabela Detalhada dos Quantitativos**

TABELA DETALHADA DOS QUANTITATIVOS

Data Center MJSP - SEDE			
ID	**Descrição**	**Tipo**	**Quantidade**
1.	Switch SPINE 32 portas	Equipamento	02
2.	Cabo de Conexão Direta 100G – (10 metros)	Equipamento	12
3.	Switch LEAF - Tipo A - 48 portas (LEAF SERVIÇOS)	Equipamento	02
4.	Transceiver 10G Multimodo (LC)	Equipamento	90
5.	Transceivers, 25G Multimodo (LC)	Equipamento	16
6.	Cordão Óptico Duplex, 10G Multimodo,(LC/LC) (10 metros)	Consumo	30
7.	Switch de Agregação - 24 portas (LEAF SERVIÇOS)	Equipamento	02
8.	Cabo de Conexão Direta 40G – (10 metros)	Equipamento	04
9.	Switch LEAF - Tipo A - 48 portas (LEAF SERVIDORES)	Equipamento	02
10.	Transceiver 10G Multimodo (LC)	Equipamento	48
11.	Switch LEAF - Tipo B (BIG DATA)	Equipamento	02
Sala Cofre - CICCN			
12.	Switch SPINE 32 portas	Equipamento	02
13.	Cabo de Conexão Direta 100G – (10 metros)	Equipamento	08
14.	Cabo de Conexão Direta 40G – (10 metros)	Equipamento	04
15.	Switch LEAF - Tipo A - 48 portas (LEAF SERVIÇOS)	-	-
16.	Licenciamento Switches existentes (Cisco Nexus 5600 Series)	Software	02
17.	Transceiver 10G Multimodo (LC)	Equipamento	12
18.	Cordão Óptico Duplex, 10G Multimodo,(LC/LC) (10 metros)	Consumo	12
19.	Switch LEAF - Tipo A - 48 portas (LEAF SERVIDORES)	Equipamento	02
20.	Transceiver 10G Multimodo (LC)	Equipamento	20
21.	Cordão Óptico Duplex, 10G Multimodo,(LC/LC) (10 metros)	Consumo	20
22.	Switch LEAF - Tipo B (BIG DATA)	Equipamento	02
Data Center MJSP - SEDE e Sala Cofre - CICCN			
23.	Sistema de Gerenciamento de Equipamentos de Data Center	Software	01
24.	Solução de Controle de Acesso – Virtual Machine	Software	01
25.	Operação Assistida	Serviço	01
Segurança Aplicada a Redes: Aquisição de Solução de Balanceamento de Carga e Segurança			
26.	Solução de segurança e balanceamento de carga - Appliance Físico - Tipo A	Equipamento	02
27	Subscrição de licença para solução de segurança e balanceamento de carga - Tipo B (Ambiente Virtual) para 36 meses	Serviço	01
28	Transceiver 10G Multimodo LC	Equipamento	16
29	Operação Assistida	Serviço	01

Tabela 11 - Tabela Detalhada dos Quantitativos

4.4. ***Parcelamento da Solução de TIC***

4.4.1. 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.

4.4.2. A presente contratação está sendo dividida em 2 Grupos (Grupo 1 - Ativos de Redes e Serviços e Grupo 2 - Ativos, soluções e serviços de Balanceamento de Carga).

4.4.2.1. O Grupo 1 possui a quantidade de 13 itens, sendo tecnicamente inviável o desmembramento do grupo em itens isolados devido à complexidade e riscos envolvidos na definição e integração de todos os ativos, serviços de instalação e manutenção necessários para prover, por completo, o perfeito funcionamento e compatibilidade dos equipamentos.

4.4.2.2. O Grupo 2 possui a quantidade de 4 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, serviços de instalação e manutenção necessários para prover, por completo, o perfeito funcionamento e compatibilidade dos equipamentos.

4.4.2.3. Para a presente contratação, devido à complexidade dos equipamentos e serviços envolvidos, está sendo considerado que cada Grupo (1 e 2) deverá ser adjudicado, cada um, por valor global, não sendo tecnicamente viável o desmembramento dos Grupos em itens isolados.

4.4.2.4. Portanto, 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.

4.5. **Justificativa para Não Participação de Consórcios e Cooperativas**

4.5.1. **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).*

4.5.2. 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 (...)".

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

4.6.1. Reestruturar e modernizar a arquitetura de rede do Ministério, provendo a reestruturação da camada core da rede e consolidação da camada de agregação do Data Center.

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

4.6.3. Prover a mitigação de impactos para as áreas de negócios decorrentes de problemas no funcionamento dos equipamentos de conectividade de rede.

4.6.4. Aumentar a velocidade de conexão entre os servidores e ativos de rede do Data Center.

4.6.5. Prover solução de gerenciamento e monitoramento eficiente dos ativos de rede do Data Center.

4.6.6. Prover mecanismos de alta disponibilidade, mecanismos de segurança e balanceamento de carga entre Data Centers dos ambientes de infraestrutura do MJSP.

4.6.7. Prover substituição de ativos de rede, sem contrato de garantia e suporte, do núcleo central do MJSP e da sala cofre do CICCN.

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

4.6.9. Manter as soluções com suporte e garantia do fabricante com por no mínimo 60 meses.

4.6.10. Adquirir solução de balanceamento de carga e mecanismos de inspeção SSL para os ambientes de infraestrutura do MJSP.

4.6.11. Prover serviço de instalação, configuração e treinamento da solução a ser adquirida.

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. Em função disso, **é inegável que a atual situação do Ministério da Justiça e Segurança Pública é precária** frente à missão institucional a ser cumprida, por meio de seus objetivos estratégicos. Um órgão que possui dimensões consideráveis, bem como competências diretamente relacionadas ao combate ao tráfico de drogas e crimes conexos, corrupção, crime organizado e crimes violentos, lavagem de dinheiro, defesa do consumidor, entre outros, deve **evitar, tratar ou mitigar**

todos os riscos que possam impactar de alguma forma no desempenho de suas atividades fim. Ademais, é de amplo conhecimento a necessidade do Governo e de seus executores de políticas públicas, de dispor de soluções de gestão completas e seguras, aptas a oferecer altos níveis de confiabilidade na geração e análise de informações permitindo, assim, soluções rápidas e ações eficientes para a tomada de decisão. Nos próximos itens serão definidos os principais requisitos que se aplicam a esta contratação.

5.3. ***Requisitos de Negócio***

5.3.1. Reduzir homicídios e outros crimes violentos.

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

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

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

5.3.5. Aperfeiçoar a gestão do sistema prisional.

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

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

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

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

5.4. ***Requisitos de Capacitação***

5.4.1. **Grupo 1**

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

5.4.1.2. 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;

5.4.1.3. 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;

5.4.1.4. A CONTRATADA deverá realizar treinamento para 1 (uma) turma com 5 (cinco) servidores indicados pela CONTRATANTE;

5.4.1.5. A capacitação deverá ser realizada em Brasília-DF, preferencialmente nas dependências da CONTRATANTE.

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

5.4.2. **Grupo 2**

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

5.4.2.2. 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;

5.4.2.3. 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;

5.4.2.4. A CONTRATADA deverá realizar treinamento para 1 (uma) turma com 5 (cinco) servidores indicados pela CONTRATANTE;

5.4.2.5. 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, e poderá ser realizada durante a Operação Assistida contratadas, com aprovação prévia da CONTRATANTE.

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

5.5. ***Requisitos Legais***

5.5.1. **Grupo 1 e 2**

5.5.1.1. 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.

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

5.5.1.2.1. 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.

5.5.1.2.2. 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.

5.5.1.2.3. 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.

5.5.1.2.4. 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.

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

5.5.1.2.6. Instrução Normativa Nº 1, 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.

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

5.6. ***Requisitos de Manutenção***

5.6.1. **Grupo 1**

5.6.1.1. Para a solução de ativos de redes, a manutenção especializada corretiva, preventiva e evolutiva não serão aplicadas. Cabendo observar, neste caso, os Requisitos de Garantia.

5.6.2. **Grupo 2**

5.6.2.1. Os serviços de natureza corretiva, preventiva e evolutiva serão prestados por meio de suporte técnico especializado com base na Solução de Segurança e Balanceamento de Carga – Tipo B (Ambiente Virtual) - **Grupo 2 - item 16**, que será firmado nas condições estabelecidas no Termo de Referência, contemplando em linhas gerais:

a) Solução de problemas de funcionamento e disponibilidade da solução, esclarecimento de dúvidas relacionadas à instalação, configuração, uso e atualização;

b) Visita trimestral (on-site) para realizar checagem da saúde e funcionamento da solução já implementada, permitindo um diagnóstico preciso do status atual da rede;

c) Atualizações de software para os equipamentos objeto deste contrato, mantendo a solução em pleno funcionamento e na versão desejada pela CONTRATANTE.

d) Desinstalação/reinstalação da solução, em caso de necessidade;

e) Consultoria Especializada;

f) Suporte técnico especializado disponível 24 (vinte e quatro) horas, 07 (sete) dias por semana, durante toda vigência do contrato.

5.6.3. Os serviços de natureza corretiva, preventiva e evolutiva da solução são detalhados no **Grupo 2 - ANEXO I-A - ESPECIFICAÇÕES TÉCNICAS.**

5.7. ***Requisitos Temporais***

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

5.8. ***Requisitos de Segurança***

5.8.1. **Grupo 1 e 2**

5.8.1.1. Os funcionários da Contratada deverão obedecer às diretrizes, normas e procedimentos

da Política de Segurança da Informação e Comunicações do Órgão, assim como:

5.8.1.1.1. 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.

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

5.8.1.1.3. 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.

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

5.9.1. **Grupo 1 e 2**

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

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

5.9.1.1.2. 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;

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

5.9.1.1.4. 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))

5.9.1.2. 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.

5.9.1.3. 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.

5.10. ***Requisitos de Arquitetura Tecnológica***

5.10.1. **Grupo 1**

5.10.1.1. Deve poder atuar como 'Parent Switch' dos Fabric Extenders existentes no Data Center do MJSP (Cisco Nexus 2348TQ);

5.10.1.2. A solução deve ser totalmente compatível com os equipamentos atuais do Ministério, como os switches Cisco Nexus 56128P (PART NUMBER N5K-C56128P) e Fabric Extenders Cisco Nexus 2348TQ (FEX) (PART NUMBER N2K-C2348TQ)

5.10.1.3. Essa é uma medida essencial e requisito fundamental ao funcionamento do parque de ativos do MJSP, sendo que alguns equipamentos da solução como switches, transceiver, e cordões ópticos devem também ser totalmente compatíveis com os ativos atuais, não possuindo qualquer tipo de adaptação em suas ligações.

5.10.1.4. Todos os Requisitos de Arquitetura Tecnológica da solução são detalhados no **ANEXO I-A - ESPECIFICAÇÕES TÉCNICAS.**

5.10.2. **Grupo 2**

5.10.2.1. Todos os Requisitos de Arquitetura Tecnológica da solução são detalhados no **ANEXO I-A - ESPECIFICAÇÕES TÉCNICAS**

5.11. ***Requisitos de Projeto e de Implementação***

5.11.1. **Grupo 1 e 2**

5.11.2. 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.

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

5.12. ***Requisitos de Implantação***

5.12.1. **Grupo 1**

5.12.1.1. Os serviços de implantação da solução, necessários para a operacionalização dos switches de Data Center (Spine/Leaf) e Agregação, além dos softwares de Gerenciamento e Controle de Acesso 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) Operação Assistida (Quantidade definida junto à CONTRATANTE);

g) Transferência de Conhecimento;

h) Garantia especializada do fabricante.

5.12.1.2. Todos os Requisitos de Implantação são detalhados no **ANEXO I-A - ESPECIFICAÇÕES TÉCNICAS - Grupo 1.**

5.12.2. **Grupo 2**

5.12.2.1. Os serviços de implantação da solução, necessários para a operacionalização da Solução de Balanceamento de Carga e Segurança 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) Operação Assistida (Quantidade definida junto à CONTRATANTE);

g) Transferência de Conhecimento;

h) Garantia especializada do fabricante;

i) Suporte Especializado (Etapa de prestação do serviço de suporte técnico especializado para a solução instalada durante toda a vigência contratual).

5.12.2.2. Todos os Requisitos de Implantação da solução são detalhados no **ANEXO I-A - ESPECIFICAÇÕES TÉCNICAS - Grupo 2.**

5.13. ***Requisitos de Suporte e Garantia***

5.13.1. **Garantia Grupo 1 e Grupo 2**

5.13.1.1. 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 CONRATANTE) junto ao fabricante;

5.13.1.2. O prazo de garantia contratual dos bens, complementar à garantia legal, é de, no mínimo, 60 (sessenta) meses, ou pelo prazo fornecido pelo fabricante, se superior, contado a partir do primeiro dia útil subsequente à data do recebimento definitivo do objeto. (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 os equipamentos: "*1.4.4.1 Para aquisição de ativos de rede, tipo equipamentos wi-fi, switches de centro e de borda, roteadores, etc, deve-se considerar* ***o tempo de vida de 5 (cinco) anos*** *para fins de posicionamento da tecnologia e de garantia de funcionamento.(grifo nosso)* ")

5.13.1.3. 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.

5.13.1.4. 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.

5.13.1.5. 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.

5.13.1.6. 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.

5.13.1.7. Uma vez notificada, a Contratada realizará a reparação ou substituição dos bens que

apresentarem vício ou defeito, utilizando a modalidade 8X5XNBD, até o próximo dia útil (Next Business Day - NBD) após a abertura do chamado, pela Contratada ou pela assistência técnica autorizada.

5.13.1.8. 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.

5.13.1.9. 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.

5.13.1.10. 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.

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

5.13.1.12. 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.

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

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

5.13.1.12.3. 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;

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

5.13.1.13. O suporte e garantia do item 16 do Grupo 2 (Solução de segurança e balanceamento de carga - Tipo B), deverá ser de 36 (trinta e seis) meses, contados a partir do Termo de Recebimento Definitivo (TRD) do item;

5.13.1.14. <u>Dos requisitos de atualização de software (Grupo 1 e Grupo 2):</u>

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

5.13.1.14.2. 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;

5.13.1.15. <u>Dos requisitos de acesso à documentação (Grupo 1 e Grupo 2):</u>

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

5.13.1.15.2. 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.

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

5.13.2.1. **Grupo 1**

5.13.2.1.1. 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.

5.13.2.2. **Grupo 2**

5.13.2.2.1. 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.

5.13.2.3. **Grupo 2 (item 16)**

5.13.2.3.1. 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.

5.13.2.4. 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.

5.13.2.5. 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.

5.13.2.6. 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.

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

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

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

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

5.13.2.11. 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.

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

5.13.2.13. 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.

5.13.2.14. 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.

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

5.14. ***Requisitos de Experiência Profissional***

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

5.15. ***Requisitos de Segurança da Informação***

5.15.1. A CONTRATADA deverá observar as melhores práticas aplicadas:

5.15.1.1. À disponibilidade da solução de TIC contratada;

5.15.1.2. À vazamento de dados e fraudes digitais;

5.15.1.3. Ao processo de gestão de riscos de segurança da informação que envolvam a solução

de TIC;

5.15.1.4. À rastreabilidade de forma a manter trilha de auditoria de segurança da informação;

5.15.1.5. À continuidade do negócio implementado pela solução;

5.15.1.6. À gestão e tratamento de incidentes de forma sistematizada;

6. RESPONSABILIDADES

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

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

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

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

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

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

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

6.1.7. 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;

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

6.1.9. 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;

6.1.10. 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 licenças de acordo com os requisitos de quantidades, especificações técnicas e manuais de operação (quando couber).

6.2.4. Entregar os ativos e licenças nos prazos previstos e locais designados, conforme especificações constantes na proposta, no Edital, e seus anexos.

6.2.5. Entregar os ativos e licenças 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 1, 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 1, de 4 de abril de 2019;

b) Entregar o TERMO DE CIÊNCIA, conforme descrito no **ANEXO I - F** 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.

7.3. **Prazos e condições**

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

7.3.2. **Locais da execução dos serviços**

Localização	Endereços
Brasília -DF	• Esplanada dos Ministérios, Bloco T, Anexo II – CEP: 70064900 • Setor Policial (SPO) - CICCN - Centro Integrado de Comando e Controle Nacional - CEP: 70297-400

Tabela 12 - 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 diversas	Contratante/Contratada	Contratante/Contratada	Sempre que 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
Termo de Encerramento do Contrato	Encerramento oficial do contrato	Contratante	Contratada	No final do contrato

Tabela 13 - 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

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 e licenças serão de 60 (sessenta) dias corridos, contados após a Emissão OS/OFB;

8.1.4. A solução será recebida definitivamente no prazo de até 45 (quarenta e cinco) dias corridos, após a entrega dos equipamentos, completa instalação 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 gestor do contrato e pelo fiscal técnico.

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 1, 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):

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) Confecção e assinatura do Termo de Recebimento Definitivo, a cargo do Fiscal Requisitante e Fiscal Técnico do Contrato;

c) Avaliar a qualidade dos serviços realizados ou dos bens entregues e as justificativas por não cumprimento de termos contratuais, de acordo com os Critérios de Aceitação definidos neste Contrato;

d) Identificar não conformidade com os termos contratuais;

e) Verificar a manutenção das condições classificatórias referentes à habilitação técnica;

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

g) Receber e atestar os documentos da despesa, quando comprovado o fiel e correto fornecimento dos serviços para fins de pagamento;

h) Comunicar, formalmente, ao Gestor deste Contrato e à CONTRATADA, irregularidades cometidas passíveis de penalidades, bem como indicar glosas na Nota Fiscal;

i) Encaminhar ao Gestor do Contrato eventuais pedidos de modificação contratual.

8.2.7. Fiscal (is) Administrativo (s):

a) Verificar aderência aos termos contratuais;

b) Verificar regularidades fiscais, trabalhistas e previdenciárias para fins de pagamento;

c) Receber do preposto do contrato os Termos de Ciência assinados pelos novos empregados envolvidos na execução dos serviços contratados;

d) Receber indicação de glosas e sanções por parte do Gestor do Contrato;

8.2.8. Fiscal (is) Requisitante (s):

a) Fiscalizar o contrato do ponto de vista de negócio e funcional da solução de TIC;

b) Confecção e assinatura do Termo de Recebimento Definitivo, a cargo do Fiscal Requisitante e Fiscal Técnico do Contrato.

c) Avaliar a qualidade dos serviços realizados ou dos bens entregues e as justificativas por não cumprimento de termos contratuais, de acordo com os Critérios de Aceitação definidos neste Contrato;

d) Identificar não conformidades com os termos contratuais;

e) Verificar a manutenção da necessidade e oportunidade da contratação;

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

g) Comunicar, formalmente, ao Gestor deste Contrato e à CONTRATADA, irregularidades cometidas passíveis de penalidades, bem como efetuar as glosas na Nota Fiscal;

h) Encaminhar ao Gestor do Contrato eventuais pedidos de modificação contratual.

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, contados após a Emissão OFB;

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) e funcionalidades (softwares) 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;

8.3.1.7.1. <u>Serviços de Operação Assistida</u>

8.3.1.7.1.1. A operação assistida consiste no acompanhamento do funcionamento da solução por técnico(s) da CONTRATADA, abrangendo também a execução de serviços não programados ou não esperados no planejamento inicial, necessários para o completo funcionamento da nova estrutura;

8.3.1.7.1.2. A CONTRATADA deverá prestar Operação Assistida à solução durante **<u>30 dias (úteis)</u>**, tendo seu início após o Termo de Recebimento Definitivo (TRD) da solução;

8.3.1.7.1.3. O escopo, atividades e tarefas da Operação Assistida estão descritos no ANEXO I-A do Termo de Referência.

ENTREGA	PREVISÃO DE ENTREGA	DA EXTRAPOLAÇÃO DOS PRAZOS
Operação Assistida	A Operação Assistida se iniciará após o Termo de Recebimento Definitivo (TRD) mediante comunicação da equipe de fiscalização.	A empresa deverá iniciar os serviços no dia útil subsequente do recebimento da comunicação. O atraso superior ao prazo estabelecido será passível das sanções previstas neste instrumento.
Relatórios de atividades de Operação Assistida	Até o quinto dia útil após o fim da Operação Assistida.	O prazo estabelecido poderá ser prorrogado por uma única vez, mediante autorização expressa da CONTRATANTE. O atraso superior ao prazo estabelecido será passível das sanções previstas neste instrumento.

Tabela 14 **- Operação Assistida**

8.3.1.7.2. <u>Solução de segurança e balanceamento de carga - Tipo B (Ambiente Virtual) para 36 meses</u>

8.3.1.7.2.1. O atendimento para abertura de pedidos de suporte técnico deverá estar disponível 24 (vinte e quatro) horas, 07 (sete) dias por semana, durante toda vigência do contrato.

ENTREGA	PREVISÃO DE ENTREGA	DA EXTRAPOLAÇÃO DOS PRAZOS
		A empresa deverá iniciar os serviços no dia

Instalação da solução	A instalação deverá ser efetuada em até 30 (trinta) dias corridos, após a emissão da Ordem de Serviço por parte da CONTRATANTE.	útil subsequente do recebimento dos equipamentos pela CONTRATANTE. O atraso superior ao prazo estabelecido será passível das sanções previstas neste instrumento.
Checagem da saúde e funcionamento da solução de **natureza preventiva**	O tempo de contagem da visita trimestral (on-site) se iniciará no dia útil após o Termo de Recebimento Definitivo (TRD), mediante comunicação da equipe de fiscalização.	A empresa deverá manter a rotina de visitas trimestrais estabelecidas junto à CONTRATANTE. O atraso superior ao prazo estabelecido será passível das sanções previstas neste instrumento.
Checagem da saúde e funcionamento da solução de **natureza evolutiva**	Mediante solicitação da CONTRATANTE, implementará atualizações de software, melhorias da solução implementada, possíveis desinstalação/reinstalação da solução para a solução objeto deste contrato, mantendo a solução em pleno funcionamento.	A empresa deverá iniciar as análises, projetos e estudos, juntamente com a CONTRATANTE, após o 5º (quinto) dia útil da abertura da solicitação junto à empresa. O atraso superior ao prazo estabelecido será passível das sanções previstas neste instrumento.
Checagem da saúde e funcionamento da solução de **natureza corretiva**	Efetuados com objetivo de solucionar problemas de funcionamento e disponibilidade da solução e de esclarecer dúvidas relacionadas à instalação, configuração, uso e atualização dos produtos.	A empresa deverá iniciar os serviços no dia útil subsequente da abertura da solicitação pela CONTRATANTE. O atraso superior ao prazo estabelecido será passível das sanções previstas neste instrumento.

Tabela 15 **- Solução de segurança e balanceamento de carga - Tipo B (Ambiente Virtual)**

8.3.1.7.3. Instalação Física e Lógica

8.3.1.7.3.1. A CONTRATADA deverá providenciar todos os materiais necessários à instalação física e lógica dos equipamentos e licenças; a CONTRATANTE será responsável pela disponibilização do(s) rack(s) e fornecimento de pontos elétricos necessários à instalação dos equipamentos;

8.3.1.7.3.2. A instalação deverá ser efetuada em até 30 (trinta) dias corridos, após a emissão da Ordem de Serviço por parte da CONTRATANTE.

8.3.1.7.3.3. 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.

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

8.3.1.7.3.5. A migração de todas as configurações e serviços dos equipamentos atualmente em uso no Data Center da CONTRATANTE para os novos equipamentos adquiridos deverá ser realizada pela CONTRATADA, podendo esta realizar o levantamento dos atuais equipamentos e configurações durante a vistoria técnica.

8.3.1.8. Níveis de Severidade dos Chamados em Garantia

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.
	Chamados associados a situações de alto impacto, referentes ao uso do produto, com equipamentos parcialmente ou totalmente		O atendimento remoto/presencial deverá ser iniciado em no máximo 03 (três) horas após a abertura	No máximo 12 (doze) horas	O atraso superior ao prazo

2 - ALTA	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	abertura do registro do chamado na CONTRATADA para início das ações correspondentes à solução definitiva ou contorno.	horas corridas após a abertura do chamado.	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.
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	O atendimento 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 16 **- Atendimento dos Chamados em 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 dos serviços, 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 3,2% por dia sobre o valor mensal 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;

8.4.2.6. 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

8.4.3. Para efeito de aplicação de multas, às infrações são atribuídos graus, de acordo com as tabelas 1 e 2:

GRAU	CORRESPONDÊNCIA
1	0,2% por dia ou hora sobre o valor adjudicado
2	0,4% por dia ou hora sobre o valor adjudicado
3	0,8% por dia ou hora sobre o valor adjudicado
4	1,6% por dia ou hora sobre o valor adjudicado
5	3,2% por dia ou hora sobre o valor adjudicado

Tabela 1

INFRAÇÃO		
Para os itens a seguir, deixar de:		
1	Cumprir os prazos estabelecidos para execução da garantia relacionada aos chamados de criticidade máxima.	5
2	Cumprir os prazos estabelecidos para execução da garantia relacionada aos chamados de criticidade alta.	4
3	Cumprir os prazos estabelecidos para execução da garantia relacionada aos chamados de criticidade média.	3
4	Cumprir os prazos estabelecidos para execução da garantia relacionada aos chamados de criticidade baixa.	2
5	Cumprir os prazos estabelecidos para os serviços da Solução de segurança e balanceamento de carga - Tipo B (Ambiente Virtual) para 36 meses - **Instalação da solução**	3
6	Cumprir os prazos estabelecidos para os serviços da Solução de segurança e balanceamento de carga - Tipo B (Ambiente Virtual) para 36 meses - **natureza preventiva**	1
7	Cumprir os prazos estabelecidos para os serviços da Solução de segurança e balanceamento de carga - Tipo B (Ambiente Virtual) para 36 meses - **natureza evolutiva**	2

8	Cumprir os prazos estabelecidos para os serviços da Solução de segurança e balanceamento de carga - Tipo B (Ambiente Virtual) para 36 meses - **natureza corretiva**	4

Tabela 2

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

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

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

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

8.4.5. 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.

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

8.4.6.1. 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.

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

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

8.4.9. 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.

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

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

8.4.12. 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. O valor máximo previsto para o **Grupo 1** é de **R$ 4.319.509,45 (quatro milhões, trezentos e dezenove mil quinhentos e nove reais e quarenta e cinco centavos)**

9.2. O valor máximo previsto para o **Grupo 2** é de **R$ 7.032.643,82 (sete milhões, trinta e dois mil seiscentos e quarenta e três reais e oitenta e dois centavos)**

9.3. O valor total estimado da contratação é de **R$ 11.352.153,27 (onze milhões, trezentos e cinquenta e dois mil cento e cinquenta e três reais e vinte e sete centavos)** , baseado na pesquisa mercadológica conforme instrui o documento (12495864) e demais apensos, conforme detalhado abaixo:

				Unidade	Valor unitário	Valor total

Grupo	Item	Descrição do Bem ou Serviço	Quantidade	de medida	máximo (R$)	máximo (R$)
1	1	Switch Spine	04	Unitário	307.235,00	1.228.940,00
	2	Switch Leaf- Tipo A	06	Unitário	139.875,00	839.250,00
	3	Switch Leaf- Tipo B	04	Unitário	290.290,00	1.161.160,00
	4	Switch de Agregação	02	Unitário	187.823,33	375.646,67
	5	Sistema de Gerenciamento de Equipamentos de Data Center	01	Unitário	57.100,00	57.100,00
	6	Solução de Controle de Acesso – Virtual Machine	01	Unitário	76.463,33	76.463,33
	7	Licenciamento Switches existentes	02	Unitário	23.900,00	47.800,00
	8	Transceiver 10G Multimodo (LC)	70	Unitário	2.443,33	171.033,33
	9	Transceiver 25G Multimodo (LC)	16	Unitário	3.033,33	48.533,33
	10	Cordão Óptico Duplex, 10G Multimodo,(LC/LC) (10 metros)	62	Unitário	254,78	15.796,11
	11	Cabo de Conexão Direta 100G – (10 metros)	20	Unitário	7.900,00	158.000,00
	12	Cabo de Conexão Direta 40G – (10 metros)	08	Unitário	3.523,33	28.186,67
	13	Operação Assistida	01	Serviço	111.600,00	111.600,00
	VALOR TOTAL DO GRUPO				**R$ 4.319.509,45**	
2	14	Solução de segurança e balanceamento de carga - Appliance Físico - Tipo A	02	Unitário	1.380.752,84	2.761.505,68
	15	Transceiver 10G Multimodo (LC) - para item 14 (Appliance Físico - Tipo A)	16	Unitário	8.568,97	137.103,55
	16	Subscrição de licença para solução de segurança e balanceamento de carga - Tipo B (Ambiente Virtual) para 36 meses	01	Unitário	4.042.308,40	4.042.308,40
	17	Operação Assistida	01	Serviço	91.726,20	91.726,20
	VALOR TOTAL DO GRUPO				**R$ 7.032.643,82**	
VALOR TOTAL DA CONTRATAÇÃO:					**R$ 11.352.153,27**	

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 2020, na classificação abaixo:

10.1.1. Programa de Trabalho: 04122003220000000001

10.1.2. Plano de Trabalho Resumido (PTRES): 172184

10.1.3. Fonte: 0100

10.1.4. Ação: 2000

10.1.5. Plano Orçamentário (PO): 000C

10.1.6. Plano Interno (PI): GL67PTCGLTI

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

Grupo	Item	Descrição do Bem ou Serviço	Natureza de Despesa
1	1	Switch Spine	44905237
	2	Switch Leaf- Tipo A	44905237
	3	Switch Leaf- Tipo B	44905237
	4	Switch de Agregação	44905237
	5	Sistema de Gerenciamento de Equipamentos de Data Center	44904005
	6	Solução de Controle de Acesso – Virtual Machine	44904005
	7	Licenciamento Switches existentes	44904005
	8	Transceiver 10G Multimodo (LC)	44905237
	9	Transceiver 25G Multimodo (LC)	44905237
	10	Cordão Óptico Duplex, 10G Multimodo,(LC/LC) (10 metros)	33903017
	11	Cabo de Conexão Direta 100G – (10 metros)	33903017
	12	Cabo de Conexão Direta 40G – (10 metros)	33903017
	13	Operação Assistida	33903504
2	14	Solução de segurança e balanceamento de carga - Appliance Físico - Tipo A	44905237
	15	Transceiver 10G Multimodo - para item 14 (Appliance Físico - Tipo A)	44905237
	16	Solução de segurança e balanceamento de carga - Tipo B (Ambiente Virtual) para 36 meses	33904006
	17	Operação Assistida	33903504

11. DA VIGÊNCIA DO CONTRATO

11.1. O prazo de vigência da contratação será de 12 meses, prorrogáveis conforme o inciso I do art. 57 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.

11.2.1. Para o item 16, o prazo de vigência do Termo de Contrato será de 36 (trinta e seis) meses com pagamento único, conforme inciso IV do art. 57 da Lei nº 8.666/93. Para esse item será firmado contrato em separado, cuja vigência está prevista para iniciar após o Termo de Recebimento Definitivo (TRD).

11.2.2. A vigência do contrato de 36 meses, com pagamento único, é utilizado em contratações com objetos semelhantes, conforme Estudo Técnico Preliminar da Contratação, item 9 (12121843).

11.2.3. Sob o ponto de vista econômico, é mais vantajosa a Aquisição de Licenciamento de Software *Enterprise Agreement* (EA) com a vigência do contrato de 36 meses com pagamento único, ao invés de renovações a cada 12 meses ou contrato de 36 meses com pagamento anual, mais detalhes dessa análise encontra-se no Estudo Técnico da Contratação, item 9 (12121843).

11.2.4. Esta contratação, com a vigência do contrato de 36 meses com pagamento único, se enquadra no inciso IV do art. 57 da Lei 8.666/93 e se dá em virtude da natureza dos serviços contratados, conforme previsto na Orientação Normativa da AGU 38 de 2011:

> *ORIENTAÇÃO NORMATIVA Nº 38, DE 13 DE DEZEMBRO DE 2011 (*)*
>
> *"NOS CONTRATOS DE PRESTAÇÃO DE SERVIÇOS DE NATUREZA CONTINUADA DEVE-SE OBSERVAR QUE: A) O PRAZO DE VIGÊNCIA ORIGINÁRIO, DE REGRA, É DE ATÉ 12 MESES; B) EXCEPCIONALMENTE, ESTE PRAZO PODERÁ SER FIXADO POR PERÍODO SUPERIOR A 12 MESES NOS CASOS EM QUE, DIANTE DA PECULIARIDADE E/OU COMPLEXIDADE DO OBJETO, FIQUE TECNICAMENTE DEMONSTRADO O BENEFÍCIO ADVINDO PARA A ADMINISTRAÇÃO E C) É JURIDICAMENTE POSSÍVEL A PRORROGAÇÃO DO CONTRATO POR PRAZO DIVERSO DO CONTRATADO ORIGINARIAMENTE." (grifo nosso)*

11.2.4.1. Diante do exposto, é mais vantajoso economicamente e tecnicamente para o Ministério da Justiça e Segurança Pública que a vigência se der pelo prazo de 36 (trinta e seis) meses, nos termos do inciso IV, do art. 57 da Lei 8.666/93.

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. DOS CRITÉRIOS DE SELEÇÃO DO FORNECEDOR

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

12.1.1. 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.

12.1.2. 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.

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

12.2.1. 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.

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

12.3.1. **Da vistoria técnica**

12.3.1.1. Para o correto dimensionamento e elaboração de sua proposta, o licitante *poderá* realizar vistoria nas instalações do local de execução dos serviços, 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**.

12.3.1.2. 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.

12.3.1.3. 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.

12.3.1.4. 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.

12.3.1.5. 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.

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

12.3.2. **Qualificação técnica**

12.3.2.1. 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:

12.3.2.1.1. **Grupo I:**

12.3.2.1.1.1. Fornecimento de 50% do quantitativo de cada item de Switches (Spine e Leaf - itens 1, 2 e 3) de Data Center com características compatíveis com as especificadas nesse Termo de Referência, contendo especificamente as seguintes funcionalidades:

12.3.2.1.1.1.1. Suporte a topologias Spine-and-Leaf;

12.3.2.1.1.1.2. Suporte à Multichassis Link Etherchannel;

12.3.2.1.1.1.3. Suporte à Fabric IP L3 com VXLAN;

12.3.2.1.1.2. Fornecimento de 50% da quantidade de Switches de Agregação (item 4) com características compatíveis com as especificadas nesse Termo de Referência;

12.3.2.1.1.3. Comprovar a instalação e configuração de equipamentos semelhantes utilizando a topologia Spine-and-Leaf;

12.3.2.1.2. **Grupo II**:

12.3.2.1.2.1. Fornecimento de 50% do quantitativo da Solução de Segurança e Balanceamento de Carga (item 14) com características compatíveis com as especificadas nesse Termo de Referência, contendo especificamente as seguintes funcionalidades:

12.3.2.1.2.1.1. Suporte a SLB e GLSB;

12.3.2.1.2.1.2. Suporte à WAF;

12.3.2.1.2.1.3. Suporte à SSL Offload, visibilidade e orquestração de tráfego SSL;

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

12.3.2.3. 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 CONTRATANTE deseja implementar. Além disso, conforme exposto na justificativa da contratação, pretende-se realizar modificações de criticidade alta na topologia de redes do MJSP, o que torna essencial, para garantir a correta implementação do projeto, que configurações adequadas, desempenho, qualidade, além da disponibilidade, cofiabilidade e integridade das informações, sejam garantidas pela LICITANTE, sendo isso exposto pelas qualificações técnicas solicitadas.

13. DOS ANEXOS

13.1. 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

14. DA EQUIPE DE PLANEJAMENTO DA CONTRAÇÃO E DA APROVAÇÃO

14.0.1. A Equipe de Planejamento da Contratação foi instituída pela Portaria SAA nº 23, de 08 de julho de 2020 (12100374).

14.0.2. 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	Leonardo Garcia Greco	Nome	Bruno Alves de Lima	Nome	Vinícius Augusto Bittencourt Dalcól
Cargo	Coordenador-Geral de Infraestrutura e Serviços	Cargo	Chefe da Divisão de Redes, Segurança e Monitoramento	Cargo	Administrador
Matrícula	1447905	Matrícula	2270209	Matrícula	1764266

Aprovo,

Autoridade Máxima da Área de TIC e Autoridade Competente	
Nome	Rodrigo Lange
Cargo	Diretor de Tecnologia da Informação e Comunicação
Matrícula	0480055

Documento assinado eletronicamente por **Bruno Alves de Lima**, **Integrante Técnico(a)**, em 16/10/2020, às 12:05, conforme o § 1º do art. 6º e art. 10 do Decreto nº 8.539/2015.

Documento assinado eletronicamente por **Leonardo Garcia Greco**, **Integrante Requisitante**, em 16/10/2020, às 12:06, conforme o § 1º do art. 6º e art. 10 do Decreto nº 8.539/2015.

Documento assinado eletronicamente por **VINICIUS AUGUSTO BITTENCOURT DALCOL**, **Integrante Administrativo**, em 16/10/2020, às 15:55, conforme o § 1º do art. 6º e art. 10 do Decreto nº 8.539/2015.

Documento assinado eletronicamente por **Rodrigo Lange**, **Diretor(a) de Tecnologia da Informação e Comunicação**, em 18/10/2020, às 10:02, conforme o § 1º do art. 6º e art. 10 do Decreto nº 8.539/2015.

A autenticidade do documento pode ser conferida no site http://sei.autentica.mj.gov.br informando o código verificador **12862295** e o código CRC **141C8605**
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.

ANEXOS DO TERMO DE REFERÊNCIA

ANEXO I-A - ESPECIFICAÇÕES TÉCNICAS

1. **ESPECIFICAÇÕES TÉCNICAS**

1.1. **Grupo 1 – Especificações gerais para switches de Data Center (Spine e Leaf):**

1.1.1. Deve suportar a operação em arquitetura CLOS Spine-and-Leaf, podendo ser inserido no Fabric IP VXLAN a ser configurado no Data Center da MJSP.

1.1.2. Deve funcionar em conjunto com os equipamentos de Data Center já existentes no MJSP, podendo atuar como elemento de um mesmo Fabric IP VXLAN que estes equipamentos;

1.1.3. Deve poder atuar como 'Parent Switch' dos Fabric Extenders existentes no Data Center do MJSP (Cisco Nexus 2348TQ);

1.1.4. Possuir LEDs que indiquem o status de funcionamento do equipamento (switch, portas, ventilação e fonte de alimentação) e a localização (Beacon LED).

1.1.5. Deve ser fornecido com todos os hardwares e licenças necessários para a implementação de todas as funcionalidades descritas nesta especificação.

1.1.6. Suporte a Jumbo Frames de no mínimo 9.198 bytes;

1.1.7. Possuir porta USB compatível com flash drives, para cópias de arquivos de configuração e arquivos de sistema operacional.

1.1.8. Deve possuir fontes de alimentação redundantes AC bivolt internas ao equipamento com ajuste automático de tensão (na faixa de 100 a 240V) e frequência (de 50/60 Hz).

1.1.9. As fontes deverão possuir alimentação independente, a fim de permitir a sua conexão a circuitos elétricos distintos.

1.1.10. Deve ser capaz de sustentar a carga de todo o equipamento com todas as portas ativas, com apenas umas das fontes instalada.

1.1.11. Deve ser capaz de realizar a troca da fonte redundante com o equipamento em pleno funcionamento, sem nenhum impacto na performance (hot-swappable).

1.1.12. As fontes deverão vir acompanhadas com cabos de energia elétrica em conformidade com o padrão NBR14.136.

1.1.13. Deve permitir operação normal em temperaturas de 0ºC até 40ºC;

1.1.14. Deve ser instalável em rack padrão de 19" e ter no máximo 1RU de altura, sendo que deverão ser fornecidos os respectivos kit's de fixação;

1.1.15. Deve possui sistema de ventilação redundante e que permita substituição em caso de falha, sem necessidade de troca do switch.

1.1.16. Deve suportar tanto sistema Back to Front (entrada de ar frio pela fonte de alimentação e exaustão de ar quente pelas conexões de rede) quanto Front to Back (entrada de ar frio pelas conexões de rede e exaustão de ar quente pela fonte de alimentação).

1.1.17. **Funcionalidades Gerais:**

1.1.17.1. Deve suportar aos modos de comutação "cut-through" e "store-and-forward" nativamente ou configurável via linha de comando.

1.1.17.2. Implementar LAN Virtual (VLAN) conforme o padrão IEEE IEEE 802.1Q, permitindo a criação e ativação simultâneas de no mínimo 3.900 VLANs ativas.

1.1.17.3. Implementar "VLAN Trunking" conforme padrão IEEE 802.1Q nas interfaces exigidas. Deve ser possível estabelecer quais VLANs serão permitidas em cada um dos troncos configurados. Deve permitir que uma certa VLAN seja adicionada e removida do tronco sem a necessidade de adicionar e remover todas as demais VLANs configuradas anteriormente.

1.1.17.4. Deve permitir a criação, remoção e distribuição de VLANs de forma dinâmica através de portas configuradas como tronco IEEE 802.1Q.

1.1.17.5. Permitir a criação de subgrupos dentro de uma mesma VLAN com conceito de portas "isoladas" e portas "promíscuas", onde portas isoladas não se comunicam com outras portas isoladas, mas apenas com as portas promíscuas de uma dada VLAN.

1.1.17.6. Deve implementar os padrões IEEE 802.1d ("STP – Spanning Tree Protocol"), IEEE 802.1s ("MSTP – Multiple Spanning Tree") e IEEE 802.1w ("RSTP – Rapid Spanning Tree").

1.1.17.7. Deve permitir a configuração de, no mínimo, 64 (sessenta e quatro) instâncias de Spanning Tree.

1.1.17.8. Implementar simultaneamente os padrões MSTP e RSTP, permitindo a configuração de, no mínimo, 64 (sessenta e quatro) instâncias simultâneas.

1.1.17.9. Implementar Spanning-tree baseado em VLAN´s, em que cada VLAN execute o protocolo STP ou RSTP de forma independente.

1.1.17.10. Implementar mecanismo de proteção da "root bridge" do algoritmo Spanning-Tree para prover defesa contra ataques do tipo "Denial of Service" no ambiente nível 2.

1.1.17.11. Deve permitir a suspensão de recebimento de BPDUs (Bridge Protocol Data Units) caso a porta esteja colocada no modo "fast forwarding" (conforme previsto no padrão IEEE 802.1w). Sendo

recebido um BPDU neste tipo de porta deve ser possível desabilitá-la automaticamente.

1.1.17.12. Implementar a funcionalidade de agregação de portas conforme padrão IEEE 802.3ad (LACP) de modo que as portas agrupadas formem uma única interface lógica com as mesmas facilidades das interfaces originais.

1.1.17.13. Deve permitir pelo menos a criação de 16 (dezesseis) grupos de portas agregadas, com pelo menos 8 (oito) portas por grupo.

1.1.17.14. O equipamento deve implementar funcionalidade que permita que este switch, em conjunto com outro switch de mesmo modelo, possa receber conexões vindas de um terceiro switch na forma de link aggregation. O terceiro switch em questão deverá perceber os dois switches logicamente como um só. Esta funcionalidade deve tomar como referências padrões como Multi-Chassis Link Aggregation (MLAG) ou Multi-Chassis EtherChannel (MEC). O único link lógico entre os dois switches descritos neste item e o terceiro switch deve eliminar convergência do Spanning Tree, possibilitando o tráfego simultâneo por mais de uma conexão (Layer 2 Multipathing).

1.1.17.15. Deve implementar o protocolo IEEE 802.1AB Link Layer Discovery Protocol (LLDP), permitindo a descoberta dos elementos de rede vizinhos.

1.1.17.16. Deve implementar, em hardware, o protocolo Virtual Extensible LAN (VXLAN) – que permite a criação de segmentos de redes virtuais e sua extensão através da camada de redes (nível 3) ao encapsular quadros Ethernet em pacotes IP através de UDP.

1.1.17.17. Deve implementar Fabric VXLAN utilizando MP-BGP EVPN (Multiprotocol BGP Ethernet VPN) como plano de controle.

1.1.17.18. Deve permitir o uso como Gateway VXLAN (VTEP) iniciando ou fechando túneis de comunicação VXLAN.

1.1.17.19. Deve suportar a implementação da função de DHCP Server, capaz de suportar, pelos menos, a atribuição de endereço IPv4.

1.1.17.20. Deve ser suportara função de DHCP Relay por VLAN para IPv4 e IPv6;

1.1.18. **Funcionalidades de QoS**

1.1.18.1. Possuir a facilidade de priorização de tráfego através do protocolo IEEE 802.1p.

1.1.18.2. Implementar pelo menos 06 (seis) filas de prioridade por porta de saída (egress port).

1.1.18.3. Implementar pelo menos 1 (uma) fila de saída com prioridade estrita (prioridade absoluta em relação às demais classes dentro do limite de banda que lhe foi atribuído) e divisão ponderada de banda entre as demais filas de saída.

1.1.18.4. Implementar classificação de tráfego baseada em endereço IP de origem e destino, portas TCP e UDP de origem e destino, endereços MAC de origem e destino.

1.1.18.5. Deve implementar classificação, marcação e priorização de tráfego baseada nos valores de classe de serviço do frame ethernet (IEEE 802.1p CoS – L2) e do campo “Differentiated Services Code Point” (DSCP) do cabeçalho IP (L3), conforme definições do IETF.

1.1.18.6. Implementar funcionalidades de “Traffic Policing”.

1.1.18.7. Deve ser possível a especificação de banda por classe de serviço. Para os pacotes que excederem a especificação deve ser possível configurar ações tais como: transmissão do pacote sem modificação, transmissão com remarcação do valor de DSCP e descarte do pacote.

1.1.18.8. Deve possuir mecanismos de controle de congestionamento e enfileiramento inteligente para tratamento diferenciado de “Mice and Elephants Flows”, definindo limites para alocação de buffer, priorizando pacotes de fluxos curtos e minimizando a alocação de buffer para pacotes longos, de modo a prevenir que fluxos do tipo rajada comprometam os demais fluxos.

1.1.19. **Funcionalidades de Roteamento**

1.1.19.1. Suportar roteamento de pacotes IPv4 e IPv6.

1.1.19.2. Deve permitir o roteamento nível 3 entre VLANs.

1.1.19.3. Deve implementar roteamento estático para IPv4 e IPv6.

1.1.19.4. Deve implementar roteamento dinâmico RIPv2 (RFCs 2082 e 2453).

1.1.19.5. Deve implementar protocolo de roteamento dinâmico OSPFv2 (RFCs 2328, 2370, 3101, 3137 e 3623).

1.1.19.6. Deve implementar protocolo de roteamento dinâmico OSPFv3 para IPv6 (RFC 2740).

1.1.19.7. Deve implementar protocolo de roteamento dinâmico BGPv4 para IPv4 e IPv6 (RFCs 1997, 2385, 2858, 3065 e 4271).

1.1.19.8. Deve suportar Bidirectional Forwarding Detection (BFD) para reduzir o tempo de convergência dos protocolos OSPF e BGP;

1.1.19.9. Deve implementar o protocolo de redundância de gateway VRRP (Virtual Router Redundancy Protocol) conforme as RFCs 3768 e 5798, suportando a configuração de 250 (duzentos e cinquenta) grupos simultaneamente.

1.1.19.10. Deve suportar PBR (Policy-Based Routing) permitindo a definição de políticas de

roteamento baseadas em endereços de origem e outras condições especiais.

1.1.19.11. Permitir a virtualização das tabelas de roteamento de camada de rede (nível 3) utilizando a tecnologia conhecida como VRF (Virtual Routing and Forwarding). As tabelas virtuais deverão ser completamente segmentadas.

1.1.19.12. Deve implementar o protocolo IGMP (Internet Group Management Protocol) v2 e v3, conforme as RFCs 2236 e 3376.

1.1.19.13. Implementar mecanismo que evite tráfego multicast seja tratado como broadcast no switch. O switch deve ser capaz de fazer "snooping" de pacotes IGMP (v1, v2 e v3).

1.1.19.14. Implementar roteamento multicast PIM (Protocol Independent Multicast) nos modos PIM-SM (Sparse Mode – RFC 4610), PIM-SSM (Source-Specific Multicast – RFC 3659) e MSDP (Multicast Source Discovery Protocol – RFC 3618).

1.1.20. **Funcionalidades de Segurança**

1.1.20.1. Deve proteger a interface CLI do equipamento através de senha.

1.1.20.2. Deve implementar listas de controle de acesso (ACLs) baseadas em endereço IPv4 ou IPv6 de origem e destino, portas TCP e UDP de origem e destino, endereços MAC de origem e destino e flags TCP.

1.1.20.3. Deve implementar ACLs baseadas em endereços IP para limitar o acesso ao switch via Telnet e SSH. Deve ser possível definir os endereços IP de origem das sessões Telnet e SSH.

1.1.20.4. Deve permitir a configuração de, no mínimo, 2.000 (duas mil) ACLs.

1.1.20.5. Implementar ACLs baseadas em políticas (Policy Based ACLs), que permitem aplicar políticas de controle de acesso em grupos de objetos;

1.1.20.6. Permitir visualização das estatísticas de filtragem das listas de controle de acesso aplicadas;

1.1.20.7. Implementar mecanismo de autenticação baseado em servidores de Autenticação/Autorização do tipo TACACS e RADIUS, para acesso local ou remoto.

1.1.20.8. Implementar AAA (Authentication, Authorization e Accounting) que utilize o protocolo TCP para prover maior confiabilidade ao tráfego dos pacotes envolvidos no controle administrativo.

1.1.20.9. Implementar a criptografia de todos os pacotes enviados ao servidor de controle de acesso e não só os pacotes referentes à senha.

1.1.20.10. Implementar Controle de Acesso por porta (IEEE 802.1x).

1.1.20.11. Permitir a associação de um endereço MAC específico a uma dada porta do switch, de modo que somente a estação que tenha tal endereço possa usar a referida porta para conexão. Deve ser possível enviar um trap SNMP caso algum MAC diferente tente se conectar à porta.

1.1.20.12. Deve ser possível estabelecer o número máximo de endereços MAC que podem estar associados a uma dada porta do switch. Deve ser possível enviar um trap SNMP caso o número de endereços MAC configurados para a porta seja excedido.

1.1.20.13. Implementar mecanismo de segurança do tipo anti-spoofing com tecnologia que utiliza a tabela de roteamento do equipamento de forma dinâmica, sem configuração de lista de acesso, e que possa ser configurado por interface.

1.1.20.14. Deve implementar NAT (Network Address Translation) e PAT (Port Address Translation) estático e dinâmico.

1.1.20.15. Possuir controle de broadcast, multicast e unicast por porta. Deve ser possível especificar limiares ("thresholds") individuais para tráfego tolerável de broadcast, multicast e unicast em cada porta do switch. Excedidos os valores pré-configurados deve ser possível enviar um trap SNMP e desabilitar a porta.

1.1.20.16. Implementar inspeção do protocolo ARP (Address Resolution Protocol) e possuir mecanismos de proteção contra ataques do tipo "ARP Poisoning".

1.1.20.17. Deve implementar funcionalidade que permita que somente servidores DHCP autorizados atribuam configuração IP aos clientes DHCP (Trusted DHCP Server).

1.1.20.18. Deve promover análise do protocolo DHCP e permitir que se crie uma tabela de associação entre endereços IP atribuídos dinamicamente, MAC da máquina que recebeu o endereço e porta física do switch em que se localiza tal MAC.

1.1.21. **Funcionalidades de Gerenciamento**

1.1.21.1. Possuir uma interface de gerenciamento baseada em WEB (HTTP) que permita aos usuários configurar e gerenciar switches através de um browser padrão, implementar o protocolo HTTPS para gerenciamento gráfico seguro do equipamento.

1.1.21.2. Suportar os protocolos Telnet e SSH versão 2 (SSHv2) para gerenciamento remoto, com no mínimo, 5 sessões simultâneas.

1.1.21.3. Deve suportar, no mínimo, o algoritmo AES-128 para criptografia da conexão SSH.

1.1.21.4. Deve implementar, em hardware, tecnologia para monitoramento de tráfego que

permita agrupar os pacotes que circulam pelo equipamento usando o conceito de fluxos (“flows”). Para cada fluxo devem ser exibidas, no mínimo, as seguintes informações: endereços IP de origem/destino, portas TCP/UDP de origem/destino, interfaces de entrada e saída do tráfego, número de pacotes transmitidos, garantindo alta visibilidade do tráfego de rede. As informações coletadas devem ser automaticamente exportáveis em intervalos pré-definidos através de Netflow v9 ou conforme a RFC 7011 (IETF - Specification of the IP Flow Information Export (IPFIX) Protocol for the Exchange of Flow Information). A ativação dessa ferramenta não poderá alterar o desempenho do switch.

1.1.21.5. Permitir o espelhamento da totalidade do tráfego de uma VLAN, de uma porta ou de um grupo de portas para uma porta especificada.

1.1.21.5.1. Deve ser possível espelhar o tráfego para outra porta localizada no mesmo switch, outro switch do Fabric IP L3 e para um endereço IP remoto.

1.1.21.5.2. Deve ser possível definir o sentido do tráfego a ser espelhado: somente tráfego de entrada, somente tráfego de saída e ambos simultaneamente.

1.1.21.5.3. Devem ser suportadas pelo menos 2 (duas) sessões simultâneas de espelhamento ativas simultaneamente.

1.1.21.6. Implementar os padrões abertos de gerência de rede SNMPv1, SNMPv2c e SNMPv3.

1.1.21.7. Implementar pelo menos os seguintes níveis de segurança para SNMP versão 3: sem autenticação e sem privacidade (noAuthNoPriv); com autenticação e sem privacidade (authNoPriv); e com autenticação e com privacidade (authPriv). Deve suportar no mínimo os algoritmos criptográficos DES no modo AuthPriv.

1.1.21.8. Possibilitar a obtenção da configuração do equipamento através do protocolo SNMP;

1.1.21.9. Permitir o controle da geração de traps SNMP, possibilitando definir quais tipos de alarmes geram traps.

1.1.21.10. Implementar a MIB privativa que forneça informações relativas ao funcionamento do equipamento.

1.1.21.11. Possuir descrição completa da MIB implementada no equipamento, inclusive a extensão privativa.

1.1.21.12. Permitir o armazenamento de sua configuração em memória não volátil, podendo, numa queda e posterior restabelecimento da alimentação, voltar à operação normalmente na mesma configuração anterior à queda de alimentação.

1.1.21.13. Permitir a atualização de software sem perda de pacotes (tecnologia conhecida como ISSU – In Services Software Upgrades) para funcionalidades de camada de rede (nível 2).

1.1.21.14. Permitir a aplicação de patches em seu sistema operacional.

1.1.21.15. Possibilitar a criação de versões de configuração e retorno de versões anteriores (rollback).

1.1.21.16. Implementar nativamente, sem uso de probes externas, pelo menos 2 grupos RMON (Alarms e Events).

1.1.21.17. Possuir ferramentas para depuração e gerenciamento em primeiro nível, tais como debug, trace, log de eventos.

1.1.21.18. Possuir armazenamento interno das mensagens de log geradas pelo equipamento.

1.1.21.19. Possuir capacidade de exportar as mensagens de log geradas pelo equipamento para um servidor syslog externo.

1.1.21.20. Possibilidade de atualização do sistema operacional através do protocolo TFTP (Trivial Fiel Transfer Protocol) ou FTP (File Transfer Protocol).

1.1.21.21. Possibilidade de transferência segura e autenticada de arquivos através de SCP (Secure Copy Protocol) ou SFTP (SSH File Transfer Protocol).

1.1.21.22. Implementar o protocolo NTP (Network Time Protocol);

1.1.21.23. Implementar o protocolo PTP (Precision Time Protocol) de acordo com o padrão IEEE 1588;

1.1.21.24. Possuir funcionalidade de tratamento de eventos, permitindo a definição de valores de limiar (thresholds) de CPU e memória do equipamento, permitindo o envio de mensagens de syslog ou traps SNMP quando estes valores forem atingidos.

1.1.21.25. Deve permitir a configuração de endereços IPv6 para gerenciamento;

1.1.21.26. Implementar protocolos de gerenciamento Ping, Traceroute, Telnet, SSH, e DNS sobre IPv6.

1.1.22. **Funcionalidades de Programabilidade**

1.1.22.1. Os switches que compõem esta solução deverão suportar funcionamento em modo switch ou modo SDN (Software Defined Network), seja através de configuração ou com a troca do sistema operacional do equipamento, com ou sem necessidade de licenciamento adicional.

1.1.22.2. Deve suportar mecanismo de auto provisionamento para simplificação do processo de

configuração e atualização de imagem e firmware do equipamento.

1.1.22.3. Deve possuir uma plataforma aberta, com flexibilidade para programação via API (Application Programming Interface) e integração com ferramentas de gerenciamento e provisionamento de configuração (Puppet, Chef, Ansible e Salt).

1.1.22.4. Deve implementar API modeladas de acordo com o padrão YANG de acordo com as definições do OpenConfig.

1.1.22.5. O fabricante deve disponibilizar em site público de forma gratuita os modelos YANG nativos (específicos desta plataforma de equipamentos) e variações dos abertos, assim como manter os modelos atualizados.

1.1.22.6. Deve implementar, no mínimo, os protocolos de gerenciamento de redes NETCONF e RESTCONF.

1.1.22.7. Deve implementar, no mínimo, as codificações de dados nos formatos XML e JSON.

1.1.22.8. Deve suportar scripts de configuração em Python nativamente na caixa.

1.1.22.9. Deve ser possível disponibilizar SDK (Software Development Kit) que implemente a API em pelo menos na linguagem de programação Python e C++.

1.1.22.10. Deve implementar integração com plataforma de telemetria utilizando padrões abertos de transportes de dados e formatos de mensagens utilizando streaming.

1.1.23. **Documentação técnica**

1.1.23.1. Deverão ser fornecidos manuais técnicos do usuário e de referência contendo todas as informações sobre os produtos com as instruções para instalação, configuração, operação e administração. Será aceito que este conteúdo seja disponibilizado na web site do fabricante livre para download e sem necessidade de senhas para download.

1.2. **Grupo 1 – Item 1 – Switch Spine**

1.2.1. O switch será utilizado para o ambiente de Fabric IP VXLAN do MJSP, devendo possuir todos os requisitos gerais para os Switches de Data Center.

1.2.2. Deve poder atuar como Spine na topologia definida.

1.2.3. Deve, adicionalmente, atender aos seguintes requisitos:

1.2.3.1. O equipamento deve possuir no mínimo 32 (trinta e duas) portas 40/100 Gigabit Ethernet compatíveis com transceivers QSFP+ e QSFP28 sem nenhum bloqueio (non-blocking) para uplink.

1.2.3.2. Deve possuir 2 (duas) portas 1/10 Gigabit Ethernet adicionais compatíveis com transceivers SFP e SFP+.

1.2.3.3. Deve possuir no mínimo 1 (uma) porta de console para gerenciamento e configuração via linha de comando (CLI – Command Line Interface) com conector RJ-45 e 1 (uma) porta Ethernet RJ-45 para administração fora de banda (out-of-band management);

1.2.3.4. Deve possuir uma matriz de comutação em camada 2 com pelo menos 6,4Tbps

1.2.3.5. Deve possuir capacidade de encaminhamento de pelo menos 2Bpps em camada 2.

1.2.3.6. Deve possuir buffer mínimo de 40 MB.

1.2.3.7. Deve possuir latência menor ou igual a 2.000 (dois mil) nanosegundos;

1.2.3.8. Possuir capacidade para no mínimo 90.000 (noventa mil) endereços MAC;

1.2.3.9. Deve ser fornecido com sistema de ventilação Back-to-Front.

1.2.3.10. Deve suportar, respectivamente, pelo menos, 400.000 (quatrocentas mil) e 200.000 (duzentas mil) rotas IPv4 e IPv6.

1.2.3.11. Deve implementar o padrão IEEE 802.1ae MAC Security (MACsec), permitindo a criptografia de tráfego na camada física (hardware) e fornecendo uma comunicação segura os devices conectados ao switch.

1.2.3.11.1. Deve implementar MACSec através do algoritmo AES-128 ou AES-256;

1.2.3.11.2. Deve suportar MACSec em pelo menos 8 (oito) portas;

1.3. **Grupo 1 – Item 2 – Switch Leaf – Tipo A**

1.3.1. O switch será utilizado para o ambiente de Fabric IP VXLAN do MJSP, devendo possuir todos os requisitos gerais para os Switches de Data Center.

1.3.2. Deve poder atuar como Leaf na topologia definida.

1.3.3. Deve, adicionalmente, atender aos seguintes requisitos:

1.3.3.1. O equipamento deve possuir no mínimo 48 (quarenta e oito) portas 1/10/25 Gigabit Ethernet compatíveis com transceivers SFP, SFP+ e SFP28 sem nenhum bloqueio (non-blocking).

1.3.3.2. O equipamento deve possuir no mínimo 06 (seis) portas 40/100 Gigabit Ethernet

compatíveis com transceivers QSFP+ e QSFP28 sem nenhum bloqueio (non-blocking) para uplink.

1.3.3.3. Deve possuir no mínimo 1 (uma) porta de console para gerenciamento e configuração via linha de comando (CLI – Command Line Interface) com conector RJ-45 e 1 (uma) porta Ethernet RJ-45 para administração fora de banda (out-of-band management);

1.3.3.4. Deve possuir uma matriz de comutação em camada 2 com pelo menos 3,6Tbps

1.3.3.5. Deve possuir capacidade de encaminhamento de pelo menos 1Bpps em camada 2.

1.3.3.6. Deve possuir buffer mínimo de 40 MB.

1.3.3.7. Deve possuir latência menor ou igual a 1.000 (mil) nanosegundos;

1.3.3.8. Possuir capacidade para no mínimo 90.000 (noventa mil) endereços MAC;

1.3.3.9. Deve ser fornecido com sistema de ventilação Back to Front.

1.3.3.10. Deve suportar, respectivamente, pelo menos, 48.000 (quarenta e oito mil) e 24.000 (vinte e quatro mil) rotas IPv4 e IPv6.

1.4. **Grupo 1 – Item 3 – Switch Leaf – Tipo B**

1.4.1. O switch será utilizado para o ambiente de Fabric IP VXLAN do MJSP, devendo possuir todos os requisitos gerais para os Switches de Data Center.

1.4.2. Deve poder atuar como Leaf na topologia definida.

1.4.3. Deve, adicionalmente, atender aos seguintes requisitos:

1.4.3.1. O equipamento deve possuir no mínimo 36 (trinta e seis) portas 40/100 Gigabit Ethernet compatíveis com transceivers QSFP+ e QSFP28 sem nenhum bloqueio (non-blocking) para uplink.

1.4.3.2. Deve possuir no mínimo 1 (uma) porta de console para gerenciamento e configuração via linha de comando (CLI – Command Line Interface) com conector RJ-45 e 1 (uma) porta Ethernet RJ-45 para administração fora de banda (out-of-band management).

1.4.3.3. Deve possuir uma matriz de comutação em camada 2 com pelo menos 7,2Tbps

1.4.3.4. Deve possuir capacidade de encaminhamento de pelo menos 2Bpps em camada 2.

1.4.3.5. Deve possuir buffer mínimo de 40 MB.

1.4.3.6. Deve possuir latência menor ou igual a 2.000 (dois mil) nanosegundos;

1.4.3.7. Possuir capacidade para no mínimo 90.000 (noventa mil) endereços MAC;

1.4.3.8. Deve ser fornecido com sistema de ventilação Back to Front.

1.4.3.9. Deve suportar, respectivamente, pelo menos, 400.000 (quatrocentas mil) e 200.000 (duzentas mil) rotas IPv4 e IPv6.

1.4.3.10. Deve implementar o padrão IEEE 802.1ae MAC Security (MACsec), permitindo a criptografia de tráfego na camada física (hardware) e fornecendo uma comunicação segura os devices conectados ao switch.

1.4.3.10.1. Deve implementar MACSec através do algoritmo AES-128 ou AES-256;

1.4.3.10.2. Deve suportar MACSec em todas as portas;

1.5. **Grupo 1 – Item 4 – Switch de Agregação**

1.5.1. O equipamento deve possuir no mínimo 24 (vinte e quatro) portas 1/10/25 Gigabit Ethernet compatíveis com transceivers SFP, SFP+ e SFP28 sem nenhum bloqueio (non-blocking).

1.5.1.1. As portas devem ser compatíveis com os padrões IEEE 802.3by (25GBase-SR), IEEE 802.3cc (25GBase-LR), IEEE 802.3ab (10GBase-SR e 10GBase-LR), IEEE 802.3z (1000Base-SX e 1000Base-LX/LH) e IEEE 802.ab (1000Base-T);

1.5.1.2. As portas 1/10/25Gbps não poderão desativar nenhuma das demais portas especificadas;

1.5.2. O equipamento deve possuir no mínimo 04 (quatro) portas 40/100 Gigabit Ethernet compatíveis com transceivers QSFP+ e QSFP28 sem nenhum bloqueio (non-blocking) para uplink.

1.5.2.1. As portas devem ser compatíveis com os padrões IEEE 802.3bm (100GBase-SR4), IEEE 802.3ba (100GBase-LR4, 40GBase-SR4, e 40GBase-LR4) e 40GBase-SR-BiDi;

1.5.2.2. As portas 40/100Gbps não poderão desativar nenhuma das demais portas especificadas;

1.5.3. Possuir LEDs que indiquem o status de funcionamento do equipamento (switch, portas, ventilação e fonte de alimentação) e a localização (Beacon LED).

1.5.4. Deve ser fornecido com todos os hardwares e licenças necessários para a implementação de todas as funcionalidades descritas nesta especificação.

1.5.5. Suporte a Jumbo Frames de no mínimo 9.198 bytes;

1.5.6. Possuir porta USB compatível com flash drives, para cópias de arquivos de configuração e arquivos de sistema operacional.

1.5.7. Deve possuir no mínimo 1 (uma) porta de console para gerenciamento e configuração via linha de comando (CLI – Command Line Interface) com conector RJ-45 e 1 (uma) porta Ethernet RJ-45 para administração fora de banda (out-of-band management).

1.5.8. Deve possuir fontes de alimentação internas e redundante com as seguintes características:

1.5.8.1. Chaveada ou com ajuste automático de tensão entre 115 a 240 volts e frequência de 60 Hz;

1.5.8.2. Operar normalmente em temperaturas de 0°C até 40°C e umidade de 5 a 90%;

1.5.8.3. Deverá ser capaz de alimentar o switch (mantendo o funcionamento das funcionalidades comuns) com apenas uma das fontes instalada;

1.5.8.4. As fontes deverão vir acompanhadas com cabos de energia elétrica em conformidade com o padrão NBR14.136.

1.5.8.5. Deve ser capaz de realizar a troca da fonte redundante com o equipamento em pleno funcionamento, sem nenhum impacto na performance (hot-swappable).

1.5.9. Deve ser instalável em rack padrão de 19" e ter no máximo 1RU de altura, sendo que deverão ser fornecidos os respectivos kit's de fixação;

1.5.10. Deve possui sistema de ventilação redundante e que permita substituição em caso de falha, sem necessidade de troca do switch.

1.5.11. Deve possuir capacidade de comutação de pelo menos 2Tbps;

1.5.12. Deve possuir capacidade de processamento de pacotes de pelo menos 1Bpps;

1.5.13. Deve possuir buffer de pacotes com, no mínimo, 36MBytes (Megabytes);

1.5.14. Possuir capacidade para no mínimo 80.000 (oitenta mil) endereços MAC;

1.5.15. Funcionalidades de Camada 2:

1.5.15.1. Implementar LAN Virtual (VLAN) conforme o padrão IEEE IEEE 802.1Q, permitindo a criação e ativação simultâneas de no mínimo 4.000 VLANs IDs e 1000 VLANs ativas simultaneamente.

1.5.15.2. Implementar "VLAN Trunking" conforme padrão IEEE 802.1Q nas interfaces exigidas. Deve ser possível estabelecer quais VLANs serão permitidas em cada um dos troncos configurados. Deve permitir que uma certa VLAN seja adicionada e removida do tronco sem a necessidade de adicionar e remover todas as demais VLANs configuradas anteriormente.

1.5.15.3. Deve permitir a criação, remoção e distribuição de VLANs de forma dinâmica através de portas configuradas como tronco IEEE 802.1Q.

1.5.15.4. Permitir a criação de subgrupos dentro de uma mesma VLAN com conceito de portas "isoladas" e portas "promíscuas", onde portas isoladas não se comunicam com outras portas isoladas, mas apenas com as portas promíscuas de uma dada VLAN.

1.5.15.5. Implementar a funcionalidade de agregação de portas conforme padrão IEEE 802.3ad (LACP) de modo que as portas agrupadas formem uma única interface lógica com as mesmas facilidades das interfaces originais.

1.5.15.6. Deve permitir pelo menos a criação de 12 (doze) grupos de portas agregadas, com pelo menos 8 (oito) portas por grupo.

1.5.15.7. Deve implementar funcionalidade que permita que este switch, em conjunto com outro switch de mesmo modelo, possa receber conexões vindas de um terceiro switch na forma de link aggregation. O terceiro switch em questão deverá perceber os dois switches logicamente como um só. Esta funcionalidade deve tomar como referências padrões como Multi-Chassis Link Aggregation (MLAG) ou Multi-Chassis EtherChannel (MEC). O único link lógico entre os dois switches descritos neste item e o terceiro switch deve eliminar convergência do Spanning Tree, possibilitando o tráfego simultâneo por mais de uma conexão (Layer 2 Multipathing).

1.5.15.8. Deve implementar o protocolo IEEE 802.1AB Link Layer Discovery Protocol (LLDP), permitindo a descoberta dos elementos de rede vizinhos.

1.5.15.9. Deve implementar, em hardware, o protocolo Virtual Extensible LAN (VXLAN) – que permite a criação de segmentos de redes virtuais e sua extensão através da camada de redes (nível 3) ao encapsular quadros Ethernet em pacotes IP através de UDP.

1.5.15.10. Deve implementar VXLAN utilizando MP-BGP EVPN (Multiprotocol BGP Ethernet VPN) como plano de controle.

1.5.15.11. Deve suportar a implementação da função de DHCP Server. capaz de suportar, pelos menos, a atribuição de endereço IPv4.

1.5.15.12. Deve ser suportara função de DHCP Relay por VLAN para IPv4 e IPv6;

1.5.15.13. Spanning Tree:

1.5.15.13.1. Implementar o padrão IEEE 802.1d ("Spanning Tree");

1.5.15.13.2. Implementar o padrão IEEE 802.1w ("Rapid Spanning Tree");

1.5.15.13.3. Implementar o padrão IEEE 802.1s ("Multiple Spanning Tree"), com suporte a no mínimo 64 (sessenta e quatro) instâncias simultâneas;

1.5.15.13.4. Implementar simultaneamente os padrões IEEE 802.1w e 802.1s com suporte a, no mínimo, 64 (sessenta e quatro) instâncias simultâneas;

1.5.15.13.5. Implementar mecanismo de Spanning-tree baseado em VLAN´s, em que cada VLAN executa o protocolo STP ou RSTP de forma independente;

1.5.15.13.6. Implementar mecanismo de proteção da "root bridge" do algoritmo Spanning-Tree para prover defesa contra ataques do tipo "Denial of Service" no ambiente nível 2.

1.5.15.13.7. Deve permitir a suspensão de recebimento de BPDUs (Bridge Protocol Data Units) caso a porta esteja colocada no modo "fast forwarding" (conforme previsto no padrão IEEE 802.1w). Sendo recebido um BPDU neste tipo de porta deve ser possível desabilitá-la automaticamente.

1.5.16. Funcionalidades de QoS

1.5.16.1. Possuir a facilidade de priorização de tráfego através do protocolo IEEE 802.1p.

1.5.16.2. Implementar pelo menos 08 (oito) filas de prioridade por porta de saída (egress port).

1.5.16.3. Implementar pelo menos 1 (uma) fila de saída com prioridade estrita (prioridade absoluta em relação às demais classes dentro do limite de banda que lhe foi atribuído) e divisão ponderada de banda entre as demais filas de saída.

1.5.16.4. Implementar classificação de tráfego baseada em endereço IP de origem e destino, portas TCP e UDP de origem e destino, endereços MAC de origem e destino.

1.5.16.5. Deve implementar classificação, marcação e priorização de tráfego baseada nos valores de classe de serviço do frame ethernet (IEEE 802.1p CoS – L2) e do campo "Differentiated Services Code Point" (DSCP) do cabeçalho IP (L3), conforme definições do IETF.

1.5.16.6. Implementar funcionalidades de "Traffic Shaping" e "Traffic Policing".

1.5.16.7. Deve ser possível a especificação de banda por classe de serviço. Para os pacotes que excederem a especificação deve ser possível configurar ações tais como: transmissão do pacote sem modificação, transmissão com remarcação do valor de DSCP e descarte do pacote.

1.5.17. Funcionalidades de Camada 3 - Roteamento (OSI):

1.5.17.1. Suportar roteamento de pacotes IPv4 e IPv6;

1.5.17.2. Deve permitir o roteamento nível 3 entre VLANs.

1.5.17.3. Deve implementar roteamento estático para IPv4 e IPv6.

1.5.17.4. Deve implementar roteamento dinâmico RIPv1 e RIPv2.

1.5.17.5. Deve implementar os protocolos de roteamento dinâmico OSPFv2 e OSPFv3. Devem ser suportados pelo menos 02 (dois) processos OSPF simultâneos;

1.5.17.6. Deve implementar protocolo de roteamento dinâmico BGPv4 para IPv4 e IPv6;

1.5.17.7. Deve suportar, pelo menos, 150.000 (cento e cinquenta mil) rotas IPv4 dinâmicas;

1.5.17.8. Deve suportar, pelo menos, 100.000 (cem mil) rotas IPv6 dinâmicas;

1.5.17.9. Deve suportar ao protocolo GRE (Generic Routing Encapsulation);

1.5.17.10. Deve implementar o protocolo de redundância de gateway VRRP (Virtual Router Redundancy Protocol) conforme as RFC 5798, suportando a configuração de 250 (duzentos e cinquenta) grupos simultaneamente.

1.5.17.11. Deve suportar PBR (Policy-Based Routing) permitindo a definição de políticas de roteamento baseadas em endereços de origem e outras condições especiais.

1.5.17.12. Deve permitir a virtualização das tabelas de roteamento de camada de rede (nível 3) utilizando a tecnologia conhecida como VRF (Virtual Routing and Forwarding), contemplando, no mínimo, as seguintes caracteŕisticas:

1.5.17.12.1. As tabelas virtuais de roteamento devem ser totalmente segregadas em cada equipamento;

1.5.17.12.2. Deve ser suportada a associação de interfaces roteáveis físicas e lógicas (sub-interfaces com 802.1q) a uma tabela virtual específica;

1.5.17.12.3. Deve ser possível criar rotas estáticas em cada uma das tabelas virtuais de roteamento;

1.5.17.12.4. Os protocolos dinâmicos de roteamento fornecidos devem suportar a troca de informações de forma completamente segregada para cada uma das tabelas virtuais criadas;

1.5.17.12.5. Deve ser possível visualizar as informações de cada uma das tabelas virtuais de roteamento de forma totalmente segmentada;

1.5.17.12.6. Suporte à associação de todas as interfaces roteadas (inclusive túneis GRE) à uma tabela virtual específica;

1.5.17.12.7. Devem ser suportadas, pelo menos, 500 (quinhentas) tabelas virtuais;

1.5.17.13. "Multicast":

1.5.17.13.1. Implementar IGMP para tráfego multicast, nas versões 1, 2 e 3;

1.5.17.13.2. Suportar, pelo menos, 1.000 (mil) grupos multicast;

1.5.17.13.3. Implementar IGMP Snooping (v1, v2 e v3). O comutador deve ser capaz de fazer

“snooping” de pacotes IGMPv1, IGMPv2 e IGMPv3;

1.5.17.13.4. Implementar roteamento multicast PIM (Protocol Independent Multicast) em modo “sparse-mode”, PIMv2 e PIM-SSM (Source-Specific Multicast);

1.5.17.13.5. Implementar em todas as interfaces do switch o protocolo MLD (Multicast Listener Discovery) Snooping (v1 e v2) para IPv6;

1.5.18. Funcionalidades de Segurança

1.5.18.1. Deve proteger a interface CLI do equipamento através de senha.

1.5.18.2. Deve implementar listas de controle de acesso (ACLs) baseadas em endereço IPv4 ou IPv6 de origem e destino, portas TCP e UDP de origem e destino, endereços MAC de origem e destino e flags TCP.

1.5.18.3. Deve implementar ACLs baseadas em endereços IP para limitar o acesso ao switch via Telnet e SSH. Deve ser possível definir os endereços IP de origem das sessões Telnet e SSH.

1.5.18.4. Deve permitir a configuração de, no mínimo, 2.000 (duas mil) ACLs.

1.5.18.5. Implementar ACLs baseadas em políticas (Policy Based ACLs), que permitem aplicar políticas de controle de acesso em grupos de objetos;

1.5.18.6. Permitir visualização das estatísticas de filtragem das listas de controle de acesso aplicadas;

1.5.18.7. Suportar autenticação, autorização e “accounting” via RADIUS.

1.5.18.8. Suportar protocolo de autenticação para controle do acesso administrativo ao equipamento que possua pelo menos as seguintes características:

1.5.18.8.1. Implemente mecanismos de AAA (Authentication, Authorization e Accounting) com garantia de entrega dos pacotes transferidos entre cliente e servidor AAA. Deve haver autenticação mútua entre o servidor AAA e o cliente AAA.

1.5.18.8.2. Implementar a criptografia de todos os pacotes enviados ao servidor de controle de acesso e não só os pacotes referentes à senha.

1.5.18.8.3. Permita controlar quais comandos os usuários e grupos de usuários podem executar nos equipamentos gerenciados. Devem ficar registrados no servidor AAA todos os comandos executados, assim como todas as tentativas não autorizadas de execução de comandos feitas por usuários que tiverem acesso ao equipamento gerenciado. Todos os comandos de administração do equipamento, executados por qualquer dos meios de acesso (interface de console, telnet, SSH e interface gráfica/HTTPS) deverão ser individualmente autorizados e registrados (“Accounting”) por este protocolo de controle de acesso administrativo.

1.5.18.8.4. Utilize o protocolo TCP para prover maior confiabilidade ao tráfego dos pacotes envolvidos no controle administrativo.

1.5.18.9. Implementar Controle de Acesso por porta (IEEE 802.1x) com as seguintes características:

1.5.18.9.1. Deve ser suportada a atribuição de VLANs após a identificação do usuário, atribuição do usuário a uma VLAN “Guest” caso a máquina que esteja utilizando para acesso à Rede n&atatilde;o tenha cliente 802.1x operacional. Caso ocorra falha de autenticação de um usuário com um cliente 802.1x operacional o mesmo deverá ser alocado em uma VLAN “quarentena” com características próprias.

1.5.18.9.2. Implementar “accounting” das conexões IEEE 802.1x. Devem ficar registradas pelo menos as seguintes informações da conexão: nome do usuário e grupo a que pertence, switch em que o computador do usuário está conectado, porta do switch usada para acesso, endereço MAC e IP da máquina usada pelo usuário, horários de início e término da conexão, bytes transmitidos e recebidos durante a sessão.

1.5.18.9.3. Implementar associação automática de VLAN da porta do switch através da qual o usuário requisitou acesso à rede (VLAN Assignment).

1.5.18.9.4. Implementar associação automática de ACL da porta do switch através da qual o usuário requisitou acesso à rede. (802.1x)

1.5.18.9.5. Deve ser possível especificar, por porta, o intervalo de tempo para obrigar o cliente a se reautenticar (reautenticação periódica).

1.5.18.9.6. Deve ser possível forçar de forma manual ou automática a reautenticação de um usuário conectado a uma porta do switch habilitada para 802.1x.

1.5.18.9.7. Suportar a autenticação 802.1x via endereço MAC em substituição à identificação de usuário, para equipamentos que não disponham de suplicantes.

1.5.18.9.8. Suportar a configuração de 802.1x utilizando autenticação via usuário e MAC simultaneamente na mesma porta do switch.

1.5.18.9.9. Deve ser capaz de intermediar o processo de autenticação 802.1x, enviando mensagens EAP-Request/Identity para o cliente 802.1x e repassando a resposta EAP-Response/Identity para o servidor.

1.5.18.9.10. Implementar serviço de DHCP Server em múltiplas VLANS simultaneamente, para que o switch possa atribuir endereços IP aos clientes 802.1x autenticados e autorizados.

1.5.18.9.11. Deve ser suportada a autenticação de múltiplos usuários em uma mesma porta.

1.5.18.9.12. Deve ser suportada a obtenção de credenciais do usuário através de navegador web (Web Authentication), caso a máquina utilizada para acesso à Rede não tenha cliente 802.1x operacional. O portal de autenticação local do switch deve utilizar protocolo HTTPS para obter de forma segura as credenciais do usuário.

1.5.18.9.13. Permitir o controle de desconexão de sessões de usuários via Radius (RFC 5176) ou implementar o mecanismo Radius “Change of Authorization”.

1.5.18.10. Permitir a associação de um endereço MAC específico a uma dada porta do switch, de modo que somente a estação que tenha tal endereço possa usar a referida porta para conexão. Deve ser possível enviar um trap SNMP caso algum MAC diferente tente se conectar à porta.

1.5.18.11. Deve ser possível estabelecer o número máximo de endereços MAC que podem estar associados a uma dada porta do switch. Deve ser possível enviar um trap SNMP caso o número de endereços MAC configurados para a porta seja excedido.

1.5.18.12. Implementar mecanismo de segurança do tipo anti-spoofing com tecnologia que utiliza a tabela de roteamento do equipamento de forma dinâmica, sem configuração de lista de acesso, e que possa ser configurado por interface.

1.5.18.13. Deve implementar NAT (Network Address Translation) e PAT (Port Address Translation) estático e dinâmico.

1.5.18.14. Possuir controle de broadcast, multicast e unicast por porta. Deve ser possível especificar limiares (“thresholds”) individuais para tráfego tolerável de broadcast, multicast e unicast em cada porta do switch. Excedidos os valores pré-configurados deve ser possível enviar um trap SNMP e desabilitar a porta.

1.5.18.15. Implementar inspeção do protocolo ARP (Address Resolution Protocol) e possuir mecanismos de proteção contra ataques do tipo “ARP Poisoning”.

1.5.18.16. Deve implementar funcionalidade que permita que somente servidores DHCP autorizados atribuam configuração IP aos clientes DHCP (Trusted DHCP Server).

1.5.18.17. Promover análise do protocolo DHCP e permitir que se crie uma tabela de associação entre endereços IP atribuídos dinamicamente, MAC da máquina que recebeu o endereço e porta física do switch em que se localiza tal MAC.

1.5.18.18. Deve suportar integração com ferramenta de solução de controle de acesso existente no MJSP, o qual está sendo atualizada através da Solução de Controle de Acesso. O switch ofertado deve constar na matriz de compatibilidade da ferramenta. Deve ser possível verificar a conformidade da máquina com a política de segurança considerando no mínimo os seguintes atributos: presença do antivírus e versão de pach to sistema operacional.

1.5.18.19. Deve implementar o padrão IEEE 802.1AE MAC Security (MACsec), permitindo a criptografia de tráfego na camada física (hardware) e fornecendo uma comunicação segura os devices conectados ao switch.

1.5.18.19.1. Deve implementar MACSec através do algoritmo AES-256;

1.5.18.19.2. Deve suportar MACSec em pelo menos 8 (oito) portas e em todas as velocidades suportadas.

1.5.19. Funcionalidades de Gerenciamento

1.5.19.1. Possuir uma interface de gerenciamento baseada em WEB (HTTP) que permita aos usuários configurar e gerenciar switches através de um browser padrão, implementar o protocolo HTTPS para gerenciamento gráfico seguro do equipamento. No caso de gerenciamento via HTTPS, deve ser suportado no mínimo os algoritmos criptográficos 3DES e AES 128.

1.5.19.2. Deve ser gerenciável via Telnet (com no mínimo 5 sessões simultâneas);

1.5.19.3. Deve ser gerenciável via SSH versão 2 (SSHv2), suportando, no mínimo, o algoritmo de criptografia 3DES, com no mínimo, 5 sessões simultâneas;

1.5.19.4. Deve implementar, em hardware, tecnologia para monitoramento de tráfego que permita agrupar os pacotes que circulam pelo equipamento usando o conceito de fluxos (“flows”). Para cada fluxo devem ser exibidas, no mínimo, as seguintes informações: endereços IP de origem/destino, portas TCP/UDP de origem/destino, interfaces de entrada e saída do tráfego, número de pacotes transmitidos, garantindo alta visibilidade do tráfego de rede. As informações coletadas devem ser automaticamente exportáveis em intervalos pré-definidos através de Netflow v9 ou conforme a RFC 7011 (IETF - Specification of the IP Flow Information Export (IPFIX) Protocol for the Exchange of Flow Information). A ativação dessa ferramenta não poderá alterar o desempenho do switch.

1.5.19.5. Permitir o espelhamento da totalidade do tráfego de uma VLAN, de uma porta ou de um grupo de portas para uma porta especificada.

1.5.19.5.1. Deve ser possível espelhar o tráfego para outra porta localizada no mesmo switch e para um endereço IP remoto.

1.5.19.5.2. Deve ser possível definir o sentido do tráfego a ser espelhado: somente tráfego de entrada, somente tráfego de saída e ambos simultaneamente.

1.5.19.5.3. Devem ser suportadas pelo menos 2 (duas) sessões simultâneas de espelhamento

ativas simultaneamente.

1.5.19.6. Implementar os padrões abertos de gerência de rede SNMPv1, SNMPv2c e SNMPv3.

1.5.19.7. Implementar pelo menos os seguintes níveis de segurança para SNMP versão 3: sem autenticação e sem privacidade (noAuthNoPriv); com autenticação e sem privacidade (authNoPriv); e com autenticação e com privacidade (authPriv). Deve suportar no mínimo os algoritmos criptográficos 3DES e AES128 no modo AuthPriv.

1.5.19.8. Possibilitar a obtenção da configuração do equipamento através do protocolo SNMP;

1.5.19.9. Permitir o controle da geração de traps SNMP, possibilitando definir quais tipos de alarmes geram traps.

1.5.19.10. Implementar a MIB privativa que forneça informações relativas ao funcionamento do equipamento.

1.5.19.11. Possuir descrição completa da MIB implementada no equipamento, inclusive a extensão privativa.

1.5.19.12. Permitir o armazenamento de sua configuração em memória não volátil, podendo, numa queda e posterior restabelecimento da alimentação, voltar à operação normalmente na mesma configuração anterior à queda de alimentação.

1.5.19.13. Permitir a atualização de software sem perda de pacotes (tecnologia conhecida como ISSU – In Services Software Upgrades) para funcionalidades de camada de rede (nível 2).

1.5.19.14. Implementar nativamente, sem uso de probes externas, os seguintes grupos RMON (Alarms e Events);

1.5.19.15. Possuir ferramentas para depuração e gerenciamento em primeiro nível, tais como debug, trace, log de eventos.

1.5.19.16. Possuir armazenamento interno das mensagens de log geradas pelo equipamento.

1.5.19.17. Possuir capacidade de exportar as mensagens de log geradas pelo equipamento para um servidor syslog externo.

1.5.19.18. Possibilidade de configuração automática via rede através de protocolo BOOTP.

1.5.19.19. Possibilidade de atualização do sistema operacional através do protocolo TFTP (Trivial Fiel Transfer Protocol) ou FTP (File Transfer Protocol).

1.5.19.20. Possibilidade de transferência segura e autenticada de arquivos através de SCP (Secure Copy Protocol) ou SFTP (SSH File Transfer Protocol).

1.5.19.21. Implementar o protocolo NTP (Network Time Protocol);

1.5.19.22. Implementar o protocolo PTP (Precision Time Protocol) de acordo com o padrão IEEE 1588;

1.5.19.23. Deve implementar mecanismo interno para responder a pacotes de teste de performance de rede, com capacidade de medir latência de conexões TCP e jitter de conexões UDP. Devem ser suportadas, no mínimo, as seguintes opções de testes a partir do switch ofertado: ICMP echo, TCP connect (em qualquer porta TCP do intervalo 1-65535 que o administrador especifique), UDP echo (em qualquer porta UDP do intervalo 1-65535 que o administrador especifique). Deve implementar pelo menos 5 (cinco) destas operações de testes simultaneamente.

1.5.19.24. Possuir funcionalidade de tratamento de eventos, permitindo a definição de valores de limiar (thresholds) de CPU e memória do equipamento, permitindo o envio de mensagens de syslog ou traps SNMP quando estes valores forem atingidos.

1.5.19.25. Deverá permitir a configuração de endereços IPv6 para gerenciamento e operar em modo dual stack (IPv4 e IPv6), suportando rotas estáticas em IPv6 assim como consulta de DNS com resolução de nomes em endereços IPv6;

1.5.19.26. Deverá implementar ICMPv6 com as seguintes funcionalidades: ICMP request, ICMP Reply, ICMP Neighbor Discovery Protocol(NDP), ICMP MTU Discovery.

1.5.19.27. Implementar protocolos de gerenciamento Ping, Traceroute, Telnet, SSH, e DNS sobre IPv6.

1.5.20. Funcionalidades de Programabilidade

1.5.20.1. Os switches que compõem esta solução deverão suportar funcionamento em modo switch ou modo SDN (Software Defined Network), seja através de configuração ou com a troca do sistema operacional do equipamento, com ou sem necessidade de licenciamento adicional.

1.5.20.2. Deve suportar mecanismo de auto provisionamento para simplificação do processo de configuração e atualização de imagem e firmware do equipamento.

1.5.20.3. Deve possuir uma plataforma aberta, com flexibilidade para programação via API (Application Programming Interface).

1.5.20.4. Deve implementar API modeladas de acordo com o padrão YANG de acordo com as definições do OpenConfig.

1.5.20.5. O fabricante deve disponibilizar em site público de forma gratuita os modelos YANG nativos (específicos desta plataforma de equipamentos) e variações dos abertos, assim como manter os modelos atualizados.

1.5.20.6. Deve implementar, no mínimo, os protocolos de gerenciamento de redes NETCONF e RESTCONF.

1.5.20.7. Deve implementar, no mínimo, as codificações de dados nos formatos XML e JSON.

1.5.20.8. Deve suportar scripts de configuração em Python nativamente na caixa.

1.5.20.9. Deve implementar integração com plataforma de telemetria utilizando padrões abertos de transportes de dados e formatos de mensagens utilizando streaming.

1.5.21. Documentação técnica

1.5.21.1. Deverão ser fornecidos manuais técnicos do usuário e de referência contendo todas as informações sobre os produtos com as instruções para instalação, configuração, operação e administração. Será aceito que este conteúdo seja disponibilizado na web site do fabricante livre para download e sem necessidade de senhas para download.

1.6. **Grupo 1 – Item 5 – Sistema de Gerenciamento para equipamentos de Data Center**

1.6.1. Deve ser entregue em formato de appliance virtual.

1.6.2. Deve estar totalmente licenciado para instalação e funcionamento bem como ser compatível com solução de virtualização VMWare ESXi na versão 5.5 ou superior.

1.6.3. Não poderá haver ônus adicionais à contratante para o pleno funcionamento do software sob qualquer das formas de virtualização do item anterior;

1.6.4. A instalação e configuração da máquina virtual e do sistema de gerenciamento deverão ser efetuadas pela contratada;

1.6.5. A máquina virtual deverá ser instalada em equipamento servidor da contratante.

1.6.6. Dispositivos Gerenciados:

1.6.6.1. O sistema deve permitir o gerenciamento dos switches para Data Center (tanto Spines quanto Leafs);

1.6.6.2. Deve estar licenciado para gerenciar TODOS os switches de Data Center (Spine/Leaf) descritos neste termo de referência, devendo seu licenciamento ser incluído em cada item;

1.6.6.3. Deve estar licenciado para gerenciar os equipamentos existentes na infraestrutura do MJSP:

1.6.6.3.1. Switches Cisco Nexus 56128P – 02 unidades;

1.6.6.3.2. Cisco Fabric Extenders 2348UPQ – 04 unidades;

1.6.7. Características Gerais – O Sistema de Gerenciamento deve:

1.6.7.1. Utilizar o protocolo gerenciamento SNMP v1, v2, e v3 autenticado para os dispositivos de rede;

1.6.7.2. Permitir a administração centralizada de todos os dispositivos da rede via interface gráfica Web GUI ou Java;

1.6.7.3. Permitir a exibição da topologia da rede; a descoberta dos equipamentos (e suas interligações) deve ser feita obrigatoriamente de forma automática, permitindo também sua configuração/personalização manual;

1.6.7.4. Exibir as representações gráficas dos equipamentos, mostrando o estado operacional das portas, permitindo inclusive a configuração e monitoramento em tempo real;

1.6.7.5. Permitir a configuração de diferentes perfis de usuários, tornando possível a criação de perfis administrativos e de perfis operacionais (visualização);

1.6.7.6. O sistema deverá suportar utilização de controle AAA (Authentication, Authorization & Accounting) através de RADIUS ou TACACS+;

1.6.7.7. Prover detecção de falhas em tempo real, além de oferecer relatórios e regras de tratamento de alarmes pré-configuradas para ações de intervenção;

1.6.7.8. Permitir a monitoração do estado das portas, realizando a intervenção de ativação e suspensão da porta na rede;

1.6.7.9. Possibilitar o acompanhamento online da situação de cada porta, apresentando informações como tráfego, quantidade de pacotes descartados, quantidade de pacotes do tipo broadcast, por exemplo;

1.6.7.10. Utilizar códigos de cores para sinalizar as situações de cada elemento da rede;

1.6.7.11. Realizar a análise das mensagens de syslog dos dispositivos de rede;

1.6.7.12. Permitir processamento de mensagens syslog ou traps SNMP para gerenciar falhas nos equipamentos;

1.6.7.13. Permitir o encaminhamento de mensagens de syslog para outros sistemas;

1.6.7.14. Possibilitar a criação, exclusão e edição de VLANs nos dispositivos de rede por meio de interface gráfica amigável;

1.6.7.15. Possibilitar a configuração e a visualização dos parâmetros de Spanning Tree;

1.6.7.16. Possibilitar a configuração e a visualização dos parâmetros de camada de rede (nível 3), como endereços IPv4 e IPv6 e redundância de roteamento (VRRP ou similar);

1.6.7.17. Possibilitar a configuração e a visualização dos parâmetros do protocolo multicast IGMPv2, IGMPv3 e IGMP Snooping (v2 e v3);

1.6.7.18. Possibilitar a configuração de cada elemento isoladamente e também em grupos; deve ser possível, por exemplo, a inclusão de uma configuração específica em vários equipamentos ao mesmo tempo por meio de ferramenta gráfica, facilitando desta forma a alteração de configurações comuns a um grande grupo de dispositivos;

1.6.7.19. Possibilitar o gerenciamento de inventário da rede, permitindo o armazenamento de várias cópias das configurações dos dispositivos e oferecendo, inclusive, opções para comparar configurações de diferentes datas para visualizar alterações realizadas;

1.6.7.20. Prover funcionalidades de agendamento de downloads das configurações dos equipamentos da rede, evitando desta forma que este procedimento seja realizado em horários nos quais a rede normalmente é mais utilizada;

1.6.7.21. Todo gerenciamento do software dos equipamentos deve ser provido pelo Sistema de Gerenciamento. O software deve ser capaz de realizar o upgrade de software nos equipamentos existentes na infraestrutura atual, facilitando desta forma o processo;

1.6.7.22. Fornecer ferramentas para verificação de tempo de resposta entre os elementos da rede, utilizando diferentes protocolos no processo de medição; a performance da rede deve poder ser acompanhada por meio de relatórios históricos e em tempo real;

1.6.7.23. Oferecer interfaces para integração com outras ferramentas de gerência;

1.6.7.24. Disponibilizar os relatórios fornecidos/gerados via interface gráfica;

1.6.7.25. Suportar notificação de eventos através de e-mail e traps;

1.6.7.26. Suportar a criação de templates para configuração dos equipamentos.

1.7. **Grupo 1 – Item 6 – Solução de Controle de Acesso – Virtual Machine**

1.7.1. Deve ser entregue em formato de appliance virtual.

1.7.2. Deve estar totalmente licenciado para instalação e funcionamento bem como ser compatível com solução de virtualização VMWare ESXi na versão 5.5 ou superior.

1.7.3. Não poderá haver ônus adicionais à contratante para o pleno funcionamento do software sob qualquer das formas de virtualização do item anterior;

1.7.4. A instalação e configuração da máquina virtual e do sistema de gerenciamento deverão ser efetuadas pela contratada;

1.7.5. A máquina virtual deverá ser instalada em equipamento servidor da contratante.

1.7.6. Deve ser compatível com o licenciamento existente no MJSP, permitindo sua migração para o novo servidor virtualizado:

1.7.6.1. Appliance SNS-3415-K9 – Cisco ISE versão 1.2.1.198 com 2000 licenças do tipo Base;

1.7.6.2. 4950 licenças Cisco ISE do tipo Base adquiridas em conjunto com os switches LAN existentes.

1.7.7. Deve suportar pelo menos 10.000 usuários em um único appliance virtual.

1.7.8. Características Gerais – O Sistema de Gerenciamento deve:

1.7.8.1. A solução deve possuir administração centralizada por console único de gerenciamento com interface gráfica intuitiva e fácil de usar, acessível via web;

1.7.8.2. Deve ser capaz de ser distribuída como um serviço gerenciado;

1.7.8.3. Deve conter mecanismo de comunicação em tempo real entre servidor e clientes, para entrega de configurações e políticas;

1.7.8.4. Deve possuir integração com Open LDAP, Microsoft Active Directory para importação da estrutura organizacional;

1.7.8.5. Deve possibilidade de aplicar regras diferenciadas baseando na localidade lógica da rede;

1.7.8.6. Deve possibilidade de aplicar regras diferenciadas por grupos de usuários e máquinas;

1.7.8.7. Deve possuir recursos para a criação e agendamento periódicos;

1.7.8.8. Deve permitir criar contas de usuário com diferentes níveis de acesso de administração e operação;

1.7.8.9. Deve permitir a atualização remota e incremental da versão do software cliente instalado;

1.7.8.10. Nas atualizações das configurações deverá ser possível realizá-las sem utilizar login scripts, agendamentos ou tarefas manuais ou outros módulos adicionais que não sejam parte integrante da solução;

1.7.8.11. Deve fornecer ferramenta de pesquisa de estações e servidores da rede que não

possuem o cliente instalado com opção de instalação remota;

1.7.8.12. Deve possuir interface para construção de regras customizadas de classificação de dispositivo com suporte a operadores lógicos;

1.7.8.13. Deve possuir uma base de regras e categorias pré-configuradas;

1.7.8.14. Deverá ser capaz de gerenciar, configurar e alterar regras e políticas através de interface gráfica web;

1.7.8.15. Deve possuir Dashboard para rápida visualização das informações sumarizadas:

1.7.8.15.1. Métrica das últimas 24 horas:

1.7.8.15.1.1. Número de dispositivos ativos;

1.7.8.15.1.2. Número de visitantes ativos;

1.7.8.15.1.3. Tempo médio para remediar os dispositivos;

1.7.8.15.1.4. Porcentagem dos dispositivos em conformidade;

1.7.8.15.1.5. Número de dispositivos descobertos.

1.7.8.15.2. Informações de performance, CPU, Memória de cada componente da solução;

1.7.8.15.3. Total de falhas de autenticação das últimas 24 horas e a principal razão;

1.7.8.16. Deve possuir tela de monitoração contínua das autenticações em tempo real com visualização imediata das seguintes informações:

1.7.8.16.1. Data e horário;

1.7.8.16.2. Link com os detalhes avançados da autenticação;

1.7.8.16.3. Status da autenticação;

1.7.8.16.4. Nome do usuário/dispositivo;

1.7.8.16.5. Endereço MAC;

1.7.8.16.6. Endereço IP;

1.7.8.16.7. NAD;

1.7.8.16.8. Interface;

1.7.8.16.9. Perfil de Autorização concedido;

1.7.8.16.10. Resultado da classificação do dispositivo – Categoria;

1.7.8.16.11. Status de Postura, conformidade;

1.7.8.16.12. Razão em caso de falha;

1.7.8.16.13. Método de autenticação;

1.7.8.16.14. Protocolo de autenticação;

1.7.8.17. Deverá ser capaz de gerar relatórios com as informações referentes ao resultado da verificação da postura da máquina;

1.7.8.18. Toda a comunicação entre o dispositivo de gerenciamento de políticas e o dispositivo gerenciado deverá ser criptografada através da utilização do SSL (Secure Socket Layer);

1.7.9. Requisitos de autenticação:

1.7.9.1. Suportar protocolos EAP (autenticação extensível), PAP (autenticação de senha) e CHAP (autenticação de handshake de desafio;

1.7.9.2. A solução deverá implementar autenticação de dispositivos e usuários utilizando o padrão IEEE802.1X suportando pelo menos os seguintes métodos EAP: EAP-MD5, EAP-TLS, PEAP-MSCHAPV2, EAP-FAST, PEAPGTC;

1.7.9.3. Deve permitir a autenticação dos usuários/dispositivos nas seguintes bases de dados:

1.7.9.3.1. Local do tipo usuário;

1.7.9.3.2. Local do tipo dispositivo;

1.7.9.3.3. Externa via RADIUS;

1.7.9.3.4. Externa via LDAP;

1.7.9.3.5. Externa via Windows Active Directory;

1.7.9.3.6. Certificado Digital;

1.7.9.4. A solução deverá permitir a integração com a base de usuários do AD (Active Directory) para login único do usuário (Sign Sign On - SSO). As credenciais do usuário utilizadas no momento de autenticação do Windows deverão ser utilizadas na autenticação do usuário na solução de controle de acesso de forma automática sem que o usuário tenha que entrar com as credenciais novamente;

1.7.9.5. Deverá oferecer suporte à SAML SSO (Security Assertion Markup Language);

1.7.9.6. A solução deverá oferecer autenticação de usuários através de portal web seguro HTTPS com redirecionamento automático;

1.7.9.7. A solução deverá implementar autenticação específica para dispositivos do tipo MAC

Address conforme método MAB (Mac Authentication Bypass);

1.7.9.8. A solução deverá possuir uma base de dados interna para registro de dispositivos do tipo MAC Address podendo esta base ser preenchida automaticamente pelo mecanismo de descoberta automático de dispositivo;

1.7.9.9. A solução deverá implementar validação de certificados digitais atendendo as seguintes caraterísticas:

1.7.9.9.1. Suportar o cadastramento de pelo menos duas CA (Certificate Authority) externos;

1.7.9.9.2. Suportar consulta periódica da lista de revogados CRL (Certificate Revogation List) via HTTP;

1.7.9.9.3. Suportar o protocolo OCSP para verificação do estado do certificado;

1.7.9.10. A solução deverá implementar mecanismo flexível de regras que permita selecionar a base de dados onde será autenticado o usuário/dispositivos com base nos atributos RADIUS existentes na solicitação enviada pelo NAD (Network Access Device) e tipo de protocolo permitindo pelo menos a seguinte combinação de regras;

1.7.9.11. Deve prover servidor Radius com suporte aos métodos EAP;

1.7.9.12. Deve implementar autenticação Radius baseada em endereço MAC (Radius-based MAC authentication) dos dispositivos clientes;

1.7.9.13. Deve implementar base de dados interna centralizada para registro dos endereços MAC dos dispositivos que serão autenticados por esta funcionalidade;

1.7.9.14. Deve permitir a carga de um arquivo contendo uma lista de endereços MAC permitidos a partir de um único ponto de cadastramento;

1.7.9.15. Deve ser capaz de identificar dispositivos de redes que não são capazes de realizar autenticação, como catracas, câmeras de vigilância, detectores de fumaça, impressoras etc. e criar políticas de acesso a rede para esses dispositivos através do endereço MAC da interface de rede;

1.7.9.16. O servidor deverá conter mecanismo de comunicação em tempo de terminado pelo administrador entre o cliente e servidor, para consulta de novas configurações e políticas;

1.7.9.17. Deve suportar redirecionamentos dos logs para um servidor de Syslog da CONTRATANTE;

1.7.9.18. Utilizar os protocolos HTTP e HTTPS para comunicação entre console de gerenciamento e o cliente gerenciado;

1.7.9.19. Deverá suportar implementar validação de certificados digitais atendendo as seguintes caraterísticas:

1.7.9.20. Deve suportar o cadastramento de CA (Certificate Authority) externos;

1.7.9.21. Deve suportar consulta periódica da lista de revogados CRL (Certificate Revogation List) via HTTP;

1.7.9.22. Deve suportar o protocolo OCSP (Online Certificate Status Protocol) para verificação do estado do certificado;

1.7.10. Requisitos de autorização:

1.7.10.1. Deve implementar atribuição de VLAN;

1.7.10.2. Deve implementar atribuição de ACL do tipo Downloadable compatível com os Switchs;

1.7.10.3. Deve implementar atribuição de ACL do tipo named compatível com os Controladores Wireless;

1.7.10.4. Deve implementar atribuição de ACL do tipo “filter-id”;

1.7.10.5. Deve implementar atribuição de ACL do tipo Redirecionamento Web;

1.7.10.6. Deve implementar atribuição de política MacSec conforme padrão IEEE802.1AE;

1.7.10.7. Deve implementar atribuição do domínio de voz para telefones IP (Voice Domain);

1.7.10.8. Deve implementar atribuição do parâmetro de re-autenticação 802.1X;

1.7.10.9. Deve permitir a customização de atributos de autorização;

1.7.10.10. Deve permitir o agrupamento de atributos de autorização;

1.7.10.11. Deve permitir a criação de perfis de usuários;

1.7.10.12. Deve permitir autorização de acesso condicional com base nos seguintes fatores:

1.7.10.12.1. Atributos LDAP do usuário autenticado;

1.7.10.12.2. Grupo de Active Directory do usuário autenticado;

1.7.10.12.3. Conteúdo do certificado digital (CN, OU);

1.7.10.12.4. Horário de conexão;

1.7.10.12.5. Tipo de acesso;

1.7.10.12.6. Localização;

1.7.10.12.7. Tipo de dispositivo (iPad, iPhone, Android, Windows, MAC OS);

1.7.10.12.8. Conformidade dos sistemas Windows e MAC OS;

1.7.10.13. Deve implementar o protocolo RADIUS Change of Authorization (CoA);

1.7.11. Deve realizar a gestão de contas temporárias (visitantes/consultores) com as seguintes:

1.7.11.1. O serviço web de autenticação (captive portal) deve ser fornecido e hospedado dentro da solução ofertada, além de permitir que as requisições possam ser redirecionadas para um serviço externo (internet);

1.7.11.2. Deve implementar um portal web seguro SSL para criação de contas temporárias do tipo "visitante, consultor" com autenticação de autorizadores em base externa do tipo Active Directory, LDAP e atribuição de privilégio ao autorizador de acordo com seu perfil;

1.7.11.3. Deve realizar a autenticação dos autorizadores em base externa do tipo Open LDAP e atribuir o privilégio ao autorizador de acordo com perfil do usuário;

1.7.11.4. Deve permitir que as contas de usuários visitantes sejam gerenciadas internamente pela solução, não havendo necessidade de integração com o Open LDAP da CONTRATANTE;

1.7.11.5. Deve permitir a criação de perfil de contas temporárias podendo atribuir privilégio de acesso a rede distintos atendendo no mínimo os seguintes privilégios:

1.7.11.5.1. Perfil Visitante – Somente acesso HTTP para Internet;

1.7.11.5.2. Perfil Consultor – Somente acesso HTTP para Internet e Intranet;

1.7.11.6. Deve permitir a criação de "Perfil de Tempo" declarando:

1.7.11.6.1. A conta temporária tem validade de 1 dia a partir de sua criação;

1.7.11.6.2. A conta temporária tem validade de 7 dias a partir de sua criação;

1.7.11.6.3. A conta temporária tem validade de 1 dia a partir do primeiro login;

1.7.11.6.4. A conta temporária tem validade de 7 dias a partir do primeiro login;

1.7.11.6.5. O autorizador determinará o início e fim de cada conta de acordo com seu privilégio de autorizador;

1.7.11.7. Deve permitir a criação de perfis de validade das credenciais, baseando o início da validade na criação da conta ou no primeiro login da conta;

1.7.11.8. Deve permitir a criação de perfis de acesso para as credenciais temporárias com diferentes privilégios de acesso à rede;

1.7.11.9. Deve permitir a criação de grupos de autorizadores com privilégios distintos de criação de contas temporárias especificando os seguintes privilégios por grupo:

1.7.11.9.1. Criar conta individual;

1.7.11.9.2. Criar contas aleatórias;

1.7.11.9.3. Importar contas de arquivo .csv;

1.7.11.9.4. Enviar credencial via Email;

1.7.11.9.5. Enviar credencial via SMS;

1.7.11.9.6. Ver a senha da conta de visitante;

1.7.11.9.7. Imprimir detalhes da conta visitante;

1.7.11.9.8. Ver e editar as contas criadas por todos os grupos de autorizadores;

1.7.11.9.9. Ver e editar as contas criadas pelo mesmo grupo de autorizadores;

1.7.11.9.10. Ver e editar as contas criadas pelo próprio autorizador;

1.7.11.9.11. Suspender contas criadas por todos os grupos de autorizadores;

1.7.11.9.12. Suspender contas criadas pelo mesmo grupo de autorizadores;

1.7.11.9.13. Suspender contas criadas pelo próprio autorizador;

1.7.11.9.14. Duração máxima da conta visitante;

1.7.11.9.15. Especificar o Perfil de acesso a rede que será atribuído a conta visitante;

1.7.11.9.16. Especificar o Perfil de Tempo que será atribuído ao visitante;

1.7.11.10. Deve permitir a customização do formulário de criação de contas temporárias a ser preenchido pelo autorizador especificando quais campos são obrigatórios e quais campos são opcionais bem como permitir a criação de novos campos:

1.7.11.10.1. Nome;

1.7.11.10.2. Sobrenome;

1.7.11.10.3. Email;

1.7.11.10.4. Empresa;

1.7.11.10.5. Telefone;

1.7.11.10.6. Campo Customizado.

1.7.11.11. Deve implementar a importação e exportação da relação de credenciais temporárias através de arquivos txt ou csv;

1.7.11.12. Deve implementar as funcionalidades de geração aleatória de lotes de credenciais temporárias;

1.7.11.13. Deve permitir a customização do nível de segurança da senha temporária que será gerada ao visitante, especificando a quantidade mínima de caracteres, quantos caracteres especiais e quantos números serão utilizados para compor a senha temporária;

1.7.11.14. Deve implementar um portal web seguro SSL a ser apresentado automaticamente aos usuários temporários (visitante/consultor) durante a sua conexão com a rede (hotspot);

1.7.11.15. Deve permitir a customização das páginas web do portal, com a inclusão de imagens, instruções em texto e campos de texto que devem ser preenchidos pelos clientes.

1.7.11.16. Deve possuir suporte nativo as línguas Inglês, Francês, Italiano, Espanhol, Alemão, Russo, Chinês e Português Brasil;

1.7.11.17. Deve permitir que o visitante crie sua própria credencial temporária ("self-service") através da portal web, sem a necessidade de um autorizador;

1.7.11.18. Deve implementar as seguintes funções no Portal Web (hotspot):

1.7.11.18.1. Permitir a troca de senha do usuário visitante diretamente pelo portal seguro;

1.7.11.18.2. Deve permitir configurar o número máximo de dias decorridos antes de exigir a troca da senha do usuário visitante;

1.7.11.18.3. Determinar o número máximo de erros de login antes de bloquear a conta;

1.7.11.18.4. Deve permitir configurar o número máximo de erros de login antes de bloquear a conta do usuário visitante;

1.7.11.18.5. Deve exigir que o usuário visitante aceite o "Termo de uso da rede" a cada login ou apenas no primeiro login;

1.7.11.18.6. Exigir somente no primeiro login o aceito do "Termo de uso aceitável de rede";

1.7.11.18.7. Customização da página de "Termo de uso aceitável de rede".

1.7.11.19. Deve implementar o envio das credenciais aos usuários registrados através de mensagens SMS (Short Message Service), email ou impressão local;

1.8. **Grupo 1 – Item 7 – Licenciamento para Switches Existentes**

1.8.1. Características Gerais

1.8.1.1. Deve ser compatível com o switch Cisco Nexus 56128P existente no MJSP;

1.8.1.2. Deve permitir a configuração do protocolo Virtual Extensible LAN (VXLAN) – que permite a criação de segmentos de redes virtuais e sua extensão através da camada de redes (nível 3) ao encapsular quadros Ethernet em pacotes IP através de UDP.

1.8.1.3. Deve permitir a configuração de Fabric VXLAN utilizando MP-BGP EVPN (Multiprotocol BGP Ethernet VPN) como plano de controle.

1.8.1.4. Deve permitir a configuração do protocolo de roteamento dinâmico BGPv4 para IPv4 e IPv6;

1.8.1.5. Deve permitir a configuração de PBR (Policy-Based Routing) permitindo a definição de políticas de roteamento baseadas em endereços de origem e outras condições especiais.

1.8.1.6. Deve permitir configurar roteamento multicast PIMv2 (Protocol Independent Multicast) nos modos PIM-SM (Sparse Mode), PIM-SSM (Source-Specific Multicast) e MSDP (Multicast Source Discovery Protocol).

1.8.1.7. Deve ser configurado e instalado para sua plena operacionalização.

1.9. **Grupo 1 – Item 8 – Transceiver 10Gbps Multimodo (LC)**

1.9.1. Características Gerais

1.9.1.1. Deve implementar o padrão 10GBase-SR, operando sobre fibras multimodo OM3/OM4 para distâncias de até 300m/400m, respectivamente;

1.9.1.2. Deve ser compatível com fibras de 850nm;

1.9.1.3. Deve permitir a instalação em slots/portas tipo SFP+;

1.9.1.4. Deve ser do tipo hot-swappable, permitindo sua conexão/desconexão com o equipamento em operação;

1.9.1.5. Deve possuir conector do tipo LC duplex;

1.9.1.6. Deve ser do mesmo fabricante e deverá constar na matriz de compatibilidade dos equipamentos listados neste grupo.

1.9.1.7. Deve possuir garantia total do fabricante por um período de pelo menos 12 (doze) meses.

1.10. **Grupo 1 - Item 9 - Transceiver 25G Multimodo (LC)**

1.10.1. Características Gerais

1.10.1.1. Deve implementar o padrão 25GBase-SR, operando sobre fibras multimodo OM3/OM4 para distâncias de até 30m/50m, respectivamente;

1.10.1.2. Deve ser compatível com fibras de 850nm;

1.10.1.3. Deve permitir a instalação em slots/portas tipo SFP28;

1.10.1.4. Deve ser do tipo hot-swappable, permitindo sua conexão/desconexão com o equipamento em operação;

1.10.1.5. Deve possuir conector do tipo LC duplex;

1.10.1.6. Deve ser do mesmo fabricante e deverá constar na matriz de compatibilidade dos equipamentos listados neste grupo.

1.10.1.7. Deve possuir garantia total do fabricante por um período de pelo menos 12 (doze) meses.

1.11. **Grupo 1 – Item 10 – Cordão Óptico Duplex, 10G Multimodo (LC/LC) - 10 metros**

1.11.1. Características Gerais

1.11.1.1. Deve ser fabricado com fibras multimodo OM3 de 850nm;

1.11.1.2. Deve possuir velocidade de operação de 10 Gigabit Ethernet;

1.11.1.3. Deve possuir comprimento mínimo de 10 (dez) metros;

1.11.1.4. Deve possuir conector do LC duplex em ambas pontas;

1.12. **Grupo 1 – Item 11 – Cabo de Conexão Direta 100G - 10 metros**

1.12.1. Características Gerais

1.12.1.1. Deve implementar tecnologia Active Optical Cable (AOC);

1.12.1.2. Deve conter transceivers 100Gbps QSFP28 integrados em ambas as pontas;

1.12.1.3. Deve permitir a instalação em slots/portas tipo QSFP28;

1.12.1.4. Deve ser do tipo hot-swappable, permitindo sua conexão/desconexão com o equipamento em operação;

1.12.1.5. Deve possuir comprimento mínimo de 10 (dez) metros;

1.12.1.6. Deve ser do mesmo fabricante e deverá constar na matriz de compatibilidade dos equipamentos listados neste grupo.

1.12.1.7. Deve possuir garantia total do fabricante por um período de pelo menos 12 (doze) meses.

1.13. **Grupo 1 – Item 12 – Cabo de Conexão Direta 40G - 10 metros**

1.13.1. Características Gerais

1.13.1.1. Deve implementar tecnologia Active Optical Cable (AOC);

1.13.1.2. Deve conter transceivers 40Gbps QSFP+ integrados em ambas as pontas;

1.13.1.3. Deve permitir a instalação em slots/portas tipo QSFP+;

1.13.1.4. Deve ser do tipo hot-swappable, permitindo sua conexão/desconexão com o equipamento em operação;

1.13.1.5. Deve possuir comprimento mínimo de 10 (dez) metros;

1.13.1.6. Deve ser do mesmo fabricante e deverá constar na matriz de compatibilidade dos equipamentos listados neste grupo.

1.13.1.7. Deve possuir garantia total do fabricante por um período de pelo menos 12 (doze) meses.

1.14. **Grupo 1 – Item 13 - Operação Assistida**

1.14.1. A CONTRATADA deverá prestar Operação Assistida à solução durante 30 dias (úteis), tendo seu início após o Termo de Recebimento Definitivo (TRD) da solução, devendo manter pelo menos 1 (um) técnico dedicado no local (on-site), 08 (oito) horas por dia, 05 (cinco) dias por semana.

1.14.2. A Operação Assistida permite o acompanhamento do funcionamento da solução por técnico certificado da contratada, abrangendo também a execução de serviços não programados ou não esperados no planejamento inicial, necessários para o correto funcionamento da nova estrutura;

1.14.3. Caso surjam situações emergenciais decorrentes de falhas nos equipamentos instalados ou nas configurações implantadas, e que impossibilitem o funcionamento da solução, a CONTRATANTE poderá exigir a presença adicional do técnico aos finais de semana ou fora do horário

comercial;

1.14.4. Durante as semanas contratadas, deverá ser prestado todo o suporte à operação do novo ambiente, minimizando o risco e proporcionando as condições ideais para transferência da tecnologia envolvida em regime de operação conjunta, até que a contratante possa assumir as atividades integralmente;

1.14.5. Deverá ser designado um corpo técnico para a realização dos trabalhos no local da instalação, sendo esperada a realização de testes, análises, medidas e ajustes que assegurem que as operações diárias sejam realizadas em conformidade com os padrões pré-estabelecidos;

1.14.6. O serviço de operação assistida deve incluir:

1.14.6.1. Execução de atividades operacionais, utilizando os procedimentos recomendados a cada rotina;

1.14.6.2. Execução de atividades de manutenção corretiva, utilizando procedimentos que permitam maior eficiência e eficácia na solução de falhas;

1.14.6.3. Execução de atividades de manutenção preventiva, rotinas de testes, análises e medidas, utilizando procedimentos que assegurem mínima interferência na operação e máxima disponibilidade dos produtos;

1.14.6.4. Elaboração de procedimentos especiais ou detalhamento dos procedimentos padrão, caso seja necessário;

1.14.6.5. Elaboração de relatórios de atividades detalhando os procedimentos realizados e eventuais ajustes, se necessário;

1.14.6.6. Apoio para interoperação das funcionalidades implementadas com os equipamentos existentes na rede da CONTRATANTE.

1.14.7. A operação assistida poderá ser realizada de forma concomitante à transferência de conhecimento, desde que alocado técnicos distintos para cada tarefa, e somente após anuência e autorização da CONTRATANTE;

1.15. **Grupo 1 – Instalação e Configuração**

1.15.1. Os serviços de instalação e configuração, necessários para a operacionalização dos switches de Data Center (Spine/Leaf) e Agregação, além dos softwares de Gerenciamento e Controle de Acesso devem ser executados pela CONTRATADA, de acordo com os requisitos abaixo.

1.15.2. A instalação, configuração e suporte dos componentes deverá seguir o cronograma a seguir:

1.15.2.1. Etapa 1 – Preparo e Iniciação do Projeto: Etapa de definição do escopo, abrangência e cronograma do projeto de instalação e configuração.

1.15.2.2. Etapa 2 – Definição de Requisitos da Solução: Etapa de definição e validação dos requisitos técnicos e de negócio da Solução.

1.15.2.3. Etapa 3 – Plano e Arquitetura da Solução: Etapa de planejamento, desenho e concepção da Solução.

1.15.2.4. Etapa 4 – Configuração e Integração da Solução: Etapa de instalação, configuração, integração e testes da Solução instalada.

1.15.2.5. Etapa 5 – Migração: Etapa de planejamento e migração de recursos da infraestrutura existente à nova Solução.

1.15.2.6. Etapa 6 – Operação Assistida: Etapa de acompanhamento da solução implementada.

1.15.2.7. Etapa 7 – Transferência de Conhecimento: Etapa de formalização da transferência do conhecimento, já realizada durante as etapas de instalação.

1.15.2.8. Etapa 8 – Garantia especializada do fabricante: A contratada auxiliará a contratante no entendimento e suporte à operação da Solução instalada em produção e deverá auxiliar a contratante no Gerenciamento de Incidentes junto ao suporte técnico da fabricante da Solução. A contratada deverá também emitir relatórios contendo o status de todos os casos abertos, bem como status de RMAs, progresso na análise de falhas e emissão de relatórios de KPIs de assuntos relacionados ao suporte técnico da fabricante da Solução.

1.15.3. A qualidade dos serviços deve ser assegurada por meio da disponibilização de equipe técnica qualificada e certificada, incluindo pelo menos 1 (um) técnico especialista de cada fabricante da solução ofertada e pelo menos um profissional com conhecimento técnico da topologia completa e dos equipamentos que compõem o grupo I.

1.15.4. Etapa 1 – Preparo e Iniciação do Projeto

1.15.4.1. Durante esta etapa, os gerentes de projeto da contratante e contratada desenvolverão o Plano, com entendimento da abrangência e cronograma do Projeto e conduzirão a reunião de kick-off para apresentar a “equipe de trabalho” e metodologia.

1.15.5. Etapa 2 – Definição de Requisitos da Solução

1.15.5.1. Nessa etapa, a contratante e a contratada definirão e validarão os requisitos técnicos e de negócio da Solução. Um documento listando todos os requerimentos da contratante deverá ser confeccionado pela contratada e deverá ser aprovado pela contratante. Todas as etapas posteriores

possuem dependência desta etapa.

1.15.5.2. A contratada, juntamente com membros designados pela contratante irá:

1.15.5.2.1. Conduzir entrevistas para revisar o atual ambiente da contratante e identificar o ponto de integração entre legado e a nova Solução.

1.15.5.2.2. Identificar todos os requerimentos para o correto funcionamento da Solução.

1.15.6. Etapa 3 – Plano e Arquitetura da Solução

1.15.6.1. Durante esta etapa, a contratada trabalhará em conjunto com a contratante para definir e documentar o plano de arquitetura e desenho da Solução. Como resultado desta etapa, será confeccionado e entregue à contratante um documento de arquitetura do tipo SOW (em tradução livre, escopo de trabalho) que deverá conter o desenho definido e detalhes da configuração que será aplicada durante a etapa de implementação:

1.15.6.1.1. Objetivo dos serviços;

1.15.6.1.2. Plano de gerenciamento de mudanças, detalhando passo-a-passo o escopo da migração;

1.15.6.1.3. Cronograma das atividades que serão realizadas, com os prazos estimados e as diretrizes para cada atividade;

1.15.6.1.4. Projeto lógico de configuração e diagrama de interconexão dos equipamentos;

1.15.6.1.5. Nome(s) do(s) gerente(s) de projetos responsável(is) e do(s) técnico(s) responsável(is) pela execução dos serviços;

1.15.6.1.6. Lista de todos os elementos instalados contendo:

1.15.6.1.7. Nome e endereço IP do equipamento;

1.15.6.1.8. Equipamento e porta na qual o equipamento foi conectado;

1.15.6.1.9. Local de instalação (prédio, andar, sala);

1.15.6.1.10. Número de série do equipamento.

1.15.6.2. O SOW deverá ser entregue pela CONTRATADA em até 30 (trinta) dias úteis após a assinatura do aceite provisório dos equipamentos, o qual deverá ser aprovado pela CONTRATANTE;

1.15.6.3. Os serviços não poderão ser iniciados antes da apresentação e assinatura de concordância de ambas as partes;

1.15.7. Etapa 4 – Configuração e Integração da Solução

1.15.7.1. Durante a etapa 4, a Equipe de Projeto deverá instalar e configurar a Solução ofertada no ambiente da contratante e deverá, se necessário, integrá-la ao ambiente já existente. Nesta fase deverá ser realizado teste dos componentes da Solução, conforme desenho apresentado no documento de arquitetura, entregue na etapa 3.

1.15.7.2. 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;

1.15.7.3. As configurações deverão seguir fielmente a padronização previamente estabelecida pela contratante.

1.15.8. Etapa 5 – Migração

1.15.8.1. A contratada deverá planejar e executar a migração de recursos do ambiente existente para a nova Solução.

1.15.8.2. A substituição da infraestrutura atual 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;

1.15.8.3. 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;

1.15.8.4. Os serviços de migração contemplam ainda a supervisão das instalações individuais dos equipamentos e a execução de um roteiro de testes para verificação da operação dos serviços, além da elaboração de relatórios gerenciais de acompanhamento dos serviços sempre que solicitados pela contratante, e a retirada dos equipamentos da infraestrutura obsoleta, que devem ser rotulados, relacionados, acondicionados em embalagens apropriadas e armazenados em local designado pela contratante;

1.15.8.5. Ao término do serviço deve 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;

1.15.9. Instalação dos itens 1 (Switch Spine), 2 (Switch Leaf – Tipo A), 3 (Switch Leaf – Tipo B) e 4 (Switch Agregação)

1.15.9.1. A instalaçãatilde;o refere-se à instalação física e lógica, no Data Center da contratante, do Switch Spine (Item 1), Switch Leaf – Tipo A (item 2), Switch Leaf – Tipo B (item 3) e Switch Agregação (item 4), respectivamente, abrangendo:

1.15.9.1.1. Sua disposição e conectorização no rack de telecomunicações;

1.15.9.1.2. A instalação dos transceivers em seus módulos/slots;

1.15.9.1.3. Sua interconexão a outros switches, roteadores, firewalls, ADCs e servidores de rede, entre outros;

1.15.9.1.4. Suas configurações de interfaces, endereçamento e serviços de rede, além de outras configurações necessárias ou constantes no Projeto de Instalação;

1.15.9.1.5. Sua identificação e a identificação de todas as suas conexões.

1.15.9.2. A contratada deverá providenciar todos os materiais necessários à instalação física dos equipamentos; a CONTRATANTE será responsável pela disponibilização do(s) rack(s) e fornecimento de pontos elétricos necessários à instalação dos equipamentos; no entanto, todo o cabeamento para interconexão dos equipamentos fornecidos é de responsabilidade da contratada;

1.15.9.3. Os serviços não poderão ser iniciados antes da apresentação e assinatura de concordância de ambas as partes;

1.15.9.4. Ao término do serviço deve 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 módulos instalados/configurados.

1.15.10. Instalação do item 5 (Sistema de Gerenciamento de Equipamentos de Data Center)

1.15.10.1. A instalação refere-se ao Sistema de Gerenciamento de Equipamentos de Data Center, na infraestrutura de virtualização existente no MJSP, e sua configuração lógica, abrangendo:

1.15.10.1.1. Suas configurações de interfaces, endereçamento e serviços de rede, além de outras configurações necessárias ou constantes no Projeto de instalação;

1.15.10.1.2. A inclusão e a configuração de todos os equipamentos do Grupo I e os equipamentos legado em sua base;

1.15.10.1.3. O ajuste dos demais parâmetros de configuração, conforme Projeto de instalação.

1.15.10.2. O Sistema de Gerenciamento será instalado em servidores/equipamentos do parque tecnológico da contratante, sendo desta a responsabilidade pela disponibilização dos recursos necessários à sua instalação;

1.15.10.3. Os serviços não poderão ser iniciados antes da apresentação e assinatura de concordância de ambas as partes;

1.15.10.4. Ao término do serviço deve 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 módulos instalados/configurados.

1.15.11. Instalação do item 6 (Solução de Controle de Acesso)

1.15.11.1. A instalação refere-se a Solução de Controle de Acesso, na infraestrutura de virtualização existente no MJSP, e sua configuração lógica, abrangendo:

1.15.11.1.1. Suas configurações de interfaces, endereçamento e serviços de rede, além de outras configurações necessárias ou constantes no Projeto de instalação;

1.15.11.1.2. Aplicação do todo o licenciamento existente;

1.15.11.1.3. O ajuste dos demais parâmetros de configuração, conforme Projeto de instalação.

1.15.11.2. A Solução de Controle de Acesso será instalada em servidores/equipamentos do parque tecnológico da contratante, sendo desta a responsabilidade pela disponibilização dos recursos necessários à sua instalação;

1.15.11.3. Os serviços não poderão ser iniciados antes da apresentação e assinatura de concordância de ambas as partes;

1.15.11.4. Ao término do serviço deve 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 módulos instalados/configurados.

1.16. **Grupo 1 - Treinamento**

1.16.1. 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;

1.16.2. 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;

1.16.3. A CONTRATADA deverá realizar treinamento para 1 (uma) turma com 5 (cinco) servidores indicados pela CONTRATANTE;

1.16.4. A transferência de conhecimento 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, e poderá ser realizada durante as semanas de Operação Assistida contratadas, desde que alocado técnicos distintos para cada tarefa, e somente após anuência e autorização da CONTRATANTE. A transferência de conhecimento não é parte integrante da carga horária de Operação Assistida contratada.

1.16.5. O treinamento deverá ser realizado em apenas 01 (um) turno, matutino ou vespertino.

1.16.6. O treinamento deverá ter carga horária mínima de 30 (trinta) horas;

1.16.7. A CONTRATADA assumirá todas as despesas e encargos inerentes à transferência de conhecimento, compreendendo as despesas com hospedagem, transporte e alimentação dos técnicos responsáveis pelo repasse e demais despesas/custos indiretos que incidirem sobre esta contratação;

1.16.8. A CONTRATADA deverá fornecer toda a infraestrutura necessária para realização do treinamento;

1.16.9. A solução utilizada para realização do treinamento deverá, no que concerne às configurações e instalação, ser idêntica à solução ofertada no certame licitatório podendo ser diferente apenas em relação à capacidade de processamento, throughput, por se tratar de treinamento;

1.16.9.1. A CONTRATADA poderá utilizar-se da solução instalada para a realização da transferência de conhecimento, garantidas as condições para que não haja interrupção da solução já implementada;

1.16.10. A CONTRATADA deverá fornecer o conteúdo didático utilizado no treinamento na forma impressa para todos os participantes;

1.16.11. A CONTRATADA deverá fornecer uma cópia digital do conteúdo didático utilizado no treinamento que deverá ser entregue para o gestor do contrato;

1.16.12. Durante a transferência de conhecimento deverão ser fornecidos aos técnicos da CONTRATANTE todo material e documentação, preferencialmente em português, necessários à perfeita compreensão da solução instalada (slides, exemplos de implementação, documentação do projeto executado na CONTRATANTE, etc.) bem como alimentação compatível com a quantidade de pessoas envolvidas, quando esta ocorrer fora da dependências das CONTRATANTE;

1.16.13. Ao término da transferência de conhecimento deverá ser realizada uma avaliação da atividade por parte da equipe da CONTRATANTE, que atribuirá as seguintes classificações: A – Mais que Suficiente, B – Suficiente e C – Insuficiente;

1.16.13.1. Caso 50% (cinquenta por cento) ou mais dos técnicos da CONTRATANTE avalie a transferência de conhecimento como insuficiente, a CONTRATADA deverá providenciar, sem ônus, outro período para a transferência de conhecimento.

1.16.14. Caberá à CONTRATADA o controle de participação no treinamento pelos servidores indicados pela CONTRATANTE;

1.16.15. Ao final do treinamento, a CONTRATADA deverá emitir certificado de participação no treinamento para os participantes;

1.16.16. O certificado emitido deverá conter:

1.16.16.1. Nome do participante;

1.16.16.2. Período de realização com dias e horários;

1.16.16.3. Carga horária do treinamento;

1.16.16.4. Percentual de frequência do participante;

1.16.16.5. Nome e assinatura do Instrutor;

1.16.16.6. Nome e assinatura do Representante da CONTRATADA;

1.16.17. O treinamento deverá abranger, no mínimo, os seguintes conteúdos:

1.16.17.1. Instalação e Configuração da Solução;

1.16.17.2. Conceitos e configuração de alta disponibilidade;

1.16.17.3. Melhores práticas;

1.16.17.4. Solução de problemas básicos;

1.16.17.5. Demais conceitos e configurações essenciais ao entendimento e manuseio da solução por parte da CONTRATANTE.

1.17. **Grupo 2 – Especificações Gerais para a Solução de Segurança e Balanceamento de Carga e Segurança (Físico e Virtual)**

1.17.1. Os softwares que compõem a solução de Segurança e Balanceamento de Carga deverão conter, no mínimo:

1.17.1.1. Compatibilidade entre si, sem perda de funcionalidades na ativação de qualquer funcionalidade;

1.17.1.2. Será permitida a participação e oferta de diferentes fabricantes como forma de prover todas as funcionalidades citadas neste Grupo de Termo de Referência.

1.17.1.3. O cluster deve operar tanto no modo ativo/passivo como no modo ativo/ativo;

1.17.1.4. Autenticação em bases remotas por LDAP;

1.17.1.5. Três níveis de usuários de administração da solução: superusuário, usuário com permissões reduzidas e usuário com direito exclusivo a leitura;

1.17.1.6. Opção de armazenamento de registros de sistema (log) na solução ou em servidores externos;

1.17.1.7. Interface gráfica com usuário GUI (Graphic User Interface) acessível via navegador web e em conformidade com os padrões W3C, com acesso e operação por HTTPS por qualquer ponto da rede TCP/IP interna do MJ, que permita operação da solução e transferência de arquivos entre a solução e a máquina onde houve o acesso à GUI de maneira criptografada;

1.17.1.8. Interface de linhas de comandos CLI (Command Line Interface) acessível e operável via SSH por qualquer ponto da rede TCP/IP interna do MJ, que permita operação da solução e transferência de arquivos entre a solução e sistemas externos de maneira criptografada;

1.17.1.9. Interface centralizada de gerência GUI e CLI para toda a solução;

1.17.1.10. Capacidade de reinicialização remota da solução por GUI e/ou CLI;

1.17.1.11. Capacidade de aplicar atualizações preventivas, corretivas e de melhoria através da GUI e/ou CLI;

1.17.1.12. Linguagem de programação ou interface (API) para automatização de atividades e configurações de sistemas, sem custo adicional;

1.17.1.13. Deverá ser disponibilizada documentação das API's dos appliances que compõem a solução;

1.17.1.14. Suporte a SMNPv3;

1.17.1.15. Ser transparente quanto ao uso do protocolo IPv4 e IPv6 para a criação, modificação, remoção ou qualquer interação com equipamentos e servidores, reais ou virtuais;

1.17.1.16. Permitir o redirecionamento de páginas de erros 403, 404 e 50x específicas para páginas definidas pelo administrador;

1.17.2. Os softwares que compõem a solução deverão permitir que a solicitação de autenticação do cliente seja configurada conforme métodos abaixo:

1.17.2.1. Por formulário, verificando as credenciais via LDAP;

1.17.2.2. Por certificado digital, enviando as informações do certificado (ex: CN, DN) à aplicação de destino por header ou cookie específico.

1.17.3. A solução deve ser capaz de limitar o número de sessões estabelecidas com cada servidor real e virtual.

1.17.4. Oferecer proteção contra ataques de negação de serviço – Denial of Service (DoS) e Distributed Denial of Service (DDoS).

1.17.5. Implementar Listas de Controle de Acesso (ACL), utilizando, no mínimo, os parâmetros de endereço IP de origem e destino.

1.17.6. Implementar limpeza de cabeçalho HTTP.

1.17.7. Possuir registro de logs com pelo menos as seguintes características:

1.17.7.1. Em cada registro de log de acesso deve ser inserido um identificador de transação HTTP que deve ser único, envolvendo o par requisição/resposta;

1.17.7.2. Os registros de log de acesso e eventos devem ser armazenados em arquivo ou banco de dados que permita a exportação ou em outro formato aberto CSV ou TXT, podendo ainda serem armazenados localmente ou carregados (upload) em servidor de log via FTP ou SCP ou armazenados em servidor externo de banco de dados;

1.17.7.3. Permitir configurar a retenção dos logs por tempo e ou volume.

1.17.8. Deverá conter a funcionalidade de integrated caching ou similar, que tem por objetivo armazenar as respostas no cache interno para aliviar a carga de consumo de banda dos servidores.

1.17.9. Deverá ter a capacidade de realizar roteamento estático, assim como roteamento dinâmico através de protocolos RIP, OSPF e BGP.

1.17.10. **Funcionalidades de Balanceamento de Carga (Load Balance)**

1.17.10.1. A solução de Load Balance deve ser capaz de balancear servidores com qualquer hardware, sistema operacional e tipo de aplicação.

1.17.10.2. A solução de Load Balance não deve utilizar agentes ou qualquer outro tipo de aplicação instalada nos servidores ou clientes para executar suas funções e gerenciamento.

1.17.10.3. A solução de Load Balance deve possuir, no mínimo, capacidade de resposta aos clientes por roteamento direto (os servidores balanceados respondem diretamente aos clientes), tunelamento (a solução é capaz de utilizar servidores de redes diferentes da que está inserida) ou fullproxy (todas as transações entre clientes e servidores são intermediadas pela solução).

1.17.10.4. A solução de Load Balance deve possuir, no mínimo, capacidade de balancear pelo menos 32 (trinta e dois) servidores virtuais por grupamento (pool) vinculados a um VIP.

1.17.10.5. A solução de Load Balance deve ser capaz de operar com os seguintes algoritmos de balanceamento:

1.17.10.5.1. Fila circular simples (Round Robin – RR);

1.17.10.5.2. Fila circular ponderada (Weighted RR – WRR);

1.17.10.5.3. Menos conexões (Least Connections);

1.17.10.5.4. Servidor com resposta mais rápida;

1.17.10.5.5. Dinâmico, baseado em parâmetros do servidor coletados via SNMP.

1.17.10.6. A solução de Load Balance deve ser capaz de monitorar servidores reais e virtuais pelos seguintes métodos:

1.17.10.6.1. ICMP;

1.17.10.6.2. Portas TCP e UDP;

1.17.10.6.3. Conexões específicas de aplicação HTTP, HTTPS, FTP, RADIUS, SMTP, LDAP (em especial, Microsoft AD), POP3, SIP, SNMP. Caso a solução apresentada não possua algum desses monitores pré-configurados (“built in”), admite-se sua criação customizada durante a fase de instalação.

1.17.10.7. Mesmo com a criação de novas sessões, a solução deve garantir a persistência de sessões existentes entre clientes e servidores:

1.17.10.7.1. por cookie – inserção de um novo cookie na sessão;

1.17.10.7.2. por cookie – utilização do valor do cookie da aplicação, sem adição de cookie;

1.17.10.7.3. por endereço IP destino;

1.17.10.7.4. por endereço IP origem;

1.17.10.7.5. por sessão SSL;

1.17.10.7.6. por análise da URL acessada;

1.17.10.7.7. por análise de qualquer parâmetro no cabeçalho (header) HTTP;

1.17.10.7.8. por análise do SIP Call ID.

1.17.10.8. A Solução deve oferecer funcionalidades de otimização, cache proxy e compressão HTTP, com capacidade de:

1.17.10.8.1. Comprimir conteúdos HTTP (com o intuito de reduzir a quantidade de informações enviadas ao cliente);

1.17.10.8.2. Possibilitar uso de compressão de dados com formato GZIP;

1.17.10.8.3. Suportar a utilização e ajuste manual de quantidade memória RAM como cache proxy de objetos HTTP, para responder às requisições dos clientes sem utilizar recursos dos servidores;

1.17.10.8.4. Permitir a definição de quais tipos de objeto serão armazenados ou não em cache;

1.17.10.8.5. Permitir a reescrita de requisições HTTP baseado no conteúdo da URL, possibilitando o redirecionamento de requisições HTTP para HTTPS;

1.17.10.8.6. Permitir a reescrita de respostas HTTP, possibilitando a inclusão de cabeçalho (header) customizado;

1.17.10.8.7. Suportar multiplexação TCP e Reuso de Sessão para reaproveitamento e uso eficiente de conexões entre a solução de balanceamento de aplicações e os servidores balanceados;

1.17.10.8.8. Utilizar cache em memória RAM para maior velocidade no tempo de resposta;

1.17.10.8.9. Suportar os protocolos HTTP, HTTP/1.1 e, no mínimo, ter no roadmap HTTP/2.0.

1.17.11. **Funcionalidades de Global Server Load Balancing (GSLB):**

1.17.11.1. A solução deverá suportar, no mínimo, as seguintes métricas para política de Global Server Load Balancing (GSLB):

1.17.11.1.1. Number of active Servers under each site;

1.17.11.1.2. Connection Load;

1.17.11.1.3. Geolocalização;

1.17.11.1.4. Health Check;

1.17.11.1.5. Least Response;

1.17.11.1.6. Number of Sessions;

1.17.11.1.7. Round Robin;

1.17.11.1.8. Balanceamento Global.

1.17.11.2. A solução deve possuir proteções contra ataques DNS, no mínimo:

1.17.11.2.1. Inspeção de Protocolo;

1.17.11.2.2. Validação de Protocolo;

1.17.11.2.3. UDP Flood;

1.17.11.2.4. Pacotes mal formados;

1.17.11.2.5. Ataque ICMP.

1.17.11.3. A solução deve ser capaz de realizar balanceamento dos servidores DNS.

1.17.11.4. A solução deve ser capaz de realizar filtragem de pacotes.

1.17.11.5. A solução deve ser capaz de realizar IP Anycast.

1.17.11.6. A solução deve ser capaz de realizar DNSSec, independente da estrutura dos servidores DNS em uso.

1.17.11.7. A solução de alta disponibilidade não deve depender de BGP ou outro protocolo de roteamento.

1.17.11.8. A solução de alta disponibilidade será realizada baseada em respostas a requisições DNS. A resposta a requisições DNS devem conter apenas endereços que estejam disponíveis no momento, e balanceadas por request, de acordo com as políticas definidas pelo administrador do GSLB.

1.17.11.9. A solução deverá aceitar resolução de nomes baseada em topologia, onde consultas de DNS são respondidas baseado no país, continente, ou endereço IP de onde veio a requisição.

1.17.11.10. Deve ser possível ajustar quantos endereços são enviados em uma única resposta.

1.17.11.11. Suporte a monitoração de estado de saúde de servidores e serviços, garantindo a disponibilidade do serviço oferecido.

1.17.11.12. Implementar persistência de conexão do usuário entre aplicações ou data centers.

1.17.11.13. A solução deverá permitir que as políticas sejam configuradas individualmente por aplicação sendo balanceada.

1.17.11.14. A solução deve ser capaz de lidar com clientes IPv6 quando o site atende apenas com IPv4 (requests AAAA ou A6).

1.17.12. **Funcionalidades de Aceleração SSL:**

1.17.12.1. A solução deve permitir a encriptação/decriptação de sessões SSL no lugar dos servidores (processo conhecido como SSL Offload);

1.17.12.2. A aceleração SSL/Troca de chaves/criptografia deverá ser feita com aceleração em hardware;

1.17.12.3. Deve possibilitar encriptação até o servidor real;

1.17.12.4. Modo de funcionamento que, se configurado, permite que requisições HTTPS possam ser enviadas diretamente aos servidores por meio de protocolo HTTP aberto;

1.17.12.5. Políticas de controle de acesso e autenticação baseadas nos atributos de certificado;

1.17.12.6. Modo de funcionamento que, se configurado, permite que o ADC recriptografe (em SSL/TLS, utilizando um certificado interno privado diferente do certificado válido) as requisições do cliente para o servidor real, antes destas serem para ele enviadas. Deve ser possível configurar um algoritmo e tamanho de chave distinto do utilizado no estabelecimento do túnel criptografado entre o cliente e o ADC;

1.17.12.7. Permitir ações caso o certificado original do servidor não seja confiável ou esteja expirado;

1.17.12.8. Permitir verificação, se configurada, da validade do certificado digital apresentado;

1.17.12.9. Pelo cliente através de Listas de Certificados Revogados LCR (CRL) ou através de listas ou OCSP (Online Certificate Status Protocol);

1.17.12.10. A solução deve usar sempre o último arquivo LCR para a consulta de Lista de Certificados Revogados;

1.17.12.11. A solução deve implementar o algoritmo de hash SHA1;

1.17.12.12. A solução deve implementar os protocolos SSL 3.0 e TLS 1.2.

1.17.12.13. Manter e gerenciar todo o tráfego criptografado com protocolo SSL versão 3.0, TLS versão 1.1 e 1.2.

1.17.12.14. Implementar renegociação de sessão.

1.17.12.15. Possuir os seguintes algoritmos de encriptação: 3DES, RSA, AES-128 e AES-256, ECCDHE (P-256, P-384 e P-521) e algoritmo de autenticação ECDSA.

1.17.12.16. Permitir geração de chaves RSA, enrollment de certificado, importação e exportação

1.17.12.17. de chaves, certificados de servidores, e checagem de LCR (Lista de Certificados Revogados).

1.17.13. **Funcionalidades de Firewall de Aplicação:**

1.17.13.1. A solução de Web Application Firewall (WAF) deve ser independente de softwares proprietários (agentes) para a execução de quaisquer funções especificadas, bem como operar em alta disponibilidade independente de qualquer protocolo de roteamento.

1.17.13.2. A solução WAF deve, no mínimo, permitir a criação de novas regras com parâmetros e expressões regulares definidos pelo administrador.

1.17.13.3. A solução WAF deve, no mínimo, permitir a criação de políticas diferenciadas por aplicação.

1.17.13.4. A solução WAF deve, no mínimo, permitir configurar de forma granular, por aplicação protegida, restrições de métodos HTTP permitidos, tipos ou versões de protocolos, tipos de caracteres e versões utilizadas de cookies.

1.17.13.5. A solução WAF deve, no mínimo, permitir a detecção e bloqueio de ataques a aplicações Web dos tipos abaixo:

1.17.13.5.1. SQL, Cookie e Command Injection;

1.17.13.5.2. Cross-Site Scripting (XSS);

1.17.13.5.3. Cross-Site Request Forgery;

1.17.13.5.4. Violações do protocolo HTTP;

1.17.13.5.5. Code Injection;

1.17.13.5.6. Ameaças Web AJAX/JSON;

1.17.13.5.7. Buffer Overflow;

1.17.13.5.8. Cookie poisoning;

1.17.13.5.9. Manipulação de campos escondidos e manipulação de cookies;

1.17.13.5.10. Sequestro de sessão;

1.17.13.5.11. XML/DoS;

1.17.13.5.12. Checagem de cabeçalho do “user-agent” para identificar clientes inválidos.

1.17.13.6. A solução WAF deve, no mínimo, permitir a detecção e bloqueio da resposta de determinada aplicação Web nos casos abaixo:

1.17.13.6.1. Ausência de tratamento de erros pela aplicação;

1.17.13.6.2. Vazamento de informações de infraestrutura.

1.17.13.7. A solução WAF deve, no mínimo, permitir a customização da resposta de bloqueio.

1.17.13.8. A solução WAF deve, no mínimo, permitir o bloqueio de métodos HTTP a critério do usuário.

1.17.13.9. A solução WAF deve, no mínimo, permitir o bloqueio de ataques no modo blacklisting e whitelisting.

1.17.13.10. A solução WAF deve, no mínimo, permitir a liberação temporária ou definitiva (whitelist) de endereços IP bloqueados por terem originados ataques detectados pela solução.

1.17.13.11. A solução WAF deve, no mínimo, possuir funcionalidade de aprendizagem automática do funcionamento de uma aplicação web, suas URLs, parâmetros, dentre outras, para a configuração do bloqueio.

1.17.13.12. A solução WAF deve, no mínimo, permitir a customização, pelo administrador, dos parâmetros aprendidos, de forma a criar regras baseadas no tamanho do parâmetro, tipo de conteúdo, e expressões regulares.

1.17.13.13. A solução WAF deve, no mínimo, possuir funcionalidade de criação automática de políticas ou modo de aprendizagem, onde a política de segurança é criada e atualizada automaticamente ou no modo de aprendizagem baseando-se no tráfego real observado à aplicação ou através de aprovação de regras pelo administrador.

1.17.13.14. Deverá ser possível desabilitar algumas assinaturas específicas ou regras em determinados parâmetros, como uma exceção à regra geral.

1.17.13.15. A solução WAF deve, no mínimo, funcionar como proxy reverso de aplicações.

1.17.13.16. A solução WAF deve, no mínimo, permitir o mapeamento de diversas aplicações em um

mesmo IP virtual, enviando informações para conjuntos de servidores diferentes de acordo com a URL requisitada.

1.17.13.17. A solução WAF deve, no mínimo, permitir o mapeamento em um mesmo IP virtual, de acordo com a URL requisitada, que exija certificado digital de cliente para algumas aplicações e não exija para outras.

1.17.13.18. A solução WAF deve, no mínimo, permitir a configuração do modo para somente de detecção ou bloqueio, globalmente ou por cada regra.

1.17.13.19. A solução WAF deve, no mínimo, permitir a aplicação de novas regras sem interromper as conexões já abertas.

1.17.13.20. A solução WAF deve, no mínimo, permitir a inclusão do IP do cliente no campo X-Forwarded-For.

1.17.13.21. A solução WAF deve, no mínimo, permitir a inclusão de parâmetros

1.17.13.22. customizados nos cabeçalhos (headers) HTTP, além da alteração dos existentes, para envio à aplicação de destino.

1.17.13.23. A solução WAF deve, no mínimo, ter suporte a SNI (Server Name Indication).

1.17.13.24. A solução WAF deve, no mínimo, permitir no mínimo 32 servidores virtuais por grupamento (pool) vinculados a cada endereço IP virtual (VIP).

1.17.13.25. A solução WAF deve, no mínimo, permitir a utilização de uma página HTML informativa e personalizável como HTTP Response aos bloqueios.

1.17.13.26. A solução WAF deve, no mínimo, implementar proteção ao JSON (JavaScript Object Notation).

1.17.13.27. A solução WAF deve, no mínimo, permitir a geração de relatórios customizados do módulo de Web Application Firewall, disponibilizando no mínimo os relatórios abaixo:

1.17.13.27.1. Top Ataques (geral ou por aplicação/servidor);

1.17.13.27.2. Top IPs de origem dos ataques;

1.17.13.27.3. Violações;

1.17.13.27.4. Países;

1.17.13.27.5. Severidade;

1.17.13.27.6. Tipos de Ataques;

1.17.13.27.7. Estatística de Tráfego;

1.17.13.27.8. URL e endereços IPs.

1.17.13.28. A solução WAF deve, no mínimo, permitir o agendamento e envio por e-mail dos relatórios, essa funcionalidade pode ser executada no equipamento ou pelo software de gerência.

1.17.13.29. A solução WAF deve, no mínimo, permitir exportar os relatórios nos formatos HTML ou PDF.

1.17.13.30. Deve suportar proteção a aplicação Web contra robôs sofisticados através da combinação de desafios enviados ao browser do usuário e técnicas avançadas de análise comportamental.

1.17.13.31. A solução deve suportar criptografia de dados e credenciais na camada de aplicação.

1.17.13.32. Essas informações devem ser criptografadas para proteger o login e as credenciais dos usuários e com isso os dados da aplicação.

1.17.13.33. Deve possuir uma proteção proativa contra ataques automatizados por robôs e outras ferramentas de ataque.

1.17.13.34. Deve suportar a criptografia de sessões HTTP desde o browser do usuário, provendo proteção contra interceptação por terceiros e evitando ataques do tipo Man in the Browser e Keyloggers.

1.17.13.35. Deve ser possível proteger esses dados criptografados de malwares.

1.17.13.36. Através da análise contínua de carga e monitoração de saúde de servidores, deve ser possível identificar anomalias e mitigá-las.

1.17.14. **Funcionalidades de Controle de Acesso às Aplicações:**

1.17.14.1. Deverá ser capaz de solicitar as credenciais do usuário somente uma vez, e autenticar o usuário em todos os portais que requeiram autenticação;

1.17.14.2. Deve ser capaz de realizar Single Sign On utilizando KERBEROS;

1.17.14.3. O equipamento deverá ser capaz de fazer cache das credenciais do usuário e utilizar a credencial correta para cada sistema;

1.17.14.4. O equipamento deverá ser capaz de implementar SSO.

1.17.14.5. Deverá implementar suporte a validação da estação do usuário para, no mínimo, os seguintes recursos:

1.17.14.5.1. Versão do Sistema Operacional;

1.17.14.5.2. Firewall ativado;

1.17.14.5.3. Antivírus instalado;

1.17.14.5.4. Antivírus atualizado;

1.17.14.5.5. Processos em execução;

1.17.14.5.6. Certificados digitais instalados na máquina.

1.17.14.6. Deverá ser possível configurar uma ação dependendo da validação da estação do usuário;

1.17.14.7. A configuração das dessas ações deverá suportar através de interface gráfica.

1.17.14.8. Deve suportar autenticação de múltiplos fatores utilizando tokens de Hardware;

1.17.14.9. Deverá ser capaz de autenticar usuários em bases de dados LDAP, RADIUS, TACACS+, ou Active Directory;

1.17.14.10. Deve possuir o modo onde o usuário estabelece túnel somente para o tráfego da aplicação, não sendo permitido outro tipo de tráfego dentro do mesmo túnel;

1.17.14.11. Deve possuir modo onde o equipamento se comporta como proxy reverso, buscando o conteúdo Web dos portais internos e apresentando-os como links seguros no portal do usuário;

1.17.14.12. Deve possuir o modo onde um usuário se conecta efetivamente à rede interna;

1.17.14.13. Deve possuir suporte a split tunneling;

1.17.14.14. Deve possuir Suporte à compressão HTTP;

1.17.14.15. Deve permitir estabelecimento de conexão segura de acesso remoto (via protocolo TLS), criando conexão segura desde o browser, sem a necessidade de instalação de um software cliente na máquina do usuário.

1.17.14.16. Deve permitir a utilização do protocolo padrão HTTPS com SSL como transporte, possibilitando a sua utilização com proxy HTTP e possibilitar utilização de encapsulamento DTLS (Datagram TLS);

1.17.14.17. Deve possibilidade de compressão de dados antes de sua criptografia;

1.17.14.18. Deve possibilitar a customização da interface gráfica da página de Login e mensagens de apresentação ao usuário;

1.17.14.19. Deve oferecer acesso remoto seguro à rede inteira para qualquer aplicação baseada em IP (TCP ou UDP);

1.17.15. **Funcionalidades de Anti-DDoS (L4-L7)**

1.17.15.1. Deve suportar as funcionalidades de segurança para proteção DDoS:

1.17.15.2. Deve suportar proteção contra todos os tipos de ataques Denial of Service (DoS e DDoS);

1.17.15.3. A solução deve proteger de ataques DDoS que utilizem SSL;

1.17.15.4. Deve aprender automaticamente o comportamento da aplicação e combinar o comportamento heurístico do tráfego com o stress do servidor de aplicação para determinar uma condição de DDoS.

1.17.15.5. Ao detectar uma condição de DDoS, assinaturas dinâmicas devem ser automaticamente criadas e implementadas em tempo real para proteção da aplicação.

1.17.15.6. Deve permitir proteção contra ataques DDoS, através da análise de comportamento de tráfego usando técnicas de análise de dados e Machine Learning.

1.17.15.7. Deve permitir proteger contra ataques de DNS DDoS utilizando mecanismo que bloqueie somente as requisições maliciosas e permita requisições legítimas aos domínios existentes.

1.17.15.8. Deve suportar Network Address Translation (NAT);

1.17.15.9. Deve limitar o número de conexões;

1.17.15.10. Deve suportar Listas de Controle de Acesso (ACL);

1.17.15.11. Deve permitir o log de ataques do tipo DoS;

1.17.15.12. A solução deve possuir ferramenta flexível baseado em linguagem de programação open-source para customizar e aumentar o nível de segurança contra ataques DDoS, incluindo a possibilidade de interação com base de reputação de endereços IP e estatísticas de tráfego.

1.17.15.13. A solução deve suportar relatórios com a detecção e mitigação dos ataques, incluindo a consolidação através de relatórios analíticos de DDoS.

1.17.15.14. Deve possuir suporte ao envio de SNMP traps para cada ataque DDoS detectado.

1.17.15.15. A solução deve possuir uma ferramenta de teste de pacotes, através da qual deve ser possível realizar testes de pacotes com atributos específicos através da solução anti-DoS.

1.17.16. **Funcionalidades de Visibilidade SSL:**

1.17.16.1. Todo tráfego SSL deverá ser decriptografado pela solução para ser inspecionado nas soluções de segurança já existentes no parque tecnológico do MJ.

1.17.16.2. Os softwares que compõem a solução deverão ser capazes de realizar a terminação de sessões SSL, instalar e manter certificados digitais, de criptografar e recriptografar tráfego em SSL, tanto para o uso em ambientes sem criptografia quanto totalmente criptografados, sem que haja queda ou comprometimento das outras funções exigidas neste documento. Considerando que a solução entregue permitirá a virtualização e a separação de funções, será aceito a divisão da caixa para atender as funcionalidades mínimas previstas.

1.17.16.3. Deve permitir alertas e dar a opção de ações caso o certificado esteja expirado.

1.17.16.4. Deve permitir que múltiplos equipamentos de segurança de diversos fabricantes tenham visibilidade tanto do tráfego de saída quanto de entrada, fazendo com que eles continuem realizando suas inspeções e procurando por malwares e exfiltração de dados.

1.17.16.5. Deve permitir o envio tráfego para dispositivos passivos, como DLPs.

1.17.16.6. Permitir configurar o equipamento para cifrar e decifrar em SSL/TLS a requisição ao enviar para o servidor, permitindo as demais otimizações em ambiente 100% criptografado.

1.17.16.7. Permitir configurar o equipamento para recriptografar em SSL a requisição ao enviar para o servidor, permitindo as demais otimizações em ambiente 100% criptografado.

1.17.16.8. Deve realizar descriptografia de SSL/TLS independente da porta TCP.

1.17.16.9. Deve permitir trabalhar com direcionamento de tráfego inteligente e dinâmico baseado em políticas de contexto, permitindo o gerenciamento de fluxo inteligente entre os dispositivos de segurança e garantindo a disponibilidade de acesso. Não será aceita solução que implemente a "ligação em cascata" dos dispositivos de segurança, em que o tráfego precisa necessariamente passar por todos os dispositivos de segurança sempre.

1.17.16.10. Deve possibilitar a monitoração e gerenciamento independente de cada dispositivo da cadeia de inspeção. Deve possuir um mecanismo de classificação contextual do tráfego que será enviado para cada dispositivo.

1.17.16.11. Deve permitir a resiliência dos serviços dentro da zona de inspeção, inclusive fazendo o balanceamento de carga entre múltiplos equipamentos do mesmo serviço.

1.17.16.12. O tráfego para essa zona de inspeção deve ser gerenciado de forma dinâmica pela solução de visibilidade SSL/TLS, ou seja, de acordo com a classificação do tráfego, o mesmo deve ser enviado para dispositivos específicos da cadeia de inspeção.

1.17.16.13. Deve ser possível ainda reduzir a latência de inspeção SSL atual que é realizada em diversos equipamentos de segurança, centralizando essa operação de criptografia/decriptografia num dispositivo único.

1.17.16.14. Deve suportar redundância ativo/standby com sincronismo dos estados das conexões dos usuários assim como suas características de atribuição de servidores.

1.17.16.15. Ser capaz de manter e gerenciar todo o tráfego criptografado com protocolo SSL versão 3.0, TLS versão 1.1 e 1.2.

1.17.16.16. Deve suportar pelo menos as seguintes cifras e protocolos: TLS1/1.1/1.2, SHA, SHA2, AES-GCM, AES;

1.17.16.17. Deve implementar geração de chaves RSA, enrollment de certificado, importação e exportação de chaves, certificados de servidores.

1.17.16.18. A solução deve terminar as conexões SSL com a finalidade de inspecioná-las.

1.17.16.19. A solução deve proteger de ataques de negação de serviço que utilizem SSL.

1.17.16.20. Deve ser possível descobrir ameaças ocultas no SSL/TLS e prevenir ataques em vários estágios, usando as soluções de segurança já existentes assim como novas soluções que venham a ser adquiridas futuramente, independente de marca/modelo.

1.17.16.21. Deve ter capacidade de gerenciar o tráfego SSL do lado do cliente para o servidor, ou seja, deve ser capaz de decifrar todo o tráfego de entrada.

1.17.16.22. Deve suportar modo Proxy explícito.

1.17.16.23. Deve suportar modo Proxy transparente.

1.17.16.24. Deve suportar monitoração cada dispositivo de segurança independentemente, permitindo realizar o by-pass em caso de falha.

1.17.16.25. Deve permitir a escalabilidade independente de cada dispositivo de segurança.

1.17.16.26. Deve suportar o envio de tráfego para dispositivos em linha camada 2 ou 3, conectando-se diretamente ao dispositivo que realizará a análise/inspeção através de um switch, desacoplando o dispositivo de segurança da interface física, porta ou VLAN.

1.17.16.27. Deve suportar o envio de tráfego ICAP para dispositivos.

1.17.16.28. Deve suportar ECDHE, RSA e DHE com suporte a Forward Secrecy.

1.17.16.29. Deve suportar SSL Forward Secrecy como uma forma de melhorar a segurança nas transações SSL/TLS.

1.17.16.30. Deve ser capaz de criar múltiplos Service Chains.

1.17.16.31. Deve suportar a renegociação de sessão;

1.17.16.32. Deve suportar mecanismos para criar usuários com no mínimo três conjuntos distintos de privilégios, sendo um deles somente leitura das configurações, para acesso às funções de gerenciamento dos equipamentos, via protocolos SSH, SNMP ou HTTPS.

1.17.16.33. Deve possibilitar a coleta de dados de gerenciamento dos equipamentos utilizando os protocolos SNMPv2c e SNMPv3.

1.17.16.34. Deve suportar MIB SNMP.

1.17.16.35. Deve permitir a configuração de endereços IPs para o envio de traps SNMP (alarmes).

1.17.16.36. Deve possibilitar a monitoração e gerenciamento independente de cada dispositivo da cadeia de inspeção. Deve possuir um mecanismo de classificação contextual do tráfego que será enviado para cada dispositivo.

1.17.16.37. A solução deve fazer a monitoração dos serviços dentro da camada de inspeção

1.17.16.38. A solução deve permitir a resiliência dos serviços dentro da zona de inspeção, inclusive fazendo o balanceamento de carga entre múltiplos equipamentos do mesmo serviço.

1.17.16.39. Deve permitir escalar os dispositivos de segurança com alta disponibilidade, usando testes de monitoração de saúde para identificar o estado de cada equipamento de segurança.

1.17.16.40. Com a solução, deve ser possível prevenir ameaças de entrada (Datacenter) e de saída (usuários), incluindo ataques de exploração, retorno de chamada e extração de dados.

1.17.17. **Funcionalidades de Análise Inteligente de Ameaças:**

1.17.17.1. A solução deve possuir lista dinâmica de endereços IP globais com atividades maliciosas;

1.17.17.2. Deve ser possível verificar o endereço de origem do pacote IP no cabeçalho IP e no parâmetro *X-forwarded-for* (XFF)

1.17.17.3. Deve possuir, pelo menos, as seguintes categorias de endereços IP: *Windows Exploits, Web Attacks, Botnets, Scanners, Denial of Service, Reputation, Phishing Proxy, Anonymous Proxy;*

1.17.18. **Funcionalidade de Gerenciamento**

1.17.18.1. A Solução de Segurança e Balanceamento de Carga deve incluir o possibilitar gerenciamento tanto para hardware físico quanto para a solução virtualizada.

1.17.18.2. Possuir funcionalidade de emissão de relatório gerencial/estatístico dos acessos em ferramenta local ou remota, além do syslog ou log interno, que contenham, no mínimo:

1.17.18.2.1. Quantidade de acessos por VIP;

1.17.18.2.2. Quantidade de acessos por serviços e servidores;

1.17.18.2.3. Disponibilidade dos serviços/VIP;

1.17.18.2.4. Quantidade de usuários conectados;

1.17.18.2.5. Quantidade de requisições por período;

1.17.18.2.6. Transações por segundo;

1.17.18.2.7. Tempo de latência do cliente e servidor;

1.17.18.2.8. Throughput de requisição e resposta;

1.17.18.2.9. Quantidade de sessões;

1.17.18.2.10. Retenção de logs para análise posterior;

1.17.18.2.11. Possuir MIB SNMP.

1.17.18.3. Ser capaz de analisar a performance de aplicações web.

1.17.18.4. Gerar informações para permitir análises históricas e auxiliar nos processos de manutenções preventivas, troubleshooting, planejamento de capacidade e análise da experiência dos usuários finais no acesso às aplicações.

1.17.18.5. As informações coletadas deverão permitir a análise dos dados por aplicações, por URL's, por clientes e por servidores, permitindo, assim, a identificação mais precisa dos eventuais ofensores do tráfego suportado pela solução.

1.17.18.6. A solução deverá gerar informações estatísticas de acesso identificando para cada aplicação os métodos de acesso HTTP (GET e Post), o tipo de sistema operacional utilizado pelos clientes, e os browsers utilizados. Caso a solução não possua este recurso nativamente poderá ser aceito solução de terceiros para atendimento da especificação.

1.17.18.7. A geração de informações históricas deverá permitir o detalhamento do tempo de resposta total de carregamento de uma URL/página.

1.17.18.8. Deverá ser disponibilizada documentação das API dos appliances que compõem a solução;

1.17.19. **Funcionalidades de Gerenciamento Centralizado:**

1.17.19.1. As funcionalidades de gerenciamento centralizado deverão ser providas através de um software instalado em ambiente compatível com solução de virtualização VMWare ESXi na versão 5.5 ou superior, a ser disponibilizado pela CONTRATANTE;

1.17.19.1.1. Não poderá haver ônus adicionais à contratante para o pleno funcionamento do software sob qualquer das formas de virtualização do item anterior;

1.17.19.2. A solução deve ser capaz de gerenciar *appliances* físicos, virtuais e ambientes de cloud.

1.17.19.3. A solução deve simplificar o gerenciamento, garantir a conformidade e entregar as ferramentas necessárias para entregar, otimizar e garantir a segurança das aplicações de forma eficiente.

1.17.19.4. Deve gerenciar centralmente licenças, políticas, certificados SSL, imagens de software e configurações dos *appliances* gerenciados (físicos e virtuais).

1.17.19.5. Deve ser capaz de gerenciar soluções de Entrega de aplicações com funcionalidades de segurança L3-L7.

1.17.19.6. Deve gerenciar os seguintes serviços de aplicações: balanceamento de carga, GSLB, Terminação SSL, WAF, Controle de Acesso às Aplicações, Anti-DDoS e Visibilidade SSL.

1.17.19.7. Deve possuir gerenciamento de licenças centralizado.

1.17.19.8. Deve possuir relatórios centralizados.

1.17.19.9. A solução de gerenciamento centralizado deve gerar alertas com relação a disponibilidade, segurança e performance das aplicações.

1.17.19.10. Deve auxiliar no processo de *troubleshooting* de aplicações através de *dashboards* e possibilidade de *drill-down* para filtrar e isolar o problema.

1.17.19.11. A solução deve simplificar o trabalho entre diferentes equipes: Infraestrutura (redes), Apps (Dev) e segurança.

1.17.19.12. Deve ter a capacidade de criar e gerenciar usuários e funções, para poder conceder acesso diferenciado aos diferentes membros da organização.

1.17.19.13. Deve permitir a configuração, backup e restauração: gerenciamento centralizado das configurações do equipamento, planejar os backups e executar as restaurações de forma centralizada.

1.17.19.14. Deve prover também a possibilidade de gerenciar instâncias virtuais dedicadas por aplicação, ou seja, cada aplicação usando uma instância específica para o gerenciamento de tráfego e segurança, sem afetar outras aplicações durante crises ou tarefas de manutenção.

1.17.19.15. Cada instância virtual deverá ser administrada através da gerência centralizada somente por pessoas autorizadas a mexerem com a aplicação em questão.

1.17.19.16. A solução de gerência centralizada deve funcionar tanto em ambientes de *cloud* públicas quanto privadas.

1.17.19.17. Deve permitir monitorar a saúde, performance e segurança das aplicações através de dashboards intuitivos.

1.17.19.18. A solução de gerência centralizada deve garantir consistência de rede e políticas de segurança, não importando onde a aplicação residir (nuvem ou *datacenter*).

1.17.19.19. A solução deve possuir controle de acesso granular, permitindo de times de aplicação e segurança possam gerenciar suas próprias aplicações sem depender do time de redes.

1.17.19.20. Deve possuir perfis de acesso pré-definidos na ferramenta e a possibilidade de criar perfis de acesso customizados para gerenciar quem terá permissão de leitura, escrita e *deploy* de políticas com acesso ao *dashboard* das aplicações.

1.17.19.21. Esses perfis podem ser associados a usuário e grupos na base local ou remoto (RADIUS, LDAP).

1.17.19.22. A solução de gerência centralizada deve analisar a performance, saúde e segurança dos serviços de aplicações existentes no ambiente da CONTRATANTE;

1.17.19.23. Através dos *Dashboards* deve ser possível monitorar a saúde e performance das aplicações de acordo com o nível de acesso de cada usuário. Portanto a equipe responsável pela aplicação "A" poderá visualizar somente o *Dashboard* dessa aplicação.

1.17.19.24. Para a equipe de segurança deve ser possível:

1.17.19.24.1. Gerenciar políticas de segurança através de vários dispositivos gerenciados virtuais ou físicos;

1.17.19.24.2. Ver e comparar políticas;

1.17.19.24.3. Enviar modificações de políticas para vários dispositivos de acordo com a necessidade;

1.17.19.24.4. Gerar relatórios de segurança por dispositivo ou grupo de dispositivos sendo gerenciados;

1.17.19.24.5. Correlacionar eventos de segurança entre os dispositivos sendo gerenciados;

1.17.19.24.6. Visualizar *Dashboards*;

1.17.19.24.7. Monitorar a efetividade de políticas de segurança;

1.17.19.25. Deve ser possível fazer a implementação e *rollback* de políticas de Balanceamento entre Sites.

1.17.19.26. Deve gerenciar a configuração de políticas nos dispositivos DNS.

1.17.19.27. A solução deve permitir visualizar estatísticas de DNS em tempo real e históricos.

1.17.19.28. Para auxiliar no processo de troubleshooting de aplicações, a solução deve no mínimo prover: Métricas de sessões, throughput, latência e transações por segundo;

1.17.19.29. A ferramenta de gerência centralizada deve ser capaz de gerenciar e possuir analíticos das aplicações (VIPs) através de um *Dashboard*. A licença não deve possuir limitações com relação ao máximo de aplicações suportadas, portanto a solução deve estar licenciada para o máximo de aplicações suportado para cada tipo de appliance (físico ou virtual) sendo gerenciado.

1.17.19.29.1. Deve ser garantida a capacidade de gerenciar e possuir analíticos para, no mínimo, 1.000 (mil) aplicações de toda a solução;

1.17.19.30. Deve prover analíticos detalhados, logging e auditoria dos dispositivos gerenciados e das devidas aplicações.

1.17.19.31. Para não impactar na performance de gerenciamento, a parte de coleta de analítico deve ser realizada em servidores específicos de logs da solução.

1.18. **Grupo 2 – Item 14 – Solução de Segurança e Balanceamento de Carga – Tipo A (Appliance Físico)**

1.18.1. Cada unidade do item em questão é composta por 1 (um) appliance físico que permita a implementação das **Especificações Gerais, de Balanceamento de Carga, Global Server Load Balancing (GSLB), Aceleração SSL, Firewall de Aplicação (WAF), Controle de Acesso às Aplicações, Anti-DDoS (L4-L7), Visibilidade SSL, Gerenciamento e Gerenciamento Centralizado – respectivamente** – devendo ser fornecido com todo o licenciamento necessário para a implementação das referidas funcionalidades.

1.18.2. As licenças para os equipamentos do Tipo A (Appliance Físico) poderão ser do tipo perpétuo ou do tipo subscrição, devendo ter o mesmo tempo de suporte e garantia que o appliance físico, ou seja 60 meses.

1.18.2.1. O licenciamento perpétuo deve funcionar sem limite de tempo e perda de recursos ou funcionalidades.

1.18.2.2. O licenciamento por subscrição, baseado em throughput e/ou número de instâncias, deverá ser entregue com as funcionalidades descritas neste item.

1.18.3. A solução deverá incluir quaisquer equipamentos e/ou componentes necessários ao pleno funcionamento e acomodação física, ambiental e lógica no ambiente do MJ, em conformidade com os padrões estabelecidos pelo fabricante;

1.18.4. A solução deverá prover redundância de fontes de alimentação elétrica e de ventiladores nos appliances físicos;

1.18.5. Incluir cabos e conectores "macho" e "fêmea" necessários à conexão elétrica dos equipamentos;

1.18.6. A solução deverá poder ser configurada sob a forma de um cluster composto por dois appliances físicos e deverá compreender o provimento de upgrades de desempenho e performance;

1.18.7. Os equipamentos pertencentes ao cluster de appliances físicos deverão possuir as seguintes características:

1.18.7.1. Deve possuir, no mínimo, 04 (quatro) portas 40 Gigabit Ethernet compatíveis com transceivers QSFP+;

1.18.7.2. Deve possuir, no mínimo, 8 (oito) portas 10 Gigabit Ethernet adicionais compatíveis com transceivers SFP+;

1.18.7.3. Deve ser possível configurar 02 (duas) das portas 10 Gigabit Ethernet para sincronização de heartbeat;

1.18.7.4. Deve possuir, no mínimo, 02 (duas) portas Ethernet RJ-45 para administração fora de banda (out-of-band management).

1.18.7.5. Deve possuir recursos de agregação de portas baseado no protocolo LACP em seus modos ativo e passivo;

1.18.7.6. Deve possuir memória RAM mínima de 32GB;

1.18.7.7. Deve possuir disco rígido com capacidade de armazenamento interno e retenção de logs para análise;

1.18.8. **Requisitos de desempenho:**

1.18.8.1. Deve suportar, no mínimo, 35Gbps de throughput em camada 7 e 40Gbps em camada 4 do modelo OSI;

1.18.8.2. Deve suportar, no mínimo, 20Gbps de compressão para tráfego HTTP;

1.18.8.3. Deve suportar, no mínimo, 5.000.000 (cinco milhões) requisições HTTP por segundo na camada 4 do modelo OSI;

1.18.8.4. Capacidade de operar, no mínimo, 1.500.000 (um milhão e quinhentas mil) requisições por segundo na camada 7 do modelo OSI;

1.18.8.5. Deve suportar, no mínimo, 600.000 (seiscentas mil) conexões por segundo na camada 4 do modelo OSI;

1.18.8.6. Deve suportar, no mínimo, 33.000.000 (trinta e três milhões) de conexões simultâneas na camada 4 do modelo OSI;

1.18.8.7. Deve suportar, no mínimo, 30.000.000 (trinta milhões) de pacotes SYN/segundo, sob ataque de SYN Flood;

1.18.8.8. Quando licenciado para as capacidades de Visibilidade SSL, através do licenciamento, deve:

1.18.8.8.1. Suportar, no mínimo, 7.8Gbps de throughput para tráfego SSL/TLS com abertura do tráfego criptografado, envio para cadeia de inspeção (aberto) e recriptografia para o destino original;

1.18.8.8.2. Suportar, no mínimo, 10.600 (dez mil e seiscentas) transações SSL por segundo, considerando toda a orquestração do tráfego SSL (abertura, direcionamento e recriptografia de tráfego);

1.18.8.8.3. Processar, no mínimo, 600.000 (seiscentas mil) sessões concorrentes SSL, considerando toda a orquestração do tráfego SSL (abertura, direcionamento e recriptografia de tráfego);

1.18.9. **Funcionalidades de Virtualização:**

1.18.9.1. Ter capacidade de executar a virtualização de serviços pela criação de diferentes balanceadores e/ou WAFs virtuais independentes (instâncias), permitindo definir níveis de garantia de recursos para as instâncias, sem cobrança adicional por licenças.

1.18.9.2. Todas as instâncias deverão estar licenciadas para o uso de todas as funcionalidades e características descritas:

1.18.9.2.1. Deve permitir a exclusão de uma instância sem interferir nas demais;

1.18.9.2.2. Não causar indisponibilidade dos serviços das outras instâncias;

1.18.9.2.3. A virtualização das instâncias deve ser do tipo “Full Virtualization”, ou seja, cada instância deverá permitir um sistema operacional diferente e completamente independente das demais instâncias;

1.18.9.2.4. A definição de cada instância será feita com base na alocação de recursos de hardware;

1.18.9.2.5. Implementar capacidade de criação e estar licenciado para, no mínimo, 8 (oito) instâncias virtuais totalmente isoladas entre si.

1.19. **Grupo 2 – Item 15 – Transceiver 10Gbps Multimodo**

1.19.1. Características Gerais

1.19.1.1. Deve implementar o padrão 10GBase-SR, operando sobre fibras multimodo OM3/OM4 para distâncias de até 300m/400m, respectivamente;

1.19.1.2. Deve ser compatível com fibras de 850nm;

1.19.1.3. Deve permitir a instalação em slots/portas tipo SFP+;

1.19.1.4. Deve possuir velocidade de operação de 10 Gigabit Ethernet;

1.19.1.5. Deve ser do tipo hot-swappable, permitindo sua conexão/desconexão com o equipamento em operação;

1.19.1.6. Deve possuir conector do tipo LC duplex;

1.19.1.7. Deve ser do mesmo fabricante e deverá constar na matriz de compatibilidade dos equipamentos listados neste grupo.

1.19.1.8. Deve possuir garantia total do fabricante por um período de pelo menos 12 (doze) meses.

1.20. **Grupo 2 – Item 16 – Solução de Segurança e Balanceamento de Carga – Tipo B (Ambiente Virtual)**

1.20.1. O item em questão permita que se instale em ambiente virtualizado da CONTRATANTE, instâncias de Solução de Segurança e Balanceamento de Carga com suporte as funcionalidades descritas anteriormente, devendo ser fornecido com o licenciamento necessário para a implementação das **Funcionalidades de Balanceamento de Carga, Global Server Load Balancing (GSLB), Aceleração SSL, Firewall de Aplicação (WAF), Controle de Acesso às Aplicações, Anti-DDoS (L4-L7), Funcionalidades de Análise Inteligente de Ameaças, Gerenciamento e Gerenciamento Centralizado – respectivamente.**

1.20.2. Todas as funções configuradas serão utilizadas considerando o throughput contratado.

1.20.3. Deve ser baseado em um serviço de subscrição, com direito de uso pelo período de 36 (trinta e seis meses) a contar da assinatura do contrato, tendo como volume máximo contratado de 20 (vinte) Gbps.

1.20.4. Requisitos de desempenho:

1.20.4.1. Deve estar licenciada para 20Gbps de throughput tanto para camada 4 quanto para camada 7 do modelo OSI. Esse tráfego total poderá ser instanciado no formato de soluções virtuais.

1.20.4.2. A CONTRATANTE utilizará soluções virtuais disponibilizadas no catálogo do fabricante ofertado com valores de throughput de 1Gbps (mínimo) à 10Gbps (máximo), totalizando ao final um somatório de todas as soluções virtuais o valor de 20Gbps;

1.20.4.3. Ainda que existam outros tamanhos disponíveis, a CONTRATANTE limitar-se-á a utilização de máquinas virtuais dentro do intervalo contratado (entre 1 e 10Gbps);

1.20.4.4. A CONTRATADA deverá implementar a capacidade de criação e estar licenciado para, no mínimo, 8 (oito) instâncias:

1.20.4.4.1. 2 (duas) instâncias gerais para o CICCN-DF;

1.20.4.4.2. 2 (duas) para utilização dos serviços em nuvem;

1.20.4.4.3. 2 (duas) para configuração de borda Global Server Load Balancing (GSLB)

1.20.4.4.4. 2 (duas) para utilização do Firewall de Aplicação (WAF)

1.20.4.5. Esse quantitativo poderá sofrer alterações caso a CONTRATANTE pretenda realocar um número maior/menor em cada um destes serviços ou, ainda, decida incluir serviços não citados no item anterior, durante a vigência do contrato.

1.20.4.6. A CONTRATADA deverá manter a CONTRATANTE informada sobre quais os tamanhos de máquinas virtuais disponíveis no catálogo do fabricante, de acordo com as funcionalidades desejadas;

1.20.4.7. Suportar, no, mínimo 2,7Gbps de compressão para tráfego HTTP.

1.20.4.8. Capacidade de operar, no mínimo, 210.000 requisições HTTP por segundo tanto para camada 4 quanto camada 7 do modelo OSI.

1.20.4.9. Capacidade de operar, no mínimo, 64.000 e 45.000 conexões por segundo nas camadas 4 e 7 do modelo OSI, respectivamente.

1.20.4.10. Capacidade de operar, no mínimo, 10.000.000 e 2.400.000 de conexões simultâneas nas camadas 4 e 7 do modelo OSI, respectivamente.

1.20.5. Deve estar totalmente licenciado para instalação e funcionamento bem como ser compatível com solução de virtualização VMWare ESXi na versão 5.5 ou superior, a ser disponibilizado pela CONTRATANTE;

1.20.6. Não poderá haver ônus adicionais à contratante para o pleno funcionamento do software sob qualquer das formas de virtualização do item anterior;

1.20.7. As instâncias virtuais poderão existir ou serem revogadas de acordo com a necessidade de negócio da CONTRATANTE.

1.20.8. A solução deve permitir a CONTRATANTE reduzir o tempo da entrega dos serviços de aplicação, através do licenciamento modelo "self-licensing" das soluções virtuais.

1.20.8.1. Através do "self-licensing" deve ser possível iniciar rapidamente as soluções virtuais para o uso de funções de segurança e entrega otimizada de aplicações.

1.20.9. Deve permitir sob demanda, iniciar e desligar novas máquinas virtuais.

1.20.10. As máquinas virtuais poderão ser implementadas em ambientes de cloud (pública e privada), assim como Datacenters locais, para garantir políticas consistentes e operação através de múltiplos ambientes distintos.

1.20.11. Deve permitir fazer a implantação e configuração de serviços do catálogo do fabricante onde e quando for necessário.

1.20.12. A solução deve ajudar a dinamicamente criar e escalar a infraestrutura de acordo com as demandas de negócio.

1.20.13. Permitir fazer a implantação de soluções virtuais com total flexibilidade de opções, lugares e timelines.

1.20.14. Permitir sempre adaptar a capacidade de acordo com os requerimentos do negócio, permitindo fazer a reconfiguração das soluções existentes, remoção de soluções que não estão mais em utilização e a troca por outras soluções do catálogo do fabricante.

1.20.15. Permitir migrar para ambientes de nuvem ou entre diferentes nuvens através da flexibilidade do uso de licenciamento rápido e "self-service".

1.20.16. Permitir o uso das soluções virtuais de acordo com a necessidade e flexibilidade de ambientes ágeis.

1.20.17. De acordo com novas demandas da CONTRATANTE, deve ser possível usar sob demanda soluções do catálogo do fabricante, sem que seja necessário passar por um novo processo de compras.

1.20.18. Deve ser possível integração e automação com soluções de TI de terceiros.

1.20.19. Deve ser possível gerenciar os ativos virtuais através de uma ferramenta de gerência centralizada que deve gerar relatórios mensais de utilização.

1.20.20. Deve ser um modelo flexível e ágil para utilização de serviços de aplicação e segurança para atender as necessidades de negócio da CONTRATANTE, possuindo relatórios mensais com visibilidade sobre o consumo.

1.20.21. Esse modelo deve permitir que a CONTRATANTE instancie e revogue licenças virtuais sob demanda para os diversos catálogos de serviço do FABRICANTE.

1.20.22. O fabricante da solução deve disponibilizar templates de implementações em nuvens.

1.20.23. Deve possuir templates para, no mínimo, AWS (Amazon Web Services), Microsoft Azure, Google Cloud Platform, Red Hat Openstack.

1.20.24. Esses templates devem permitir reduzir os erros humanos e o tempo de implantação da solução.

1.20.25. Deve possuir atualizações de versões e suporte 24x7 do fabricante durante o período de 36 (trinta e seis meses).

1.21. **Grupo 2 – Item 17 – Operação Assistida**

1.21.1. A CONTRATADA deverá prestar Operação Assistida à solução durante 30 dias (úteis), tendo seu início após o Termo de Recebimento Definitivo (TRD) da solução, devendo manter pelo menos 1 (um) técnico dedicado no local (on-site), 08 (oito) horas por dia, 05 (cinco) dias por semana.

1.21.2. A Operação Assistida permite o acompanhamento do funcionamento da solução por técnico certificado da contratada, abrangendo também a execução de serviços não programados ou não esperados no planejamento inicial, necessários para o correto funcionamento da nova estrutura;

1.21.3. Caso surjam situações emergenciais decorrentes de falhas nos equipamentos instalados ou nas configurações implantadas, e que impossibilitem o funcionamento da solução, a CONTRATANTE poderá exigir a presença adicional do técnico aos finais de semana ou fora do horário comercial;

1.21.4. Durante as semanas contratadas, deverá ser prestado todo o suporte à operação do novo ambiente, minimizando o risco e proporcionando as condições ideais para transferência da tecnologia envolvida em regime de operação conjunta, até que a contratante possa assumir as atividades integralmente;

1.21.5. Deverá ser designado um corpo técnico para a realização dos trabalhos no local da instalação, sendo esperada a realização de testes, análises, medidas e ajustes que assegurem que as operações diárias sejam realizadas em conformidade com os padrões pré-estabelecidos;

1.21.6. O serviço de operação assistida deve incluir:

1.21.6.1. Execução de atividades operacionais, utilizando os procedimentos recomendados a cada rotina;

1.21.6.2. Execução de atividades de manutenção corretiva, utilizando procedimentos que permitam maior eficiência e eficácia na solução de falhas;

1.21.6.3. Execução de atividades de manutenção preventiva, rotinas de testes, análises e medidas, utilizando procedimentos que assegurem mínima interferência na operação e máxima disponibilidade dos produtos;

1.21.6.4. Elaboração de procedimentos especiais ou detalhamento dos procedimentos padrão, caso seja necessário;

1.21.6.5. Elaboração de relatórios de atividades detalhando os procedimentos realizados e eventuais ajustes, se necessário;

1.21.6.6. Apoio para interoperação das funcionalidades implementadas com os equipamentos existentes na rede da CONTRATANTE.

1.21.7. A operação assistida poderá ser realizada de forma concomitante à transferência de conhecimento, desde que alocado técnicos distintos para cada tarefa, e somente após anuência e autorização da CONTRATANTE;

1.22. **Grupo 2 – Serviço de Instalação, Configuração e Suporte Especializado**

1.22.1. Os serviços de instalação e configuração, necessários para a operacionalização da Solução de Segurança de Balanceamento de Carga, devem ser executados pela CONTRATADA, de acordo com os requisitos abaixo.

1.22.2. A instalação, configuração e suporte dos componentes deverá seguir o cronograma a seguir:

1.22.2.1. Etapa 1 – Preparo e Iniciação do Projeto: Etapa de definição do escopo, abrangência e cronograma do projeto de instalação e configuração.

1.22.2.2. Etapa 2 – Definição de Requisitos da Solução: Etapa de definição e validação dos requisitos técnicos e de negócio da Solução.

1.22.2.3. Etapa 3 – Plano e Arquitetura da Solução: Etapa de planejamento, desenho e concepção da Solução.

1.22.2.4. Etapa 4 – Configuração e Integração da Solução: Etapa de instalação, configuração, integração e testes da Solução instalada.

1.22.2.5. Etapa 5 – Migração: Etapa de planejamento e migração de recursos da infraestrutura existente à nova Solução.

1.22.2.6. Etapa 6 – Operação Assistida: Etapa de acompanhamento da solução implementada.

1.22.2.7. Etapa 7 – Transferência de Conhecimento: Etapa de formalização da transferência do conhecimento, já realizada durante as etapas de instalação.

1.22.2.8. Etapa 8 – Garantia especializada do fabricante: A contratada auxiliará a contratante no entendimento e suporte à operação da Solução instalada em produção e deverá auxiliar a contratante no Gerenciamento de Incidentes junto ao suporte técnico da fabricante da Solução. A contratada deverá também emitir relatórios contendo o status de todos os casos abertos, bem como status de RMAs, progresso na análise de falhas e emissão de relatórios de KPIs de assuntos relacionados ao suporte técnico da fabricante da Solução.

1.22.2.9. Etapa 9 – Suporte Especializado: Etapa de prestação do serviço de suporte técnico especializado para a solução instalada durante toda a vigência contratual;

1.22.3. A qualidade dos serviços deve ser assegurada por meio da disponibilização de equipe técnica qualificada e certificada, incluindo pelo menos 1 (um) técnico especialista de cada fabricante da solução ofertada e pelo menos um profissional com conhecimento técnico da topologia completa e dos equipamentos que compõem o grupo 2.

1.22.4. Etapa 1 – Preparo e Iniciação do Projeto

1.22.4.1. Durante esta etapa, os gerentes de projeto da contratante e contratada desenvolverão o Plano, com entendimento da abrangência e cronograma do Projeto e conduzirão a reunião de kick-off para apresentar a “equipe de trabalho” e metodologia.

1.22.5. Etapa 2 – Definição de Requisitos da Solução

1.22.5.1. Nessa etapa, a contratante e a contratada definirão e validarão os requisitos técnicos e de negócio da Solução. Um documento listando todos os requerimentos da contratante deverá ser confeccionado pela contratada e deverá ser aprovado pela contratante. Todas as etapas posteriores possuem dependência desta etapa.

1.22.5.2. A contratada, juntamente com membros designados pela contratante irá:

1.22.5.2.1. Conduzir entrevistas para revisar o atual ambiente da contratante e identificar o ponto de integração entre legado e a nova Solução.

1.22.5.2.2. Identificar todos os requerimentos para o correto funcionamento da Solução.

1.22.6. Etapa 3 – Plano e Arquitetura da Solução

1.22.6.1. Durante esta etapa, a contratada trabalhará em conjunto com a contratante para definir e documentar o plano de arquitetura e desenho da Solução. Como resultado desta etapa, será confeccionado e entregue à contratante um documento de arquitetura do tipo SOW (em tradução livre, escopo de trabalho) que deverá conter o desenho definido e detalhes da configuração que será aplicada durante a etapa de implementação:

1.22.6.1.1. Objetivo dos serviços;

1.22.6.1.2. Plano de gerenciamento de mudanças, detalhando passo-a-passo o escopo da migração;

1.22.6.1.3. Cronograma das atividades que serão realizadas, com os prazos estimados e as diretrizes para cada atividade;

1.22.6.1.4. Projeto lógico de configuração e diagrama de interconexão dos equipamentos;

1.22.6.1.5. Nome(s) do(s) gerente(s) de projetos responsável(is) e do(s) técnico(s) responsável(is) pela execução dos serviços;

1.22.6.1.6. Lista de todos os elementos instalados contendo:

1.22.6.1.7. Nome e endereço IP do equipamento;

1.22.6.1.8. Equipamento e porta na qual o equipamento foi conectado;

1.22.6.1.9. Local de instalação (prédio, andar, sala);

1.22.6.1.10. Número de série do equipamento.

1.22.6.2. O SOW deverá ser entregue pela CONTRATADA em até 30 (trinta) dias úteis após a assinatura do aceite provisório dos equipamentos, o qual deverá ser aprovado pela CONTRATANTE;

1.22.6.3. Os serviços não poderão ser iniciados antes da apresentação e assinatura de concordância de ambas as partes;

1.22.7. Etapa 4 – Configuração e Integração da Solução

1.22.7.1. Durante a etapa 4, a Equipe de Projeto deverá instalar e configurar a Solução ofertada no ambiente da contratante e deverá, se necessário, integrá-la ao ambiente já existente. Nesta fase deverá ser realizado teste dos componentes da Solução, conforme desenho apresentado no

documento de arquitetura, entregue na etapa 3.

1.22.7.2. 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;

1.22.7.3. As configurações deverão seguir fielmente a padronização previamente estabelecida pela contratante.

1.22.8. Etapa 5 – Migração

1.22.8.1. A contratada deverá planejar e executar a migração de recursos do ambiente existente para a nova Solução.

1.22.8.2. A substituição da infraestrutura atual 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;

1.22.8.3. 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;

1.22.8.4. Os serviços de migração contemplam ainda a supervisão das instalações individuais dos equipamentos e a execução de um roteiro de testes para verificação da operação dos serviços, além da elaboração de relatórios gerenciais de acompanhamento dos serviços sempre que solicitados pela contratante, e a retirada dos equipamentos da infraestrutura obsoleta, que devem ser rotulados, relacionados, acondicionados em embalagens apropriadas e armazenados em local designado pela contratante;

1.22.8.5. Ao término do serviço deve 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;

1.22.8.6. A critério da contratante, poderá ser elaborado um único as-built contendo todas as informações de todos os equipamentos instalados e configurados;

1.22.9. Etapa 6 – Operação Assistida

1.22.10. Etapa 7 – Transferência de Conhecimento

1.22.11. Etapa 8 – Garantia técnica do fabricante

1.22.12. Etapa 9 – Suporte Técnico Especializado

1.22.12.1. O serviço de suporte técnico especializado deverá ser executado conjuntamente com a Solução de Segurança e Balanceamento de Carga – Tipo B (Ambiente Virtual) - item 16, devendo a CONTRATADA atuar no ambiente configurado.

1.22.12.2. Os serviços de suporte técnico abrangem os serviços de natureza corretiva, preventiva e evolutiva do ambiente virtual.

1.22.12.3. Os serviços de **natureza corretiva** são aqueles efetuados com objetivo de solucionar problemas de funcionamento e disponibilidade da solução e de esclarecer dúvidas relacionadas à instalação, configuração, uso e atualização dos produtos. São previstos como serviços de **natureza corretiva**:

1.22.12.3.1. Reinstalação de softwares, configuração, gerenciamento, com vistas a normalidade da operação dos serviços por ele prestados;

1.22.12.3.2. Reparar, corrigir, remover, refazer, no todo ou em parte, imperfeições, vícios, defeitos ou incorreções, dentro dos prazos estabelecidos;

1.22.12.3.3. Corrigir defeitos do projeto de instalação da solução;

1.22.12.3.4. Detectar problemas e limitações de desempenho da SOLUÇÃO ADC relacionados a software e/ou firmware instalados nos elementos que fazem parte do objeto desta contratação, substituindo-os por nova versão que implemente suas correções;

1.22.12.3.5. Substituir software e/ou firmware instalados nos elementos que fazem parte do objeto desta contratação por nova versão eventualmente lançada, quando esta implementar correções a possíveis problemas ou limitações de desempenho da SOLUÇÃO ADC;

1.22.12.4. Os serviços de **natureza preventiva** são aqueles nas quais a CONTRATADA, mediantes visita trimestral (on-site), realiza uma checagem da saúde e funcionamento da solução já implementada, permitindo um diagnóstico preciso do status atual da rede. São previstos como serviços de **natureza preventiva**:

1.22.12.4.1. Procedimentos técnicos destinados a prevenir a ocorrência de erros e defeitos de forma proativa;

1.22.12.4.2. Realização de inspeções nos softwares de configuração gerenciam a solução;

1.22.12.4.3. Verificação com vistas a manter sua plena funcionalidade e saúde da solução;

1.22.12.4.4. Analisar logs de sistema e sugerir mudanças para uma melhor prática de utilização da

ferramenta. A equipe técnica da CONTRATANTE decidirá sobre a aplicação ou não das recomendações;

1.22.12.4.5. Sugerir, preventivamente, a aplicação de novas correções, patches, fixes, updates, service packs, novas releases, versions, builds e upgrades.

1.22.12.5. Os serviços de **natureza evolutiva** são aqueles em que a CONTRATADA, mediante solicitação da CONTRATANTE, implementará atualizações de software para a solução objeto deste contrato, mantendo a solução em pleno funcionamento e na versão desejada pela CONTRATANTE.

1.22.12.6. Durante todo o suporte técnico, a CONTRATADA deverá dispor e tornar disponível à CONTRATANTE uma estrutura de suporte técnico, através de meio telefônico ou outro recurso de comunicação que se faça disponível e conveniente às partes, para realização de manutenções corretivas, esclarecimento de dúvidas e orientação com relação ao produto;

1.22.12.7. Através do suporte técnico especializado, CONTRATADA e CONTRATANTE devem poder atuar em conjunto para melhoria da solução implementada;

1.22.12.8. Além de serviços de implementação de melhorias da solução implementada, os serviços especializados também poderão ser utilizados para:

1.22.12.8.1. Desinstalação/reinstalação da solução;

1.22.12.8.2. Consultoria Especializada;

1.22.12.8.3. Repasse adicional de conhecimento.

1.22.12.9. Independentemente do tipo de atendimento realizado (corretivo, preventivo ou evolutivo), deverão ser registrados detalhadamente em relatório próprio todos os procedimentos adotados para a solução dos problemas encontrados ou implementação de melhorias, onde constem informações referentes à identificação do chamado, data e hora do chamado, início e término do atendimento, além de todos os envolvidos no chamado;

1.22.12.10. O atendimento para abertura de pedidos de suporte técnico deverá estar disponível 24 (vinte e quatro) horas, 07 (sete) dias por semana, durante toda vigência do contrato.

1.23. Grupo 2 – Serviço de instalação da Solução de Segurança e Balanceamento de Carga – Tipo A – Appliance Físico

1.23.1. Refere-se à instalação física e lógica, no Data Center da CONTRATANTE, da Solução Segurança e Balanceamento de Carga – Tipo A – Appliance Físico, que abrange:

1.23.1.1. Sua disposição e conectorização no rack que o acomodará;

1.23.1.2. A instalação dos transceivers em seus módulos/slots;

1.23.1.3. Sua interconexão a seu par redundante;

1.23.1.4. Sua interconexão a outros switches, roteadores e servidores de rede, entre outros;

1.23.1.5. Suas configurações de interfaces, endereçamento e serviços de rede, além das configurações das políticas de segurança da informação e de balanceamento de aplicações, e de outras configurações necessárias ou constantes no Projeto Executivo;

1.23.1.6. Sua identificação e a identificação de todas as suas conexões.

1.23.2. O escopo de instalação abrange a instalação da Solução de Segurança e Balanceamento de Carga (Tipo A – Appliance Físico) e a inclusão e configuração de todos os licenciamentos previstos no Grupo II para esta plataforma;

1.23.3. O escopo de instalação abrange ainda a instalação da plataforma de gerência inerente à Solução de Segurança e Balanceamento de Carga, que será instalada em servidores/equipamentos do parque tecnológico da contratante, sendo desta a responsabilidade pela disponibilização dos recursos necessários à sua instalação;

1.23.4. A contratada deverá providenciar todos os materiais necessários à instalação física dos equipamentos; a contratante será responsável pela disponibilização do(s) rack(s) e fornecimento de pontos elétricos necessários à instalação dos equipamentos; no entanto, todo o cabeamento para interconexão dos equipamentos fornecidos é de responsabilidade da contratada;

1.23.5. Os serviços não poderão ser iniciados antes da apresentação e assinatura de concordância de ambas as partes;

1.23.6. Ao término do serviço deve 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 módulos instalados/configurados.

1.24. Grupo 2 - Instalação da Solução de Segurança e Balanceamento de Carga – Tipo B – Ambiente Virtual

1.24.1. Refere-se à instalação da Solução de Segurança e Balanceamento de Carga – Tipo B - Ambiente Virtual, na infraestrutura de virtualização existente no MJSP e sua configuração lógica, abrangendo:

1.24.1.1. Suas configurações de interfaces, endereçamento e serviços de rede, além de outras configurações necessárias ou constantes no Projeto Executivo;

1.24.1.2. O ajuste dos demais parâmetros de configuração, conforme Projeto de Instalação.

1.24.2. Todo o ambiente virtual será instalado em servidores/equipamentos do parque tecnológico da contratante, sendo desta a responsabilidade pela disponibilização dos recursos necessários à sua instalação;

1.24.3. Os serviços não poderão ser iniciados antes da apresentação e assinatura de concordância de ambas as partes;

1.24.4. Ao término do serviço deve 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 módulos instalados/configurados.

1.25. **Grupo 2 - Treinamento**

1.25.1. 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;

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

1.25.3. A CONTRATADA deverá realizar treinamento para 1 (uma) turma com 5 (cinco) servidores indicados pela CONTRATANTE;

1.25.4. A transferência de conhecimento 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, e poderá ser realizada durante as semanas de Operação Assistida contratadas, desde que alocado técnicos distintos para cada tarefa, e somente após anuência e autorização da CONTRATANTE. A transferência de conhecimento não é parte integrante da carga horária de Operação Assistida contratada.

1.25.5. O treinamento deverá ser realizado em apenas 01 (um) turno, matutino ou vespertino.

1.25.6. O treinamento deverá ter carga horária mínima de 40 (quarenta) horas;

1.25.7. A CONTRATADA assumirá todas as despesas e encargos inerentes à transferência de conhecimento, compreendendo as despesas com hospedagem, transporte e alimentação dos técnicos responsáveis pelo repasse e demais despesas/custos indiretos que incidirem sobre esta contratação;

1.25.8. A CONTRATADA deverá fornecer toda a infraestrutura necessária para realização do treinamento;

1.25.9. A solução utilizada no para realização do treinamento deverá, no que concerne às configurações e instalação, ser idêntica à solução ofertada no certame licitatório podendo ser diferente apenas em relação à capacidade de processamento, throughput, por se tratar de treinamento;

1.25.9.1. A CONTRATADA poderá utilizar-se da solução instalada para a realização da transferência de conhecimento, garantidas as condições para que não haja interrupção da solução já implementada;

1.25.10. A CONTRATADA deverá fornecer o conteúdo didático utilizado no treinamento na forma impressa para todos os participantes;

1.25.11. A CONTRATADA deverá fornecer uma cópia digital do conteúdo didático utilizado no treinamento que deverá ser entregue para o gestor do contrato;

1.25.12. Durante a transferência de conhecimento deverão ser fornecidos aos técnicos da CONTRATANTE todo material e documentação, preferencialmente em português, necessários à perfeita compreensão da solução instalada (slides, exemplos de implementação, documentação do projeto executado na CONTRATANTE, etc.) bem como alimentação compatível com a quantidade de pessoas envolvidas, quando esta ocorrer fora da dependências das CONTRATANTE;

1.25.13. Ao término da transferência de conhecimento deverá ser realizada uma avaliação da atividade por parte da equipe da CONTRATANTE, que atribuirá as seguintes classificações: A – Mais que Suficiente, B – Suficiente e C – Insuficiente;

1.25.13.1. Caso 50% (cinquenta por cento) ou mais dos técnicos da CONTRATANTE avalie a transferência de conhecimento como insuficiente, a CONTRATADA deverá providenciar, sem ônus, outro período para a transferência de conhecimento.

1.25.14. Caberá à CONTRATADA o controle de participação no treinamento pelos servidores indicados pela CONTRATANTE;

1.25.15. Ao final do treinamento, a CONTRATADA deverá emitir certificado de participação no treinamento para os participantes;

1.25.16. O certificado emitido deverá conter:

1.25.16.1. Nome do participante;

1.25.16.2. Período de realização com dias e horários;

1.25.16.3. Carga horária do treinamento;

1.25.16.4. Percentual de frequência do participante;

1.25.16.5. Nome e assinatura do Instrutor;

1.25.16.6. Nome e assinatura do Representante da CONTRATADA;

1.25.17. O treinamento deverá abranger, no mínimo, os seguintes conteúdos:

1.25.17.1. Instalação e Configuração da Solução;

1.25.17.2. Conceitos e configuração de alta disponibilidade;

1.25.17.3. Conceitos de segurança

1.25.17.4. Solução de problemas básicos;

1.25.17.5. Demais conceitos e configurações essenciais ao entendimento e manuseio da solução por parte da CONTRATANTE.

ANEXO I - B - PROPOSTA DE PREÇOS

(EMITIR EM PAPEL TIMBRADO DA EMPRESA)

PROPOSTA DE PREÇOS

Objeto: Contratação de solução de ativos de rede, balanceamento de carga e segurança para os Data Centers, incluindo serviços especializados, aquisição de equipamentos e softwares, modernização e expansão da capacidade atual para atendimento das necessidades do Ministério da Justiça e Segurança Pública.

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

DIRETORIA 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 do Bem ou Serviço	Quantidade	Unidade de medida	Valor unitário máximo (R$)	Valor total máximo (R$)
	1	Switch Spine	04	Unitário		
	2	Switch Leaf- Tipo A	06	Unitário		
	3	Switch Leaf- Tipo B	04	Unitário		
	4	Switch de Agregação	02	Unitário		
	5	Sistema de Gerenciamento de Equipamentos de Data Center	01	Unitário		

1	6	Solução de Controle de Acesso – Virtual Machine	01	Unitário		
	7	Licenciamento Switches existentes	02	Unitário		
	8	Transceiver 10G Multimodo (LC)	70	Unitário		
	9	Transceiver 25G Multimodo (LC)	16	Unitário		
	10	Cordão Óptico Duplex, 10G Multimodo,(LC/LC) (10 metros)	62	Unitário		
	11	Cabo de Conexão Direta 100G – (10 metros)	20	Unitário		
	12	Cabo de Conexão Direta 40G – (10 metros)	08	Unitário		
	13	Operação Assistida	01	Serviço		
	VALOR TOTAL DO GRUPO				**R$**	
2	14	Solução de segurança e balanceamento de carga - Appliance Físico - Tipo A	02	Unitário		
	15	Transceiver 10G Multimodo (LC) - para item 14 (Appliance Físico - Tipo A)	16	Unitário		
	16	Subscrição de licença para solução de segurança e balanceamento de carga - Tipo B (Ambiente Virtual) para 36 meses	01	Unitário		
	17	Operação Assistida	01	Serviço		
	VALOR TOTAL DO GRUPO				**R$**	
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			

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 ___/2020, cujo objeto é a Contratação de solução de ativos de rede e balanceamento de carga para os Data Centers, incluindo serviços especializados, aquisição de equipamentos e softwares, modernização e expansão da capacidade atual para atendimento das necessidades do Ministério da Justiça e Segurança Pública.

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>	*<Nome>*
Matrícula: *<Matr.>*	*<Qualificação>*
Testemunhas	
Testemunha 1	**Testemunha 2**
_____	_____
<Nome>	*<Nome>*
<Qualificação>	*<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 ___/2020, 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>	***<Nome>***	***<Nome>***
Matrícula: *<Matr.>*	**Matrícula: *<Matr.>***	**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

Criado por bruno.alves, versão 11 por leonardo.greco em 16/10/2020 12:03:55.

Documento assinado eletronicamente por **ALEXANDRA LACERDA FERREIRA RIOS**, **Chefe da Divisão de Licitações**, em 21/10/2020, às 12:21, conforme o § 1º do art. 6º e art. 10 do Decreto nº 8.539/2015.

A autenticidade do documento pode ser conferida no site http://sei.autentica.mj.gov.br informando o código verificador **12928775** e o código CRC **70D5606D**
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.

Ministério da Justiça e Segurança Pública
Secretaria-Executiva
Divisão de Licitações

ANEXO II DO EDITAL

VALORES MÁXIMOS ADMISSÍVEIS

Grupo	Item	Descrição do Bem ou Serviço	Qtd.	Unid. medida	Valor unitário (R$)	Valor máximo total (R$)
1	1	Switch Spine	04	Unidade	307.235,00	1.228.940,00
	2	Switch Leaf- Tipo A	06	Unidade	139.875,00	839.250,00
	3	Switch Leaf- Tipo B	04	Unidade	290.290,00	1.161.160,00
	4	Switch de Agregação	02	Unidade	187.823,33	375.646,67
	5	Sistema de Gerenciamento de Equipamentos de Data Center	01	Unidade	57.100,00	57.100,00
	6	Solução de Controle de Acesso – Virtual Machine	01	Unidade	76.463,33	76.463,33
	7	Licenciamento Switches existentes	02	Unidade	23.900,00	47.800,00
	8	Transceiver 10G Multimodo (LC)	70	Unidade	2.443,33	171.033,33
	9	Transceiver 25G Multimodo (LC)	16	Unidade	3.033,33	48.533,33
	10	Cordão Óptico Duplex, 10G Multimodo,(LC/LC) (10 metros)	62	Unidade	254,78	15.796,11
	11	Cabo de Conexão Direta 100G – (10 metros)	20	Unidade	7.900,00	158.000,00
	12	Cabo de Conexão Direta 40G – (10 metros)	08	Unidade	3.523,33	28.186,67
	13	Operação Assistida	01	Unidade	111.600,00	111.600,00
	VALOR TOTAL DO GRUPO I				**R$ 4.319.509,45**	
2	14	Solução de segurança e balanceamento de carga - Appliance Físico - Tipo A	02	Unidade	1.380.752,84	2.761.505,68
	15	Transceiver 10G Multimodo (LC) - para item 14 (Appliance Físico - Tipo A)	16	Unidade	8.568,97	137.103,55
	16	Subscrição de licença para solução de segurança e balanceamento de carga - Tipo	01	Unidade	4.042.308,40	4.042.308,40

		B (Ambiente Virtual) para 36 meses				
	17	Operação Assistida	01	Unidade	91.726,20	91.726,20
	VALOR TOTAL DO GRUPO II				**R$ 7.032.643,82**	
VALOR TOTAL DA CONTRATAÇÃO:					**R$ 11.352.153,27**	

Documento assinado eletronicamente por **ALEXANDRA LACERDA FERREIRA RIOS**, **Chefe da Divisão de Licitações**, em 21/10/2020, às 13:07, conforme o § 1º do art. 6º e art. 10 do Decreto nº 8.539/2015.

A autenticidade do documento pode ser conferida no site http://sei.autentica.mj.gov.br informando o código verificador **12927725** e o código CRC **256FEC5B**
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.

Ministério da Justiça e Segurança Pública
Secretaria-Executiva

Esplanada dos Ministérios, Bloco T, Anexo II 6º andar, Sala 612/614, - Bairro Zona Cívico-Administrativa, Brasília/DF, CEP 70064-900
Telefone: (61) 2025-7645 - - https://www.justica.gov.br

ANEXO DO EDITAL III

Minuta de Contrato 1

TERMO DE CONTRATO Nº ……../…., QUE ENTRE S CELEBRAM A UNIÃO, REPRESENTADA PELO MINISTÉRIO DA JUSTIÇA E SEGURANÇA PÚBLICA, PO INTERMÉDIO DA DIRETORIA DE TECNOLOGIA DA INFORMAÇÃO E COMUNICAÇÃO, DA COORDENAÇÃO-GERAL DE LICITAÇÕES E CONTRATOS, E A EMPRESA XXXXXXXX.

PROCESSO Nº 08006.000602/2020-71

A União, representada pelo **MINISTÉRIO DA JUSTIÇA E SEGURANÇA PÚBLICA - MJSP**, com sede na Esplanada dos Ministérios, CEP 70064-900, Brasília/DF, inscrito no CNPJ 00.394.494/0013-70, neste ato representada pelo Diretor de Tecnologia da Informação e Comunicação, Senhor **RODRIGO LANGE**, brasileiro, casado, portador do RG nº 38542508 - SSP/PR e CPF nº 017.698.019-95, nomeado por meio da Portaria n° 29 de 2 de janeiro de 2019, publicada no D.O.U de 2 de janeiro de 2019 - Edição Extra,com delegação de competência fixada pela Portaria nº 77, de 17 de janeiro de 2020, publicada no D.O.U de 20 de janeiro de 2020, e pela Coordenadora-Geral de Licitações e Contratos, **Sra. DÉBORA DE SOUZA JANUÁRIO**, brasileira, solteira, portadora do RG nº 3.558.79980– SSP/SP e do CPF nº 712.315.791-53, nomeada por meio da Portaria n° 1.087, de 06 de novembro de 2015, publicada na D.O.U de 09 de novembro de 2015 e com delegação de competência fixada pela Portaria nº 03, de 22 de janeiro de 2020, publicada no D.O.U. de 24 de janeiro de 2020, doravante denominada **CONTRATANTE,** e a Empresa **[NOME DA CONTRATADA EM CAIXA ALTA E NEGRITO]**, estabelecida na [endereço da contratada], CEP: [número do CEP], [cidade] - [UF]**,** inscrita no MF/CNPJ sob o nº [número do CNPJ da contratada], neste ato representada pelo **Sr. [NOME DO REPRESENTANTE LEGAL DA CONTRATADA EM CAIXA ALTA E NEGRITO]**, [nacionalidade], [estado civil], portador do RG [número do RG - órgão expeditor] e do CPF nº: [número do CPF]**,** doravante denominada **CONTRATADA**, tendo em vista o que consta no Processo nº 08006.000602/2020-71 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 – DO OBJETO

1.1. O objeto do presente Termo de Contrato é a contratação de solução de ativos de rede e balanceamento de carga para os Data Centers, incluindo serviços especializados, aquisição de equipamentos e softwares, modernização e expansão da capacidade atual para atendimento das necessidades do Ministério da Justiça e Segurança Pública.

1.2. Este Termo de Contrato vincula-se ao Edital do Pregão, identificado no preâmbulo e à proposta vencedora, independentemente de transcrição.

1.3. Objeto da contratação:

GRUPO	ITEM	DESCRIÇÃO DO BEM OU SERVIÇO	CÓDIGO CATMAT/CATSER	QUANTIDADE	MÉTRICA OU UNIDADE	VALOR UNITÁRIO	VALOR TOTAL
1	1	Switch Spine	**122971**	04	Unidade		
	2	Switch Leaf- Tipo A	**122971**	06	Unidade		
	3	Switch Leaf- Tipo B	**122971**	04	Unidade		
	4	Switch de Agregação	**122971**	02	Unidade		
	5	Sistema de Gerenciamento de Equipamentos de Data Center	**27464**	01	Unidade		
	6	Solução de Controle de Acesso – Virtual Machine	**27464**	01	Unidade		
	7	Licenciamento Switches existentes	**27464**	02	Unidade		
	8	Transceiver 10G Multimodo (LC)	**150812**	70	Unidade		
	9	Transceiver 25G Multimodo (LC)	**150812**	16	Unidade		
	10	Cordão Óptico Duplex, 10G Multimodo,(LC/LC) (10 metros)	**41521**	62	Unidade		
	11	Cabo de Conexão Direta 100G – (10 metros)	**150812**	20	Unidade		
	12	Cabo de Conexão Direta 40G – (10 metros)	**150812**	08	Unidade		
	13	Operação Assistida	**27340**	01	Unidade		
Grupo	**Item**	**Descrição do Bem ou Serviço**	**Código CATMAT/CATSER**	**Quantidade**	**Métrica ou Unidade**		
2	14	Solução de segurança e balanceamento de carga - Appliance Físico - Tipo A	**150100**	02	Unidade		
	15	Transceiver 10G Multimodo - para item 14 (Appliance Físico - Tipo A)	**150812**	16	Unidade		

	17	Operação Assistida	**27340**	01	Unidade		

2. CLÁUSULA SEGUNDA – VIGÊNCIA

2.1. O prazo de vigência deste Termo de Contrato é aquele fixado no Edital, com início na data de ...../...../..... e encerramento em ...../...../....., prorrogável na forma do art. 57, § 1°, da Lei n° 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.

3. CLÁUSULA TERCEIRA - PREÇO

3.1. O valor total da contratação é de R$..... (.....)

3.2. No valor acima estão incluídas todas as despesas ordinárias diretas e indiretas decorrentes da execução do objeto, inclusive tributos e/ou impostos, encargos sociais, trabalhistas, previdenciários, fiscais e comerciais incidentes, taxa de administração, frete, seguro e outros necessários ao cumprimento integral do objeto da contratação.

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

4. CLÁUSULA QUARTA - DOTAÇÃO ORÇAMENTÁRIA

4.4. As despesas decorrentes desta contratação estão programadas em dotação orçamentária própria, prevista no orçamento da União, para o exercício de 20XX, na classificação abaixo:

4.4.1. Programa de Trabalho: 04122003220000000001

4.4.2. Plano de Trabalho Resumido (PTRES): 172184

4.4.3. Fonte: 0100

4.4.4. Ação: 2000

4.4.5. Plano Orçamentário (PO): 000C

4.4.6. Plano Interno (PI): GL67PTCGLTI

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

Grupo	Item	Descrição do Bem ou Serviço	Natureza de Despesa
1	1	Switch Spine	44905237
	2	Switch Leaf- Tipo A	44905237
	3	Switch Leaf- Tipo B	44905237
	4	Switch de Agregação	44905237
	5	Sistema de Gerenciamento de Equipamentos de Data Center	44904005
	6	Solução de Controle de Acesso – Virtual Machine	44904005
	7	Licenciamento Switches existentes	44904005
	8	Transceiver 10G Multimodo (LC)	44905237
	9	Transceiver 25G Multimodo (LC)	44905237
	10	Cordão Óptico Duplex, 10G Multimodo,(LC/LC) (10 metros)	33903017
	11	Cabo de Conexão Direta 100G – (10 metros)	33903017
	12	Cabo de Conexão Direta 40G – (10 metros)	33903017
	13	Operação Assistida	33903504
		Solução de segurança e balanceamento de carga - Appliance Físico -	

2	14	Solução de segurança e balanceamento de carga - Appliance Físico - Tipo A	44905237
	15	Transceiver 10G Multimodo - para item 14 (Appliance Físico - Tipo A)	44905237
	17	Operação Assistida	33903504

4.5. No(s) exercício(s) seguinte(s), as despesas correspondentes correrão à conta dos recursos próprios para atender às despesas da mesma natureza, cuja alocação será feita no início de cada exercício financeiro.

5. CLÁUSULA QUINTA - PAGAMENTO

5.1. O prazo para pagamento à CONTRATADA e demais condições a ele referentes encontram-se definidos no Termo de Referência e no Anexo XI da IN SEGES/MPDG n. 5/2017.

6. CLÁUSULA SEXTA - REAJUSTAMENTO DE PREÇOS EM SENTIDO AMPLO

6.1. Os preços são fixos e irreajustáveis.

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 dos serviços a serem executados pela CONTRATADA, os materiais que serão empregados, a disciplina do recebimento do objeto e a fiscalização pela CONTRATANTE são aqueles previstos no Termo de Referência, anexo do Edital.

9. CLÁUSULA NONA – OBRIGAÇÕES DA CONTRATANTE E DA CONTRATADA

9.1. As obrigações da CONTRATANTE e da CONTRATADA 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 Termo de Referência, anexo do Edital.

11. CLÁUSULA DÉCIMA PRIMEIRA – RESCISÃO

11.1. O presente Termo de Contrato poderá ser rescindido:

11.1.1. por ato unilateral e escrito da Administração, nas situações previstas nos incisos I a XII e XVII do art. 78 da Lei nº 8.666, de 1993, e com as consequências indicadas no art. 80 da mesma Lei, sem prejuízo da aplicação das sanções previstas no Termo de Referência, anexo ao Edital;

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

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

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

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

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

11.4.2. Relação dos pagamentos já efetuados e ainda devidos;

11.4.3. Indenizações e multas.

12. CLÁUSULA DÉCIMA SEGUNDA – VEDAÇÕES E PERMISSÕES

12.1. É vedado à CONTRATADA interromper a execução dos serviços sob alegação de inadimplemento por parte da CONTRATANTE, salvo nos casos previstos em lei.

12.2. É permitido à CONTRATADA caucionar ou utilizar este Termo de Contrato para qualquer operação financeira, nos termos e de acordo com os procedimentos previstos na Instrução Normativa SEGES/ME nº 53, de 8 de Julho de 2020.

12.2.1. A cessão de crédito, a ser feita mediante celebração de Termo Aditivo, dependerá de comprovação da regularidade fiscal e trabalhista da cessionária, bem como da certificação de que a cessionária não se encontra impedida de licitar e contratar com o Poder Público, conforme a legislação em vigor, nos termos do Parecer JL-01, de 18 de maio de 2020.

12.2.2. A crédito a ser pago à cessionária é exatamente aquele que seria destinado à cedente (CONTRATADA) pela execução do objeto contratual, com o desconto de eventuais multas, glosas e prejuízos causados à Administração, sem prejuízo da utilização de institutos tais como os da conta vinculada e do pagamento direto previstos na IN SEGES/ME nº 5, de 2017, caso aplicáveis.

13. CLÁUSULA DÉCIMA TERCEIRA – ALTERAÇÕES

13.1. Eventuais alterações contratuais reger-se-ão pela disciplina do art. 65 da Lei nº 8.666, de 1993, bem como do ANEXO X da IN/SEGES/MPDG nº 05, de 2017.

13.2. A CONTRATADA é obrigada a aceitar, nas mesmas condições contratuais, os acréscimos ou supressões que se fizerem necessários, até o limite de 25% (vinte e cinco por cento) do valor inicial atualizado do Contrato.

13.3. As supressões resultantes de acordo celebrado entre as partes contratantes poderão exceder o limite de 25% (vinte e cinco por cento) do valor inicial atualizado do Contrato.

14. CLÁUSULA DÉCIMA QUARTA – DOS CASOS OMISSOS

14.1. Os casos omissos serão decididos pela CONTRATANTE, segundo as disposições contidas na Lei nº 8.666, de 1993, na Lei nº 10.520, de 2002 e demais normas federais aplicáveis e, subsidiariamente, segundo as disposições contidas na Lei nº 8.078, de 1990 – Código de Defesa do Consumidor – e normas e princípios gerais dos contratos.

15. CLÁUSULA DÉCIMA QUINTA - ASSINATURA ELETRÔNICA

15.1. O presente Termo de Contrato será firmado por meio de assinatura eletrônica e/ou digital, certificada pelo Sistema Eletrônico de Informações-SEI! do Ministério da Justiça e Segurança Pública, garantida a eficácia das Cláusulas.

15.2. Em conformidade com o disposto no § 2º, art. 10, da MPV 2.200/01, a assinatura deste Termo de Contrato 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.

15.3. A sua 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.

16. CLÁUSULA DÉCIMA SEXTA – PUBLICAÇÃO

16.4. Incumbirá à CONTRATANTE providenciar a publicação deste Termo de Contrato, por extrato, no Diário Oficial da União, no prazo previsto na Lei nº 8.666, de 1993.

17. CLÁUSULA DÉCIMA SÉTIMA – FORO

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

Para firmeza e validade do pactuado, o presente Termo de Contrato, depois de lido e achado em

ordem, vai assinado pelos contraentes e por duas testemunhas.

RODRIGO LANGE
Diretor de Tecnologia da Informação e Comunicação
Ministério da Justiça e Segurança Pública

DÉBORA DE SOUZA JANUÁRIO
Coordenadora-Geral de Licitações e Contratos
Ministério da Justiça e Segurança Pública

XXXXXXXXXXXXX
Representante da Empresa Contratada

TESTEMUNHAS:

1.

2.

Ministério da Justiça e Segurança Pública
Secretaria-Executiva

Esplanada dos Ministérios, Bloco T, Anexo II 6º andar, Sala 612/614, - Bairro Zona Cívico-Administrativa, Brasília/DF, CEP 70064-900
Telefone: (61) 2025-7645 - - https://www.justica.gov.br

ANEXO DO EDITAL VI

Minuta de Contrato 2

TERMO DE CONTRATO Nº ……../…., QUE ENTRE S CELEBRAM A UNIÃO, REPRESENTADA PELO MINISTÉRIO DA JUSTIÇA E SEGURANÇA PÚBLICA, PO INTERMÉDIO DA DIRETORIA DE TECNOLOGIA DA INFORMAÇÃO E COMUNICAÇÃO, DA COORDENAÇÃO-GERAL DE LICITAÇÕES E CONTRATOS, E A EMPRESA XXXXXXXX.

PROCESSO Nº 08006.000602/2020-71

A União, representada pelo **MINISTÉRIO DA JUSTIÇA E SEGURANÇA PÚBLICA - MJSP**, com sede na Esplanada dos Ministérios, CEP 70064-900, Brasília/DF, inscrito no CNPJ 00.394.494/0013-70, neste ato representada pelo Diretor de Tecnologia da Informação e Comunicação, Senhor **RODRIGO LANGE**, brasileiro, casado, portador do RG nº 38542508 - SSP/PR e CPF nº 017.698.019-95, nomeado por meio da Portaria n° 29 de 2 de janeiro de 2019, publicada no D.O.U de 2 de janeiro de 2019 - Edição Extra,com delegação de competência fixada pela Portaria nº 77, de 17 de janeiro de 2020, publicada no D.O.U de 20 de janeiro de 2020, e pela Coordenadora-Geral de Licitações e Contratos, **Sra. DÉBORA DE SOUZA JANUÁRIO**, brasileira, solteira, portadora do RG nº 3.558.79980– SSP/SP e do CPF nº 712.315.791-53, nomeada por meio da Portaria n° 1.087, de 06 de novembro de 2015, publicada na D.O.U de 09 de novembro de 2015 e com delegação de competência fixada pela Portaria nº 03, de 22 de janeiro de 2020, publicada no D.O.U. de 24 de janeiro de 2020, doravante denominada **CONTRATANTE,** e a Empresa **[NOME DA CONTRATADA EM CAIXA ALTA E NEGRITO]**, estabelecida na [endereço da contratada], CEP: [número do CEP], [cidade] - [UF]**,** inscrita no MF/CNPJ sob o nº [número do CNPJ da contratada], neste ato representada pelo **Sr. [NOME DO REPRESENTANTE LEGAL DA CONTRATADA EM CAIXA ALTA E NEGRITO]**, [nacionalidade], [estado civil], portador do RG [número do RG - órgão expeditor] e do CPF nº: [número do CPF]**,** doravante denominada **CONTRATADA**, tendo em vista o que consta no Processo nº 08006.000602/2020-71 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 – DO OBJETO

1.1. O objeto do presente Termo de Contrato é a contratação de solução de ativos de rede e balanceamento de carga para os Data Centers, incluindo serviços especializados, aquisição de equipamentos e softwares, modernização e expansão da capacidade atual para atendimento das necessidades do Ministério da Justiça e Segurança Pública.

1.2. Este Termo de Contrato vincula-se ao Edital do Pregão, identificado no preâmbulo e à proposta vencedora, independentemente de transcrição.

1.3. Objeto da contratação:

GRUPO	ITEM	DESCRIÇÃO DO BEM OU SERVIÇO	CÓDIGO CATMAT/CATSER	QUANTIDADE	MÉTRICA OU UNIDADE	VALOR UNITÁRIO	VALOR TOTAL
2	16	Solução de segurança e balanceamento de carga - Tipo B (Ambiente Virtual) para 36 meses	27502	01	Unidade		

2. CLÁUSULA SEGUNDA – VIGÊNCIA

2.1. O prazo de vigência deste Termo de Contrato é aquele fixado no Edital, com início na data de ...../...../..... e encerramento em ...../...../....., podendo ser prorrogado por interesse das partes até o limite de 48 (quarenta e oito) meses, desde que haja autorização formal da autoridade competente, atentando, em especial para o cumprimento dos seguintes requisitos:

2.1.1. Esteja formalmente demonstrado que a forma de prestação dos serviços tem natureza continuada;

2.1.2. Seja juntado relatório que discorra sobre a execução do contrato, com informações de que os serviços tenham sido prestados regularmente;

2.1.3. Seja juntada justificativa e motivo, por escrito, de que a Administração mantém interesse na realização do serviço;

2.1.4. Seja comprovado que o valor do contrato permanece economicamente vantajoso para a Administração;

2.1.5. Haja manifestação expressa da CONTRATADA informando o interesse na prorrogação;

2.1.6. Seja comprovado que a CONTRATADA mantém as condições iniciais de habilitação.

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

2.3. A prorrogação de contrato deverá ser promovida mediante celebração de Termo Aditivo.

3. CLÁUSULA TERCEIRA - PREÇO

3.1. O valor total da contratação é de R$..... (.....)

3.2. No valor acima estão incluídas todas as despesas ordinárias diretas e indiretas decorrentes da execução do objeto, inclusive tributos e/ou impostos, encargos sociais, trabalhistas, previdenciários, fiscais e comerciais incidentes, taxa de administração, frete, seguro e outros necessários ao cumprimento integral do objeto da contratação.

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

4. CLÁUSULA QUARTA - DOTAÇÃO ORÇAMENTÁRIA

4.4. As despesas decorrentes desta contratação estão programadas em dotação orçamentária própria, prevista no orçamento da União, para o exercício de 20XX, na classificação abaixo:

4.4.1. Programa de Trabalho: 04122003220000000001

4.4.2. Plano de Trabalho Resumido (PTRES): 172184

4.4.3. Natureza da Despesa: 33904006

4.4.4. Fonte: 0100

4.4.5. Ação: 2000

4.4.6. Plano Orçamentário (PO): 000C

4.4.7. Plano Interno (PI): GL67PTCGLTI

4.4.8. No(s) exercício(s) seguinte(s), as despesas correspondentes correrão à conta dos recursos próprios para atender às despesas da mesma natureza, cuja alocação será feita no início de cada exercício financeiro.

5. CLÁUSULA QUINTA - PAGAMENTO

5.1. O prazo para pagamento à CONTRATADA e demais condições a ele referentes encontram-se definidos no Termo de Referência e no Anexo XI da IN SEGES/MPDG n. 5/2017.

6. CLÁUSULA SEXTA - REAJUSTAMENTO DE PREÇOS EM SENTIDO AMPLO

6.1. Os preços são fixos e irreajustáveis.

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 dos serviços a serem executados pela CONTRATADA, os materiais que serão empregados, a disciplina do recebimento do objeto e a fiscalização pela CONTRATANTE são aqueles previstos no Termo de Referência, anexo do Edital.

9. CLÁUSULA NONA – OBRIGAÇÕES DA CONTRATANTE E DA CONTRATADA

9.1. As obrigações da CONTRATANTE e da CONTRATADA 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 Termo de Referência, anexo do Edital.

11. CLÁUSULA DÉCIMA PRIMEIRA – RESCISÃO

11.1. O presente Termo de Contrato poderá ser rescindido:

11.1.1. por ato unilateral e escrito da Administração, nas situações previstas nos incisos I a XII e XVII do art. 78 da Lei nº 8.666, de 1993, e com as consequências indicadas no art. 80 da mesma Lei, sem prejuízo da aplicação das sanções previstas no Termo de Referência, anexo ao Edital;

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

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

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

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

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

11.4.2. Relação dos pagamentos já efetuados e ainda devidos;

11.4.3. Indenizações e multas.

12. CLÁUSULA DÉCIMA SEGUNDA – VEDAÇÕES E PERMISSÕES

12.1. É vedado à CONTRATADA interromper a execução dos serviços sob alegação de inadimplemento por parte da CONTRATANTE, salvo nos casos previstos em lei.

12.2. É permitido à CONTRATADA caucionar ou utilizar este Termo de Contrato para qualquer operação financeira, nos termos e de acordo com os procedimentos previstos na Instrução Normativa SEGES/ME nº 53, de 8 de Julho de 2020.

12.2.1. A cessão de crédito, a ser feita mediante celebração de Termo Aditivo, dependerá de comprovação da regularidade fiscal e trabalhista da cessionária, bem como da certificação de que a cessionária não se encontra impedida de licitar e contratar com o Poder Público, conforme a legislação em vigor, nos termos do Parecer JL-01, de 18 de maio de 2020.

12.2.2. A crédito a ser pago à cessionária é exatamente aquele que seria destinado à cedente (CONTRATADA) pela execução do objeto contratual, com o desconto de eventuais multas, glosas e prejuízos causados à Administração, sem prejuízo da utilização de institutos tais como os da conta vinculada e do pagamento direto previstos na IN SEGES/ME nº 5, de 2017, caso aplicáveis.

13. CLÁUSULA DÉCIMA TERCEIRA – ALTERAÇÕES

13.1. Eventuais alterações contratuais reger-se-ão pela disciplina do art. 65 da Lei nº 8.666, de 1993, bem como do ANEXO X da IN/SEGES/MPDG nº 05, de 2017.

13.2. A CONTRATADA é obrigada a aceitar, nas mesmas condições contratuais, os acréscimos ou supressões que se fizerem necessários, até o limite de 25% (vinte e cinco por cento) do valor inicial atualizado do Contrato.

13.3. As supressões resultantes de acordo celebrado entre as partes contratantes poderão exceder o limite de 25% (vinte e cinco por cento) do valor inicial atualizado do Contrato.

14. CLÁUSULA DÉCIMA QUARTA – DOS CASOS OMISSOS

14.1. Os casos omissos serão decididos pela CONTRATANTE, segundo as disposições contidas na Lei nº 8.666, de 1993, na Lei nº 10.520, de 2002 e demais normas federais aplicáveis e, subsidiariamente, segundo as disposições contidas na Lei nº 8.078, de 1990 – Código de Defesa do Consumidor – e normas e princípios gerais dos contratos.

15. CLÁUSULA DÉCIMA QUINTA - ASSINATURA ELETRÔNICA

15.1. O presente Termo de Contrato será firmado por meio de assinatura eletrônica e/ou digital, certificada pelo Sistema Eletrônico de Informações-SEI! do Ministério da Justiça e Segurança Pública, garantida a eficácia das Cláusulas.

15.2. Em conformidade com o disposto no § 2º, art. 10, da MPV 2.200/01, a assinatura deste Termo de Contrato 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.

15.3. A sua 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.

16. CLÁUSULA DÉCIMA SEXTA – PUBLICAÇÃO

16.4. Incumbirá à CONTRATANTE providenciar a publicação deste Termo de Contrato, por extrato, no Diário Oficial da União, no prazo previsto na Lei nº 8.666, de 1993.

17. CLÁUSULA DÉCIMA SÉTIMA – FORO

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

Para firmeza e validade do pactuado, o presente Termo de Contrato, depois de lido e achado em ordem, vai assinado pelos contraentes e por duas testemunhas.

RODRIGO LANGE
Diretor de Tecnologia da Informação e Comunicação
Ministério da Justiça e Segurança Pública

DÉBORA DE SOUZA JANUÁRIO
Coordenadora-Geral de Licitações e Contratos
Ministério da Justiça e Segurança Pública

XXXXXXXXXXXXX
Representante da Empresa Contratada

TESTEMUNHAS:

1.

2.