3329800 00135.214051/2021-24

MINISTÉRIO DA MULHER, DA FAMÍLIA E DOS DIREITOS HUMANOS
COORDENAÇÃO DE PROCEDIMENTOS LICITATÓRIOS
SCS Quadra 09 - Lote C, Ed. Parque Cidade Corporate, Torre-A, 10º Andar
Brasília, DF. CEP 70308-200. - http://www.mdh.gov.br

EDITAL Nº 11/2022

PROCESSO Nº 00135.214051/2021-24

Torna-se público que o Ministério da Mulher, da Família e dos Direitos Humanos - MMFDH, por meio da Coordenação-Geral de Logística, sediada no Setor Comercial Sul, Bloco B, Quadra 09, Lote C, Edifício Parque Cidade Corporate, Torre A, CEP 70308-200, na cidade de Brasília/DF, realizará licitação, na modalidade PREGÃO, na forma ELETRÔNICA, **com critério de julgamento menor preço global**, sob a forma de execução indireta, no regime de empreitada por preço global, nos termos da Lei nº 10.520, de 17 de julho de 2002, da Lei nº 8.248, de 22 de outubro de 1991, do Decreto nº 10.024, de 20 de setembro de 2019, do Decreto 9.507, de 21 de setembro de 2018, do Decreto nº 7.746, de 05 de junho de 2012, do Decreto nº 7.174, de 12 de maio de 2010, da Instrução Normativa SGD/ME nº 1, de 4 de abril de 2019, das Instruções Normativas SEGES/MP nº 05, de 26 de maio de 2017 e nº 03, de 26 de abril de 2018 e da Instrução Normativa SLTI/MPOG nº 01, de 19 de janeiro de 2010, da Lei Complementar n° 123, de 14 de dezembro de 2006, da Lei nº 11.488, de 15 de junho de 2007, do Decreto n° 8.538, de 06 de outubro de 2015, aplicando-se, subsidiariamente, a Lei nº 8.666, de 21 de junho de 1993 e as exigências estabelecidas neste Edital.

Data da sessão: **30/12/2022**

Horário: **09:00h**

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

Critério de Julgamento: Menor preço

Regime de Execução: Empreitada por preço global

1. DO OBJETO

1.1. O objeto da presente licitação é a escolha da proposta mais vantajosa para a Contratação de modernização da Solução de Balanceamento de Carga de Servidores e Solução de Segurança Web existente, incluindo renovação do suporte técnico e expansão do licenciamento, conforme condições, quantidades e exigências estabelecidas no Termo de Referência do presente Edital.

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

1.3. O critério de julgamento adotado será o menor preço global, 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 2022, na classificação abaixo:

Gestão/Unidade: 00001/810005

Fonte: 0100

PTRES: 174791

Programa de Trabalho: 14.122.0032.2000.0001

Natureza de Despesa: 339040

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, assumir 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 da senha, 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, concordata ou insolvência, em processo de dissolução ou liquidação;

4.2.6. entidades empresariais que estejam reunidas em consórcio;

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

4.2.8. sociedades cooperativas, considerando a vedação contida no art. 10 da da Instrução Normativa/SEGES nº 05/2017.

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 nº 7.203, de 2010, é vedada, ainda, a utilização, na execução dos serviços contratados, de empregado da futura Contratada que seja familiar de agente público ocupante de cargo em comissão ou função de confiança neste órgão contratante.

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

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

4.5.1.1. nos itens exclusivos para participação de microempresas a empresa de pequeno porte, a assinalação do campo "não" impedirá o prosseguimento no certame.

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

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

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

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

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

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

5. DA APRESENTAÇÃO DA PROPOSTA E DOS DOCUMENTOS DE HABILITAÇÃO

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

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

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

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

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

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

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

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

6. PREENCHIMENTO DA PROPOSTA

6.1. O licitante deverá enviar sua proposta mediante o preenchimento, no sistema eletrônico, do seguinte campo:

6.1.1. Valor unitário e total dos itens;

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

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

6.3. Nos valores propostos estarão inclusos todos os custos operacionais, encargos previdenciários, trabalhistas, tributários, comerciais e quaisquer outros que incidam direta ou indiretamente no fornecimento da solução, apurados mediante o preenchimento do modelo de proposta de preços, conforme anexo deste Edital;

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

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

6.4. 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 fornecer a solução nos seus termos, bem como de fornecer os materiais, equipamentos, ferramentas e utensílios necessários, em quantidades e qualidades adequadas à perfeita execução contratual, promovendo, quando requerido, sua substituição.

6.8. 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 DE LANCES

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

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

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

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

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

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

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

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

7.5.1. ***O lance deverá ser ofertado pelo valor total por item.***

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

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

7.8. O intervalo mínimo de diferença de valores ou percentuais entre os lances, que incidirá tanto em relação aos lances intermediários quanto em relação à proposta que cobrir a melhor **oferta deverá ser de R$100,00 (cem reais).**

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

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

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

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

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

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

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

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

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

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

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

7.20. Em relação a itens não exclusivos para participação de microempresas e empresas de pequeno porte, uma vez encerrada a etapa de lances, será efetivada a verificação automática, junto à

Receita Federal, do porte da entidade empresarial. O sistema identificará em coluna própria as microempresas e empresas de pequeno porte participantes, procedendo à comparação com os valores da primeira colocada, se esta for empresa de maior porte, assim como das demais classificadas, para o fim de aplicar-se o disposto nos arts. 44 e 45 da LC nº 123, de 2006, regulamentada pelo Decreto nº 8.538, de 2015.

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

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

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

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

7.25. 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 objeto executado:

7.26.1. por empresas brasileiras;

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

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

7.27. 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 prevista deste 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.

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

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

8. DA ACEITABILIDADE DA PROPOSTA VENCEDORA

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

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

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

8.3. A proposta de preços deverá ser encaminhada pelo licitante exclusivamente via sistema, no prazo de 2 (duas) horas, contado da solicitação do Pregoeiro, com os respectivos valores adequados ao lance vencedor e será analisada pelo Pregoeiro no momento da aceitação do lance vencedor.

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

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

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

8.5.2. contenha vício insanável ou ilegalidade;

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

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

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

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

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

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

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

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

8.8.1. Na hipótese de necessidade de suspensão de sessão pública para a realização de diligências, com vista ao saneamento das propostas, a sessão pública somente poderá ser reiniciada mediante aviso prévio no sistema com, no mínimo, vinte e quatro horas de antecedência, e a ocorrência será registrada em ata.

8.9. 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.

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

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

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

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

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

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

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

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

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

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

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

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

9. DA HABILITAÇÃO

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

a) SICAF;

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

c) Cadastro Nacional de Condenações Cíveis por Atos de Improbidade Administrativa, mantido pelo Conselho Nacional de Justiça (https://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://certidoes-apf.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 licitante será verificada por meio do SICAF, nos documentos por ele abrangidos, em relação à habilitação jurídica, à regularidade fiscal e à qualificação econômica financeira, 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 a apresentação dos documentos originais não-digitais quando houver dúvida em relação à integridade do documento digital .

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

9.6. Se o licitante for a matriz, todos os documentos deverão estar em nome da matriz, e se o licitante for a filial, todos os documentos deverão estar em nome da filial, exceto 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 diferentes números de documentos pertinentes ao CND e ao CRF/FGTS, quando for comprovada a centralização do recolhimento dessas contribuições.

9.7. Ressalvado o disposto do item 5.3, os licitantes deverão encaminhar, nos termos deste Edital, a documentação nos itens a seguir, para fins de habilitação.

9.8. **Habilitação jurídica:**

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

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

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

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

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

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

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

9.9. **Regularidade fiscal e trabalhista:**

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

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

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

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

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

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

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

9.10. **Qualificação Econômico-Financeira:**

9.10.1. 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;

9.10.1.1. 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;

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

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

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

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

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

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

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.

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

9.11.3. **No mínimo 1 (um) Atestado de Capacidade Técnica, fornecido por pessoa jurídica de direito público ou privado, que comprove que a empresa licitante já realizou a entrega deste referido serviço;**

9.11.3.1. **Poderá ser admitida, para fins de comprovação de quantitativo mínimo do serviço, a apresentação de diferentes atestados de serviços executados de forma concomitante, pois essa situação se equivale, para fins de comprovação de capacidade técnico-operacional, a uma única contratação.**

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

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

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

9.11.7. 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 equivale, para fins de comprovação de capacidade técnico-operacional, a uma única contratação, nos termos do item "10.9" do Anexo VII-A da IN SEGES/MPDG n. 5/2017.

9.11.8. Os atestados ou certidões recebidos estão sujeitos à verificação do pregoeiro e da sua equipe de apoio quanto à veracidade dos respectivos conteúdos.

9.11.9. O pregoeiro e da sua equipe de apoio poderá realizar diligência para verificação da autenticidade dos conteúdos dos atestados, nos termos do art. 43, §3º da Lei nº 8.666/93.

9.11.10. Encontrada divergência entre o especificado nos atestados e o apurado em eventual diligência, inclusive validação do contrato de prestação de serviços entre o emissor do atestado e a licitante, além da desclassificação no processo licitatório, fica sujeita a licitante, às penalidades cabíveis.

9.11.11. O licitante disponibilizará todas as informações necessárias à comprovação da legitimidade dos atestados apresentados, apresentando, dentre outros documentos, cópia do contrato que deu suporte à contratação, endereço atual da contratante e local em que foram prestados os serviços, consoante o disposto no item 10.10 do Anexo VII-A da IN SEGES/MPDG n. 5/2017.

9.11.12. 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.

9.12. 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.

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

9.13. 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.

9.14. 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.

9.15. 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.

9.16. 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.

9.17. 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.

9.18. 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 proposta de preços e formação de preços, devidamente ajustada ao lance vencedor, em conformidade com o modelo anexo a este instrumento convocatório.

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

10.1.4. Ainda, juntamente com sua proposta final, a Licitante deverá entregar, preenchido e assinado pelo responsável legal o **Termo de Integridade** (modelo anexo III do TR) e **Termo de Compromisso de Manutenção de Sigilo** (modelo anexo II do Termo de Referência), sob pena de desclassificação da licitante durante a sessão pública.

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 qual(is) decisão(ões) pretende recorrer e por quais motivos, em campo próprio do sistema.

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

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

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

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

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

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

12. DA REABERTURA DA SESSÃO PÚBLICA

12.1. A sessão pública poderá ser reaberta:

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

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

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

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

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

13. DA ADJUDICAÇÃO E HOMOLOGAÇÃO

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

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

14. DA GARANTIA DE EXECUÇÃO

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

15. DO TERMO DE CONTRATO OU INSTRUMENTO EQUIVALENTE

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

15.2. O adjudicatário terá o prazo de 10 (dez) dias úteis, contados a partir da data de sua convocação, para assinar o Termo de Contrato no qual prestará garantia no valor correspondente a 3% (três por cento) do valor do Contrato, que será liberada de acordo com as condições previstas no Edital, conforme disposto no Art. 56 da Lei nº 8.666, de 1993, desde que cumpridas as obrigações contratuais. Por mais, poderá ser aceito 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. Alternativamente à convocação para comparecer perante o órgão ou entidade para a assinatura do Termo de Contrato, a Administração poderá encaminhá-lo para assinatura, mediante correspondência postal com aviso de recebimento (AR) ou meio eletrônico, para que seja assinado e devolvido no prazo de 05 (cinco) dias, a contar da data de seu recebimento.

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 36 (trinta e seis) meses, prorrogável na forma do art. 57, § 1°, da Lei n° 8.666/93.

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 ou da ata

de registro de preços.

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, a Administração, sem prejuízo da aplicação das sanções das demais cominações legais cabíveis a esse licitante, poderá convocar outro licitante, respeitada a ordem de classificação, para, após a comprovação dos requisitos para habilitação, analisada a proposta e eventuais documentos complementares e, feita a negociação, assinar o contrato ou ata de registro de preços.

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. DA ACEITAÇÃO DO OBJETO E DA FISCALIZAÇÃO

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

18. DAS OBRIGAÇÕES DA CONTRATANTE E DA CONTRATADA

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

19. DO MODELO DE GESTÃO DO CONTRATO

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

20. DO PAGAMENTO

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

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

21. DAS SANÇÕES ADMINISTRATIVAS

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

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

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

21.1.3. apresentar documentação falsa;

21.1.4. deixar de entregar os documentos exigidos no certame;

21.1.5. ensejar o retardamento da execução do objeto;

21.1.6. não mantiver a proposta;

21.1.7. cometer fraude fiscal;

21.1.8. comportar-se de modo inidôneo;

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

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

21.4. O licitante/adjudicatário que cometer qualquer das infrações discriminadas nos subitens anteriores ficará sujeito, sem prejuízo da responsabilidade civil e criminal, e quando0 não houver disposição especifica no Termo de Referência, às seguintes sanções:

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

21.4.2. Multa de 10% (dez por cento) sobre o valor estimado do(s) item(s) prejudicado(s) pela conduta do licitante;

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

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

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

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

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

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

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

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

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

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

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

21.12. As penalidades serão obrigatoriamente registradas no SICAF.

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

22. DA IMPUGNAÇÃO AO EDITAL E DO PEDIDO DE ESCLARECIMENTO

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

22.2. A impugnação poderá ser realizada por forma eletrônica, pelo e-mail: licitacao@mdh.gov.br, ou por petição dirigida ou protocolada no endereço constante no preâmbulo deste Edital.

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

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

22.5. 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.

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

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

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

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

23. **DAS DISPOSIÇÕES GERAIS**

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

23.2. 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.

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

23.4. 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.

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

23.6. 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.

23.7. 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.

23.8. 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.

23.9. 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.

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

23.11. O Edital está disponibilizado, na íntegra, no endereço eletrônico https://www.gov.br/mdh/pt-br/acesso-a-informacao/licitacoes-e-contratos/mmfdh, e também poderão ser lidos e/ou obtidos no endereço descrito no preâmbulo deste Edital, nos dias úteis, no horário das 10:00 horas às 17:00 horas, mesmo endereço e período no qual os autos do processo administrativo permanecerão com vista franqueada aos interessados.

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

23.12.1. ANEXO I - Termo de Referência e seus anexos;

23.12.2. ANEXO II – Minuta de Termo de Contrato.

23.12.3. ANEXO III- Estudos Técnicos Preliminares

Brasília, 19 de dezembro de 2022

Assinatura da autoridade competente

Documento assinado eletronicamente por **Celiane Damascena Nunes**, **Coordenador(a), Substituto(a)**, em 19/12/2022, às 11:14, conforme horário oficial de Brasília, com fundamento no **§ 3º do art. 4º do Decreto nº 10.543, de 13 de novembro de 2020**.

A autenticidade deste documento pode ser conferida no site https://sei.mdh.gov.br/autenticidade, informando o código verificador **3329800** e o código CRC **8473D5A1**.

TERMO DE REFERÊNCIA

PROCESSO Nº 00135.214051/2021-24

1. DO OBJETO DA CONTRATAÇÃO

1.1. Contratação de Modernização da Solução de Balanceamento de Carga de Servidores e Solução de Segurança Web existente, incluindo renovação do suporte técnico e expansão do licenciamento, conforme condições, quantidades e exigências estabelecidas neste Termo de Referência e seus anexos.

2. DESCRIÇÃO DA SOLUÇÃO DE TIC

2.1. Bens e serviços que compõem a solução

Grupo	Item	Descrição	CATSER	Medida	Qtd.
1	1	Extensão do suporte técnico, licenciamento e atualização de versão da Solução de Balanceamento de Carga de Servidores e Solução de Segurança Web - F5 Networks BIG IP i2800 Best Bundle, por 36 meses	27740	Unid.	2
	2	Expansão do licenciamento da Solução de Balanceamento de Carga de Servidores e Solução de Segurança Web - módulo F5 BIG-IP Virtual Edition, com suporte técnico e atualização de versão por 36 meses	27502	Unid.	1

Tabela 1 - Relação dos serviços e bens

3. JUSTIFICATIVA PARA A CONTRATAÇÃO

3.1. Contextualização e Justificativa da Contratação

3.1.1. Um dos meios de comunicação utilizado pelo Ministério, tanto para fins institucionais quanto para relacionamento com a sociedade, é a internet. A utilização deste meio de comunicação requer um mecanismo de constante atualização tecnológica e segurança operacional, com a finalidade de assegurar a continuidade e a manutenção dos serviços prestados.

3.1.2. O presente processo visa a solução de balanceamento de Carga de Servidores e Segurança para as Aplicações Web do Ministério da Mulher, Família e dos Direitos Humanos - MMFDH. Tendo em vista a relevância das informações coletadas, é de extrema importância que a infraestrutura computacional do Ministério acompanhe as mudanças e atualizações necessárias. Além disso, o Ministério necessita também que a infraestrutura garanta estabilidade, segurança, alta-disponibilidade e agilidade na utilização e no armazenamento de dados.

3.1.3. Neste contexto, a Coordenação-Geral de Tecnologia da Informação (CGTI) é a unidade responsável por desenvolver, aperfeiçoar, manter e dar suporte aos sistemas informatizados e aos bancos de dados do MMFDH. A CGTI administra os recursos de informação, informática e telecomunicação do Ministério. Nesse aspecto, a Coordenação-Geral vem promovendo ações de melhoria na infraestrutura computacional do MMFDH, visando o melhor aproveitamento de hardware, software, serviços de rede. Além disso, CGTI tem promovido utilização de novas tecnologias, contando com a infraestrutura já disponível e em utilização, com ativos de rede, balanceamento de carga, segurança de rede e infraestrutura de servidores de computação. A ampliação desta infraestrutura, tanto em nível de hardware quanto software, garante a robustez e a estabilidade dos serviços do MMFDH.

3.1.4. A infraestrutura do MMFDH, do cabeamento físico aos servidores de aplicações, está em contínua evolução. Esta evolução tem como principal objetivo o contínuo aumento do acesso público aos serviços e às informações prestadas pelo órgão. Além do quesito desempenho, considera-se também a necessidade de melhorias na segurança de TI, que acompanham a evolução das tecnologias. Os ataques ao ambiente tecnológico do Ministério da Mulher, Família e dos Direitos Humanos - MMFDH, estão cada vez mais sofisticados e, caso não houvesse atualização das proteções, desempenho dos serviços prestados à sociedade seriam impactados. Esses ataques ocorrem constantemente e, muita vezes, em momentos críticos para o Ministério.

3.1.5. A introdução de novos sistemas ou migração adequação atualização de sistemas legados, deve ser feito de forma a evitar problemas de lentidão e indisponibilidade da infraestrutura. Deixar os sistemas computacionais indisponíveis é um grande risco para as atividades desenvolvidas por qualquer órgão da Administração Pública.

3.1.6. Com os sistemas cada vez mais 'online' e usuários acessando uma infinidade de aplicativos Web ou remotos, a implementação de controles e políticas de segurança da informação tornam-se ainda mais essenciais. O

MMFDH necessita estar atento aos ataques e possíveis incidentes que visam prejudicar a sua rede tecnológica, e utilizando as tecnologias mais atuais para proteção e segurança dos dados.

3.1.7. Nos últimos anos a demanda por serviços disponibilizados pelo MMFDH através da Internet cresceu exponencialmente. Foram criadas também novas aplicações e sistemas utilizados pela sociedade. Esse fato gerou a necessidade de expansão do parque tecnológico do Ministério. Operacionalmente foram criados diversos servidores de aplicação que direcionados a atender o público externo. Com isso, surgiu a necessidade de adquirir equipamentos de balanceamento de carga. Esse equipamento, irá a balancear todas as aplicações nos diversos servidores criados, melhorando o desempenho, além propiciar diversas camadas de segurança para proteção dos ativos de informação.

3.1.8. No passado, o Ministério adquiriu clusters de balanceamento de carga de alto desempenho, que ainda estão sendo utilizados. Essa solução garante a distribuição uniforme da carga de conexões geradas pelos usuários dos sistemas, proporcionando otimização de recursos, maximização de desempenho e minimização do tempo de resposta. Além disso, ele permite a transmissão e a recepção apenas de dados autorizados, evitando acessos indevidos.

3.1.9. As contratações dos produtos relacionados aos balanceadores de carga venceram no final do ano de 2019, incluindo as vigências das garantias, licenciamentos e suporte técnico especializado. Um aditivo contratual permitiu estender o suporte técnico especializado e a garantia do produto em 36 meses, vencendo em 13/12/2021. A não atualização desses itens irá impedir a abertura de chamados e resolução de problemas de software e de hardware. Em consequência, há risco de indisponibilidade da solução e todos as aplicações Web dependentes.

3.1.10. Neste contexto, demonstra-se a necessidade de garantir a continuidade do balanceamento de carga e da segurança provida pela solução às aplicações.

3.1.11. A presente aquisição pretende contemplar atualização de licenças de uso, garantia para os equipamentos e suporte técnico especializado que consiste em suporte técnico preventivo e corretivo do Ministério sem que haja pausa ou interrupção na proteção, requalificação dos analistas e técnicos do MMFDH já capacitados.

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

3.2.1. A aquisição pretendida atenderá aos seguintes objetivos estratégicos:

Objetivos Estratégicos - CICLO 2019 - 2023 (SEI 2396898 e 2396900) Fonte: https://www.gov.br/mdh/pt-br/acesso-a-informacao/governanca/planejamento-estrategico	
ID	**Objetivos Estratégicos**
P1	Assegurar transparência e sistematização de informações para o aperfeiçoamento de políticas de direitos humanos
A3	Prover recursos orçamentários, financeiros e tecnológicos de forma eficiente
A4	Buscar a inovação dos serviços e processos com foco na simplificação, eficiência e melhoria da qualidade

Estratégia de Governo Digital - 2020 a 2022 Fonte: https://www.gov.br/governodigital/pt-br/EGD2020	
Objetivo 11	Garantia da segurança das plataformas de governo digital e de missão crítica
Iniciativa 11.1	Garantir, no mínimo, 99% de disponibilidade das plataformas compartilhadas de governo digital, até 2022.
Iniciativa 11.3	Definir padrão mínimo de segurança cibernética a ser aplicado nos canais e nos serviços digitais, até 2022.

ALINHAMENTO AO PDTIC 2022-2023 (SEI 2838829) Fonte: https://www.gov.br/mdh/pt-br/acesso-a-informacao/tecnologia-da-informacao			
ID	**Ação do PDTIC**	**ID**	**Meta do PDTIC associada**
A078	EQUIPAMENTO SEGURANÇA REDE	M07	- Aprimorar a Segurança Física e do Ambiente quanto ao Controle do Acesso, Armazenamento e Disponibilidade da informação

ALINHAMENTO AO PAC 2022 (SEI 2648557) Fonte: https://www.gov.br/mdh/pt-br/acesso-a-informacao/licitacoes-e-contratos/pac-2022	
Item	**Descrição**
310	EQUIPAMENTO SEGURANÇA REDE

3.3. **Estimativa da demanda**

3.3.1. Apresenta-se a seguir o quadro contendo a solução a ser contemplada com a contratação proposta.

3.3.2. O Estudo Técnico Preliminar da Contratação DIVPRO (SEI nº 3094781) realizado indicou qual forma de contratação melhor atenderia à demanda, do ponto de vista técnico-econômico.

3.3.3. Existe hoje em pleno e efetivo funcionamento no Ministério a chamada Solução de Balanceamento de Carga de Servidores e Solução de Segurança Web - F5 Networks BIG IP, contratada por intermédio do Contrato n° 35/2018.

3.3.4. O item 2 do quadro indica a necessidade de expansão das funcionalidades em uso, haja vista a evolução tecnológica ocorrida desde a formalização do Contrato n° 35/2018, ocorrida no segundo semestre do ano 2018, além da necessidade de uso em outro unidade física do MMFDH (em TIC o termo SITE).

GRUPO	ITEM	DESCRIÇÃO	QTD.
1	1	Extensão do suporte técnico, licenciamento e atualização de versão da Solução de Balanceamento de Carga de Servidores e Solução de Segurança Web - F5 Networks BIG IP i2800 Best Bundle, por 36 meses	2
	2	Expansão do licenciamento da Solução de Balanceamento de Carga de Servidores e Solução de Segurança Web - módulo F5 BIG-IP Virtual Edition, com suporte técnico e atualização de versão por 36 meses	1

Tabela 2 - Estimativa da contratação

3.4. **Relação da quantidade estimada x quantidade necessária**

3.4.1. O quantitativo proposto para contratação foi definido estritamente com base no Contrato n° 35/2018 (2 Appliances da Solução já existente), bem como na necessidade de atualização tecnológica que permita, por exemplo, contemplar a funcionalidades de segurança, desempenho, disponibilidade e abordagem a ameaças avançadas nos serviços de nuvem. Para essa atualização tecnológica, uma única unidade é suficiente para atendimento das necessidades técnicas durante o prazo estimado para vigência contratual.

3.5. **Parcelamento da Solução de TIC**

3.5.1. O agrupamento e adjudicação em Grupo é lícito, “desde que os lotes sejam integrados por itens de uma mesma natureza e que guardem relação entre si" (Acórdão TCU 5.260/2011-1ª Câmara). É certo que, conforme disserta o Acórdão TCU n° 861/2013, o “aumento da eficiência administrativa do setor público passa pela otimização do gerenciamento de seus contratos de fornecimento. Essa eficiência administrativa também é de estatura constitucional e deve ser buscada pela administração pública”.

3.5.2. Ao se admitir diversos fornecedores, além da perda de uniformidade e padronização da solução, corre-se o risco de haver descompasso no fornecimento dos itens, além da elevação da complexidade dos procedimentos de gestão contratual.

3.5.3. Além disso, em consequência do grande vínculo existente entre as funções que fazem parte do escopo dos serviços, caso sejam fracionados, corre-se o risco de haver equipes distintas pouco integradas, podendo ocasionar danos à operação de TIC do MMFDH, haja vista que, como serviços de missão crítica, qualquer interrupção ou incidente que comprometa a sua efetiva continuidade pode causar sérios prejuízos a este Ministério, com a efetiva continuidade dos serviços prestados a sociedade.

3.5.4. Desse modo, avaliando as características do objeto pretendido neste Termo de Referência, consideramos que o agrupamento da pretensão contratual é técnica e economicamente viável sendo que sua divisão pode prejudicar o conjunto do objeto, além de gerar outros custos relacionados à coexistência de diversos contratos, potencializando riscos e dificuldades na gestão técnica e administrativa de uma pluralidade de contratos autônomos.

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

3.7. O intuito principal da contratação é:

a) Satisfação dos clientes e usuários de serviço de TIC.

b) Infraestrutura de TIC adequada para suportar os serviços providos.

c) Continuidade dos serviços e ferramentas utilizadas pelos usuários do Órgão.

d) Disponibilidade, manutenção e suporte do licenciamento existente.

e) Segurança dos equipamentos servidores, seus componentes e de suas aplicações.

f) Integridade dos dados e informações disponibilizadas.

g) Aprimoramento da camada de proteção contra fraudes e ameaças digitais.

3.8. **Da participação de consórcio**

3.8.1. Pela natureza e baixa complexidade do objeto, não será permitida a participação de licitantes em consórcio no certame, além de que, a própria natureza do objeto e o vulto da licitação, por si só, já justificam tal vedação.

3.8.2. A participação de empresas em consórcio, trata-se de escolha discricionária da Administração Pública, o que evidentemente não significa autorização para decisões arbitrárias ou imotivadas.

3.8.3. Assim, compete-nos justificar que, via de regra, prevalece a vedação à participação dos consórcios em licitações em que o objeto for comum, simples e de pequena monta; a opção da Administração por vedar ou permitir a participação de empresas reunidas em consórcio na licitação deve ter como parâmetro a conjugação de elementos como vulto, dimensão e complexidade, devendo ser assegurada no caso concreto a ampla competitividade no certame.

3.8.4. O objeto em exame, embora possua valor significativo, está bem abaixo daquele valor considerado de grande vulto, definido no Art. 6º, Inciso I, da Lei 8.666/93, cujo valor estimado seja superior a 25 (vinte e cinco) vezes o limite estabelecido na alínea "c" do inciso I do art. 23 desta Lei, além do objeto não esbarrar em questões de **maior complexidade técnica**, não se justificando, de fato, a necessidade de formação de consórcios entre empresas para que o interesse público seja alcançado.

3.8.5. A ausência de consórcio não trará prejuízos à competitividade do certame, visto que, em regra, a formação de consórcios é admitida quando o objeto a ser licitado envolve questões de alta complexidade ou de relevante vulto, em que empresas, isoladamente, não teriam condições de suprir os requisitos de habilitação do edital. Nestes casos, a Administração, com vistas a aumentar o número de participantes, admite a formação de consórcio.

4. ESPECIFICAÇÃO DOS REQUISITOS DA CONTRATAÇÃO

4.1. Requisitos de Negócio

4.1.1. Atender às necessidades no Ministério para o serviço de suporte técnico e garantia por empresa especializada, contemplando a solução de tratamento e entrega de dados do MMFDH:

4.1.2. Garantir o acesso seguro aos recursos de Tecnologia da Informação para a prestação de serviços digitais do MMFDH.

4.1.3. Prover acesso seguro aos sistemas administrativos e corporativos utilizados pelo MMFDH (SEI, correio eletrônico, Internet, dentre outros) para o desempenho de suas funções.

4.1.4. Prover acesso de boa qualidade aos recursos providos externamente a rede do MMFDH através do tratamento e melhor utilização da capacidade oferecida pelos links de internet.

4.1.5. Prover acesso de boa qualidade priorizando o tráfego das aplicações classificadas como essenciais para alcançar os objetivos primários do Órgão.

4.1.6. O Suporte deverá ser especializado, podendo ser executado remotamente ou localmente dependendo da criticidade. A avaliação do chamado quanto a criticidade será feita pelo Ministério;

4.1.7. A documentação produzida durante a execução dos serviços, seja em papel ou meio eletrônico, será de propriedade do MMFDH e não deverá ser divulgado sem sua expressa autorização.

4.2. Requisitos de Capacitação

4.2.1. A documentação técnica deverá garantir a transferência de conhecimento à CONTRATANTE, a fim de proporcionar o nível de informação necessário à operação da solução e possíveis intervenções.

4.3. Requisitos Legais

4.3.0.1. Lei Federal nº 8.666/1993: Institui normas para licitações e contratos da Administração Pública e dá outras providências;

4.3.0.2. Lei Federal nº 10.520/2002: Institui no âmbito da União, Estados, Distrito Federal e Municípios, modalidade de licitação denominada pregão, para aquisição de bens e serviços comuns, e dá outras providências;

4.3.0.3. 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;

4.3.0.4. Decreto nº 7.174/2010: Regulamenta a contratação de bens e serviços de informática e automação pela administração pública federal;

4.3.0.5. Decreto nº 10.222 de 5 de fevereiro de 2020: A presente Estratégia Nacional de Segurança Cibernética - E-Ciber é orientação manifesta do Governo federal à sociedade brasileira sobre as principais ações por ele pretendidas, em termos nacionais e internacionais, na área da segurança cibernética e terá validade no quadriênio 2020-2023.

4.3.0.6. Decreto nº 9.637, de 26 de dezembro de 2018: Institui a Política Nacional de Segurança da Informação, dispõe sobre a governança da segurança da informação, e altera o Decreto nº 2.295, de 4 de agosto de 1997, que regulamenta o disposto no art. 24, caput, inciso IX, da Lei nº 8.666, de 21 de junho de 1993, e dispõe sobre a dispensa de licitação nos casos que possam comprometer a segurança nacional.

4.3.0.7. Instrução Normativa SGD/ME nº 01/2019: 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;

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

4.4. Requisitos de serviço de instalação e configuração.

4.4.1. Contemplar instalação e configuração na aquisição da solução, a fim de mantê-los em plenas condições de uso no início da vigência contratada. Exigir que o conhecimento da operação da solução seja repassado à equipe do MMFDH que irá executar atividades relacionadas aos produtos contratados.

4.5. **Requisitos Temporais**

4.5.1. A entrega das licenças deverá ocorrer em até 5 (cinco) dias úteis, contados da data da emissão de Ordem de Serviços - OS por parte da CONTRATANTE.

4.5.2. Caso se veja impossibilitada de cumprir com o prazo estipulado no item anterior, a empresa CONTRATADA deverá, por escrito, solicitar prorrogação do prazo e apresentar justificativas.

4.5.3. O pedido de prorrogação, com indicação do novo prazo, quando for o caso, deverá ser encaminhado à fiscalização do CONTRATANTE, que poderá, de modo justificado, acolher ou não o pedido. Vencidos os prazos de entrega ou de prorrogação e não cumprida a obrigação de entrega, o CONTRATANTE oficiará a empresa CONTRATADA acerca do transcurso da data limite, passando o inadimplemento, sendo aplicáveis as sanções previstas no Termo de Referência e demais instrumentos legais.

4.5.4. Não há necessidade de fornecimento de mídias físicas para o licenciamento a ser adquirido.

4.5.5. As licenças e chaves de ativação necessárias deverão ser enviadas via protocolo e compor a documentação de entrega, após emissão de OS . Somente será considerado entregue após confirmação de recebimento pela CONTRATANTE.

4.5.6. As licenças fornecidas deverão estar cobertas por garantia integral pelo período mínimo de 36 (trinta e seis) meses a contar da data do recebimento.

4.5.7. Problema no licenciamento, caso comprovado, deverá ser sanado dentro dos tempos estipulados. Quando não for possível solucionar o problema no prazo estipulado, caso autorizado pela Contratante, deverá ser fornecido outra licença de igual configuração ou superior, até resolução definitiva do problema.

4.5.8. Considerando que os recursos fornecidos pela solução a ser contratada são imprescindíveis à execução diária das atividades deste Ministério e que, se paralisados, podem pôr em risco a continuidade das atividades da Administração, não se mostra sensato exigir que sua vigência fique limitada a 12 (doze) meses, já que a prática administrativa é de prorrogar contratos desta natureza pelo período máximo permitido em lei (60 meses). Portanto, é notável a vantagem para a Administração Pública adotar vigência superior a 12 (doze)meses para serviços de natureza continua, uma vez que o interesse real é de contratá-los por maior período. Dessa maneira, além de permitir maior competitividade, reduz os custos administrativos e mitiga os riscos de indisponibilidade dos serviços de TIC por problemas que possam surgir nos processos de renovações contratuais.

4.5.9. Assim, a vigência da contratação é de 36 (trinta e seis) meses a partir da data de assinatura do contrato, prorrogável na forma do art. 57, § 1°, da Lei n° 8.666/93.

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

4.6.1. Aumentar o nível de segurança da operação de tecnologia do Contratante;

4.6.2. O serviço terá a participação e cooperação da Área de TI do Contratante durante toda a duração do contrato;

4.6.3. A Contratada irá prestar auxílio à equipe de Segurança da Informação do Contratante no suporte direto à solução contratada.

4.6.4. Todos os profissionais devem ser credenciados junto à Contratante, para que sejam autorizados a retirar e a entregar documentos, bem como prestar serviços em qualquer dependência da Contratante;

4.6.5. A Contratada deverá observar e respeitar, rigorosamente, todas as normas e procedimentos de segurança implementados no ambiente de Tecnologia da Informação do MMFDH, assim como as suas atualizações;

4.6.6. Deve ser mantido sigilo sobre todos os ativos de informações e de processos que se refiram ao Contratante, conforme TERMO DE COMPROMISSO e TERMO DE CIÊNCIA, que comporão o presente processo;

4.6.7. A Contratada não poderá divulgar quaisquer informações a que tenha acesso em virtude dos trabalhos a serem executados ou de que tenha tomado conhecimento em decorrência da execução do objeto, sem autorização, por escrito, da Contratante, sob pena de aplicação das sanções cabíveis;

4.6.8. Observância às diretrizes estabelecidas pela Política de Segurança da Informação e Comunicações do Contratante e demais normas sobre o assunto, no que couber.

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

4.7.1. É dever da Contratada observar entre outras: o menor impacto sobre recursos naturais como flora, fauna, ar, solo e água; preferência para materiais, tecnologias e matérias-primas de origem local; maior eficiência na utilização de recursos naturais como água e energia; maior geração de empregos, preferencialmente com mão de obra local; maior

vida útil e menor custo de manutenção do bem e da obra; uso de inovações que reduzam a pressão sobre recursos naturais; e origem ambientalmente regular dos recursos naturais utilizados nos bens, serviços e obras. O ambiente físico da Contratada para fins de execução do serviço deve ser compatível com o disposto na NR17 do Ministério do Trabalho e Emprego – MTE e na recomendação técnica DSST nº 01/2005 do Ministério do Planejamento, Desenvolvimento e Gestão, no que couber.

4.7.2. O objeto a ser contratado deve estar adequado a Política Nacional de Resíduos Sólidos (PNRS), Lei Nº 12.305/2010, foi aprovada em agosto de 2010, dispondo sobre seus princípios, objetivos e instrumentos, bem como sobre as diretrizes relativas à gestão integrada e ao gerenciamento de resíduos sólidos, incluindo os perigosos, às responsabilidades dos geradores e do poder público e aos instrumentos econômicos aplicáveis, no que couber.

4.8. **Requisitos de Arquitetura Tecnológica**

4.8.1. Não aplicável a esta contratação.

4.9. **Requisitos de Garantia e Assistência Técnica**

4.9.1. A garantia, o Suporte e a Manutenção funcionarão de acordo com o item “Suporte Técnico da Contratada, Manutenção e Garantia da Solução” estabelecido no ANEXO I - Especificações Técnicas da Solução deste Termo de Referência.

4.10. **Requisitos de Experiência Profissional**

4.10.1. Os profissionais da Contratante deverão ser certificados na solução tecnológica.

4.11. **Requisitos de Formação da Equipe**

4.11.1. No âmbito da solução os serviços deverão ser supervisionados por pelo menos um especialista da Contratada certificado pelo fabricante na solução ofertada.

4.12. **Requisitos de Metodologia de Trabalho**

4.12.1. Os serviços serão executados de forma indireta por meio da Contratada e mensurados os resultados pelo Contratante.

4.12.2. As demandas para entrega das licenças e para transferência de conhecimento serão formalizadas pelo Contratante mediante Ordem de Serviço - OS.

4.12.3. Os serviços de suporte técnico independem de formalização de demanda pelo Contratante, e deverão ter início imediatamente à emissão do Termo de Recebimento Definitivo das licenças.

4.13. **Outros Requisitos Aplicáveis**

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

5. **RESPONSABILIDADES**

5.1. **Deveres e responsabilidades da CONTRATANTE**

a) A contratante deverá se alinhar aos dispositivos previstos na Instrução Normativa SGD-ME nº 1, de 4 de abril de 2019, no tocante a todas as etapas do processo de compra, desde o planejamento (que deve incluir o Documento de Oficialização da Demanda e o Estudo Técnico Preliminar) até a etapa de execução, gestão e fiscalização do contrato, atentando para a devida instrução processual;

b) Instruir os autos do processo administrativo, físico ou eletrônico, com os documentos afetos ao recebimento provisório e definitivo dos bens, tais como: termo de recebimento provisório (TRP) e definitivo (TRD), devidamente assinados pelo gestor do contrato; metodologia adotada no recebimento definitivo dos bens, contendo a definição da amostra ou a totalidade dos itens a serem testados e inspecionados (exame qualitativo); resultados dos testes de atendimento aos critérios de aceitação e das verificações de conformidade aplicados em cada equipamento avaliado;

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

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

e) Exigir o cumprimento de todas as obrigações assumidas pela CONTRATADA, de acordo com as cláusulas contratuais avençadas;

f) Providenciar as assinaturas pela CONTRATADA no Termo de Compromisso de Manutenção de Sigilo e Respeito às Normas de Segurança e no Termo de Ciência da Declaração de Manutenção de Sigilo;

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

h) Prestar as informações e esclarecimentos relativos ao objeto desta contratação que venham a ser solicitado pelo preposto da CONTRATADA;

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

j) Encaminhar formalmente a demanda por meio de Ordem de Serviço - OS, de acordo com os critérios estabelecidos neste Termo de Referência;

k) Aplicar à contratada as sanções administrativas regulamentares e contratuais cabíveis.

l) Acompanhar e fiscalizar o cumprimento das obrigações da CONTRATADA, por intermédio de servidor especialmente designado, anotando em registro próprio as falhas detectadas, indicando dia, mês e ano, bem como o nome dos empregados eventualmente envolvidos, e encaminhando os apontamentos à autoridade competente para as providências cabíveis;

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

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

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

p) Atestar as notas fiscais/faturas desde que tenham sido entregues como determina este Termo de Referência, verificar os relatórios apresentados, encaminhar as notas fiscais e/ou faturas, devidamente atestadas, para pagamento no prazo determinado.

q) Efetuar o pagamento à CONTRATADA no valor correspondente ao fornecimento do objeto, de acordo com as condições contratuais, no prazo e condições estabelecidas neste Termo de Referência, e no caso de cobrança indevida, glosar os valores considerados em desacordo com o contrato.Efetuar as retenções tributárias devidas sobre o valor da Nota Fiscal/Fatura da contratada, no que couber, em conformidade com o item 6 do Anexo XI da IN SEGES/MP n°. 5/2017;

r) Não praticar atos de ingerência na administração da CONTRATADA, tais como:

- exercer o poder de mando sobre os empregados da CONTRATADA, devendo reportar-se somente aos prepostos ou responsáveis por ela indicados, exceto quando o objeto da contratação previr o atendimento direto, tais como nos serviços de recepção e apoio ao usuário;
- direcionar a contratação de pessoas para trabalhar nas empresas contratadas;
- considerar os trabalhadores da CONTRATADA como colaboradores eventuais do próprio órgão ou entidade responsável pela contratação, especialmente para efeito de concessão de diárias e passagens;

s) Fornecer por escrito as informações necessárias para o desenvolvimento do objeto do contrato;

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

u) Fiscalizar o cumprimento dos requisitos legais, quando a CONTRATADA houver se beneficiado da preferência estabelecida pelo art. 3º, § 5º, da Lei nº 8.666, de 1993;

v) Liquidar o empenho e efetuar o pagamento à CONTRATADA, dentro dos prazos preestabelecidos em contrato;

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

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

5.2. **Deveres e responsabilidades da CONTRATADA**

a) 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;

b) Efetuar a entrega do objeto em perfeitas condições, conforme especificações e prazo constante no Termo de Referência e seus anexos e no local na Ordem de Serviço - OS, acompanhado da respectiva nota fiscal, na qual constarão as indicações referentes a: *marca, fabricante, modelo, procedência e prazo de garantia ou validade;*

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

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

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

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

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

g) Executar o objeto do certame em estreita observância dos ditames estabelecido pela Lei nº 13.709, de 14 de agosto de 2018 (Lei Geral de Proteção de Dados Pessoais - LGPD). A CONTRATADA deverá disponibilizar em até 10 (dez) dias úteis da assinatura do contrato, preferencialmente, em sítio eletrônico as informações referentes ao encarregado da credenciada responsável pela proteção de dados em relação ao objeto deste Termos de Referência, nos termos do art. 41 da Lei nº 13.709, de 2018.

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

i) Fornecer e utilizar os materiais e equipamentos, ferramentas e utensílios necessários, na qualidade e quantidade adequadas especificadas neste Termo de Referência e em sua proposta;

j) Entregar os equipamentos nos endereços vinculados aos CNPJs da CONTRATANTE, conforme as OSs;

k) Utilizar empregados habilitados e com conhecimentos básicos dos serviços a serem executados, em conformidade com as normas e determinações em vigor;

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

m) 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;

n) Prestar as informações e os esclarecimentos que venham a ser solicitados pela CONTRATANTE por intermédio de preposto designado para acompanhamento do contrato nos seguintes prazos, a contar de sua solicitação:

- em até 2 dias úteis nas capitais; e
- em até 4 dias úteis nas demais localidades;

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

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

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

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

r) Atender prontamente quaisquer orientações e exigências da Equipe de Fiscalização do Contrato, inerentes à execução do objeto contratual;

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

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

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

u) Responsabilizar-se pelos vícios e danos decorrentes do fornecimento dos equipamentos e prestação dos serviços de suporte e garantia, bem como por todo e qualquer dano causado à União ou à entidade federal, devendo ressarcir imediatamente a Administração em sua integralidade, resguardado o devido processo legal, ficando a CONTRATANTE autorizada a descontar da garantia, caso exigida no edital, ou dos pagamentos devidos à CONTRATADA, o valor correspondente aos danos sofridos.

v) Reparar quaisquer danos diretamente causados à CONTRATANTE ou a terceiros por culpa ou dolo de seus representantes legais, prepostos ou empregados, em decorrência da relação contratual, não excluindo ou reduzindo a responsabilidade da fiscalização ou o acompanhamento da execução dos serviços pela CONTRATANTE;

w) Propiciar todos os meios necessários à fiscalização do contrato pela CONTRATANTE, cujo o Gestor do contrato terá poderes para sustar o fornecimento, total ou parcial, em qualquer tempo, sempre que considerar a medida necessária e desde que motivadas as causas e justificativas desta decisão;

x) Acatar as orientações da CONTRATANTE, sujeitando-se à mais ampla e irrestrita fiscalização, prestando os esclarecimentos solicitados e atendendo as reclamações formuladas;

y) Prestar esclarecimentos à CONTRATANTE sobre eventuais atos ou fatos noticiados que se refiram à CONTRATADA, independente de solicitação;

z) Comunicar à CONTRATANTE, por escrito, qualquer anormalidade e prestar os esclarecimentos julgados necessários;

aa) Sujeitar-se aos acréscimos e supressões contratuais estabelecidos na forma do art. 65 da Lei n° 8.666/93, quais sejam, alterações quantitativas do contrato de acréscimos ou supressões que se fizerem necessários, até o limite de 25% (vinte e cinco por cento) do valor atualizado do contrato.

ab) Não veicular publicidade ou qualquer outra informação acerca da prestação dos serviços do contrato, sem prévia autorização da CONTRATANTE;

ac) Não fazer uso das informações prestadas pela CONTRATANTE para fins diversos do estrito e absoluto cumprimento do contrato em questão;

ad) Responder, integralmente, por perdas e danos que vier a causar à CONTRATANTE ou a terceiros em razão de ação ou omissão, dolosa ou culposa, sua ou de prepostos, independentemente de outras cominações contratuais ou legais a que estiver sujeita; e

ae) Cumprir outras obrigações que se apliquem, de acordo com o objeto da contratação.

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

5.3.1. Não se aplica.

6. **MODELO DE EXECUÇÃO DO CONTRATO**

6.1. **Rotinas de Execução do Contrato**

6.1.1. **Da inicialização do contrato**

6.1.1.1. Após a assinatura do Contrato e a nomeação do Gestor e Fiscais do Contrato, será realizada a Reunião Inicial de alinhamento com o objetivo de nivelar os entendimentos acerca das condições estabelecidas no Contrato, Edital e seus anexos, e esclarecer possíveis dúvidas acerca da execução dos serviços, a qual ocorrerá nas dependências do Ministério, em Brasília/DF ou de forma remota.

6.1.1.2. A reunião será realizada em conformidade com o previsto no inciso I do Art. 31 da IN SGD-ME nº 01/2019 e ocorrerá em até 10 (dez) dias úteis da nomeação do Gestor e Fiscais do Contrato, podendo ser prorrogada a critério da CONTRATANTE.

6.1.1.3. A pauta desta reunião observará, pelo menos:

a) Apresentação do Preposto da empresa pelo representante legal da Contratada. A Carta de apresentação do Preposto deverá conter no mínimo o nome completo e CPF do funcionário da empresa designado para acompanhar a execução do contrato e atuar como interlocutor principal junto à CONTRATANTE, incumbido de receber, diligenciar, encaminhar e responder as principais questões técnicas, legais e administrativas referentes ao andamento contratual.

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

6.1.2. **Ordem de Serviço**

6.1.2.1. A execução dos serviços será condicionada à abertura e autorização prévia de ordem de serviço (OS) emitida pelo sistema próprio de gestão de demandas da Contratante, que também controlará prazos, quantidades e produtos/serviços a serem entregues.

6.1.2.2. As OS registrarão as etapas, os prazos, o detalhamento dos serviços, as atividades previstas, os padrões a serem seguidos, os produtos a serem entregues, o custo estimado, bem como demais informações técnicas necessárias para a execução dos serviços por parte da Contratada.

6.1.2.3. Após aprovação das demandas, o Gestor do Contrato encaminhará a OS para a Contratada, bem como as informações necessárias para sua execução.

6.1.2.4. Cada demanda deverá ser executada atendendo as especificações, de acordo com a arquitetura, aspectos metodológicos, estrutura, padrões e melhores práticas, além das que constarem da OS.

6.1.2.5. Será gerada OS complementar sempre que houver alguma alteração na OS original. Portanto, não serão aceitas justificativas para não cumprimento de prazos devido a alterações no escopo da OS.

6.1.2.6. Uma OS poderá ser suspensa por decisão do usuário gestor, do gestor do contrato ou de um dos fiscais técnicos do contrato. Nesse momento, os prazos serão suspensos e redefinidos, caso a OS seja retomada.

6.1.2.7. No cancelamento de uma OS, deverá ser apurado o serviço já realizado e discutido com o gestor do contrato a forma de faturamento, se necessário.

6.1.3. Os produtos serão recebidos nas condições abaixo:

6.1.4. **Provisoriamente**, no prazo de 5 dias úteis, por meio de servidores designados para este fim, no ato da entrega, para verificação da conformidade, qualidade e quantidade dos produtos e, mediante a emissão do TERMO DE RECEBIMENTO PROVISÓRIO (modelo disponível no em https://www.gov.br/governodigital/pt-br/contratacoes/templates-e-listas-de-verificacao - Termo de Recebimento Provisório (atualizado em 24/05/2021).

6.1.5. Após o recebimento provisório, caso se constaste que a entrega dos produtos ocorreu em desacordo com o especificado neste Termo de Referência, com defeito ou incompleto, posteriormente a notificação por escrito à empresa, serão interrompidos os prazos de recebimento até que sejam substituídos os produtos e/ou componentes. Sendo que as despesas relativas à substituição dos produtos/componentes correrão às expensas da Contratada.

6.1.6. A Contratada deverá substituir às suas expensas os equipamentos rejeitados no prazo de 30 (trinta) dias corridos, sob pena de incorrer em sanções legais cabíveis, garantida a ampla defesa.

6.1.7. **Definitivamente**, no prazo de até 20 (vinte) dias corridos, contados a partir do registro do recebimento provisório, após a verificação da conformidade qualitativa e quantitativa dos produtos e sua consequente aceitação pela Comissão ou servidor designado, mediante a emissão do TERMO DE RECEBIMENTO DEFINITIVO (modelo disponível no em https://www.gov.br/governodigital/pt-br/contratacoes/templates-e-listas-de-verificacao - Termo de Recebimento Definitivo (atualizado em 24/05/2021).

6.1.8. Os serviços poderão ser rejeitados, no todo ou em parte, quando em desacordo com as especificações constantes neste Termo de Referência e na proposta, devendo ser substituídos no prazo de 15 (quinze) dias úteis, a contar da notificação da contratada, às suas custas, sem prejuízo da aplicação das penalidades. Ainda, conforme o art. 69 da Lei 8.666/1993, a CONTRATADA é obrigada a reparar, corrigir, remover, reconstruir ou substituir, às suas expensas, no total ou em parte, o objeto do contrato em que se verificarem vícios, defeitos ou incorreções resultantes da execução ou de materiais empregados.

6.1.9. A inserção das informações referidas no item acima deverá ser comprovada por ocasião da apresentação da cobrança, sendo esta uma condição para o pagamento.

6.1.10. De posse da documentação comprobatória da entrega, o Fiscal do Contrato encaminhará a documentação de cobrança para o setor responsável pelo pagamento, incluindo relatórios de entrega do sistema informatizado.

6.1.11. Caso sejam verificadas irregularidades que impeçam a liquidação e o pagamento da despesa, o GESTOR DO CONTRATO deve indicar as cláusulas contratuais pertinentes, solicitando à contratada, por escrito, as respectivas medidas de correção.

6.1.12. Serão aceitos para fins de emissão de Termo de Recebimento Definitivo:

a) a solução fornecida que atendam à configuração mínima descrita neste termo de referência e que estejam em funcionamento de acordo com as condições estabelecidas neste Termo de Referência.

6.1.13. Só haverá o recebimento definitivo, após a análise da qualidade dos serviços, em face da aplicação dos critérios de aceitação, resguardando-se ao CONTRATANTE o direito de não receber o OBJETO cuja qualidade seja comprovadamente baixa ou em desacordo com as especificações definidas neste Termo de Referência – situação em que poderão ser aplicadas à CONTRATADA as penalidades previstas em lei, neste Termo de Referência e no CONTRATO. Quando for o caso, a empresa será convocada a refazer todos os serviços rejeitados, sem custo adicional.

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

6.1.15. O pagamento observará o disposto na seção 7.5 deste Termo de Referência.

6.2. **Do controle e fiscalização do contrato**

6.2.1. Nos termos do art. 67 Lei nº 8.666, de 1993, será designado representante para acompanhar e fiscalizar a entrega, anotando em registro próprio todas as ocorrências relacionadas com a execução e determinando o que for necessário à regularização de falhas ou defeitos observados.

6.2.2. O recebimento da solução no valor superior a R$ 176.000,00 (cento e setenta e seis mil reais) será confiado a uma comissão de, no mínimo, 3 (três) membros, designados pela autoridade.

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

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

6.3. **Quantidade mínima da solução para comparação e controle**

6.3.1. Cada OS conterá a quantidade a ser fornecida, incluindo a sua localização e o prazo, conforme definições deste TR.

6.4. **Mecanismos formais de comunicação**

6.4.1. São mecanismos formais de comunicação entre a Contratada e a Contratante:

a) E-mails: forma rápida de comunicação para tratar de informações pouco críticas;

b) Ofícios: Comunicação para tratar de assuntos gerais;

c) Ordem de Serviço: elaborada, por demanda, pela Contratante e encaminhada à Contratada, com a função de demandar serviços contratados;

d) Termo de Recebimento Provisório: termo elaborado pela Contratante e encaminhado à Contratada;

e) Termo de Recebimento Definitivo: termo elaborado pela Contratante e encaminhado à Contratada; e

f) Toda a comunicação entre a Administração Pública e a Contratada deverá ser sempre formal como regra, exceto em casos excepcionais que justifiquem outro canal de comunicação.

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

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

6.5.2. O **Termo de Compromisso**, contendo declaração de manutenção de sigilo e respeito às normas de segurança vigentes na entidade, a ser assinado pelo representante legal da Contratada; e **Termo de Ciência**, a ser

assinado por todos os empregados da Contratada diretamente envolvidos na contratação, encontram-se nos ANEXOS deste TR.

7. MODELO DE GESTÃO DO CONTRATO

7.1. Critérios de Aceitação

7.1.1. Todo e qualquer fornecimento se dará mediante demanda da Contratante, situação em que será emitida a Ordem de Serviços - OS.

7.1.2. Os serviços serão executados nos locais e endereços descritos nas Ordens de Serviço.

7.1.3. Os serviços que compõem a solução serão recebidos:

7.1.4. A Administração rejeitará, no todo ou em parte, a entrega dos serviços em desacordo com as especificações técnicas exigidas.

7.1.5. A recusa parcial ou total no atendimento de uma OS emitida, será oficiada à Contratada pela Contratante, que deverá prontamente prestar o serviço de acordo com o estabelecido na respectiva Ordem de Serviço;

7.1.6. A aceitação definitiva dar-se-á após a assinatura do termo de recebimento definitivo, correspondente a cada Ordem de serviço.

7.2. Procedimentos de Teste e Inspeção

7.2.1. Os serviços serão recebidos após a verificação do atendimento dos Níveis Mínimos de Serviços Exigidos.

7.2.2. Todas as atividades devem ser relacionadas e fornecidas à fiscalização do Contratante.

7.3. Níveis de Garantia e Assistência Técnica

7.3.1. Durante o período de garantia, suporte técnico e manutenção, a Contratada deverá atender às solicitações do Ministério, em qualquer horário e prazos estabelecidos, respeitando as condições e os níveis de serviços no qual serão contados a partir da abertura do chamado e será classificado conforme as severidades especificadas no **ANEXO I - ESPECIFICAÇÕES TÉCNICAS.**

7.3.2. O atendimento de suporte para a solução deverá ser do tipo 24 x 7 (vinte e quatro horas por dia, sete dias por semana), e deverá ser realizado por profissionais especializados.

7.3.3. Não haverá limite para o número de chamados de suporte técnico.

7.3.4. O descumprimento dos prazos de nível de serviço de atendimento implicará na aplicação das sanções administrativas previstas no contrato.

7.3.5. Nos casos em que as manutenções necessitarem de paradas do ambiente, o Ministério deverá ser imediatamente notificado para que se proceda a aprovação da manutenção, ou para que seja agendada nova data, a ser definida pelo Contratante, para execução das atividades de manutenção.

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

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

7.4.1.1. Inexecutar total ou parcialmente qualquer das obrigações assumidas em decorrência da contratação;

7.4.1.2. ensejar o retardamento da execução do objeto;

7.4.1.3. falhar ou fraudar na execução do contrato;

7.4.1.4. comportar-se de modo inidôneo; ou

7.4.1.5. cometer fraude fiscal.

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

7.4.2.1. **Advertência**, por faltas leves, assim entendidas aquelas que não acarretem prejuízos significativos para a Contratante;

7.4.2.2. multa moratória de 1% (um por cento) por dia de atraso injustificado sobre o valor da parcela inadimplida, até o limite de 30 (trinta) dias;

7.4.2.3. multa compensatória de 5% (cinco por cento) sobre o valor total do contrato, no caso de inexecução total do objeto;

7.4.2.4. em caso de inexecução parcial, a multa compensatória, no mesmo percentual do subitem acima, será aplicada de forma proporcional à obrigação inadimplida;

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

7.4.2.6. **Impedimento de licitar e contratar com órgãos e entidades da União**, com o consequente descredenciamento no SICAF pelo prazo de até cinco anos;

7.4.2.7. a sanção de impedimento de licitar e contratar prevista neste subitem também é aplicável em quaisquer das hipóteses previstas como infração administrativa no subitem 7.1 deste Termo de Referência.

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

7.4.2.9. As sanções previstas nos subitens 7.4.2.1, 7.4.2.5 e 7.4.2.8 poderão ser aplicadas à CONTRATADA juntamente com as de multa, descontando-a dos pagamentos a serem efetuados.

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

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

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

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

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

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

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

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

7.4.8. 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.

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

7.4.10. 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 2013, seguirão seu rito normal na unidade administrativa.

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

7.4.12. As penalidades serão obrigatoriamente registradas no SICAF.

7.4.13. Nos casos de inadimplemento na prestação dos serviços, as ocorrências serão registradas pela CONTRATANTE, conforme a tabela abaixo:

Id	Ocorrência	Glosa / Sanção
1	Não comparecer injustificadamente à Reunião Inicial.	Advertência. Em caso de reincidência, 0,5% sobre o valor total do Contrato.
2	Quando convocado dentro do prazo de validade da sua proposta, não celebrar o Contrato, deixar de entregar ou apresentar documentação falsa exigida para o certame, ensejar o retardamento da execução de seu objeto, não manter a proposta, falhar ou fraudar na execução do Contrato, comportar-se de modo inidôneo ou cometer fraude fiscal.	A Contratada ficará impedida de licitar e contratar com a União, Estados, Distrito Federal e Municípios e, será descredenciada no SICAF, ou nos sistemas de cadastramento de fornecedores a que se refere o inciso XIV do art. 4º da Lei nº 10.520/2002, pelo prazo de até 5 (cinco) anos, sem prejuízo das demais cominações legais, e multa de 5% do valor da contratação.

3	Ter praticado atos ilícitos visando frustrar os objetivos da licitação.	A Contratada será declarada inidônea para licitar e contratar com a Administração.
4	Demonstrar não possuir idoneidade para contratar com a Administração em virtude de atos ilícitos praticados.	Suspensão temporária de 6 (seis) meses para licitar e contratar com a Administração, sem prejuízo da Rescisão Contratual.
5	Não executar total ou parcialmente os serviços previstos no objeto da contratação.	Suspensão temporária de 6 (seis) meses para licitar e contratar com a Administração, sem prejuízo da Rescisão Contratual.
6	Suspender ou interromper, salvo motivo de força maior ou caso fortuito, os serviços solicitados, por até de 30 dias, sem comunicação formal ao gestor do Contrato.	Multa de até 3% sobre o valor total do Contrato. Em caso de reincidência, configura-se inexecução total do Contrato por parte da empresa, ensejando a rescisão contratual unilateral.
7	Suspender ou interromper, salvo motivo de força maior ou caso fortuito, os serviços solicitados, por mais de 30 (trinta) dias, sem comunicação formal ao gestor do contrato.	Contratada será declarada inidônea para licitar e contratar com a Administração, sem prejuízo da Rescisão Contratual.
8	Não prestar os esclarecimentos imediatamente, referente à execução dos serviços, salvo quando implicarem em indagações de caráter técnico, hipótese em que serão respondidos no prazo máximo estabelecido neste Termo de Referência	Advertência. Em caso de reincidência, 0,5% sobre o valor total do Contrato.
9	Provocar intencionalmente a indisponibilidade da prestação dos serviços quanto aos componentes de software (sistemas, portais, funcionalidades, banco de dados, programas, relatórios, consultas, etc).	A Contratada será declarada inidônea para licitar ou contratar com a Administração Pública, sem prejuízo às penalidades decorrentes da inexecução total ou parcial do contrato, o que poderá acarretar a rescisão do Contrato, sem prejuízo das demais penalidades previstas na Lei nº 8.666, de 1993.
10	Permitir intencionalmente o funcionamento dos sistemas de modo adverso ao especificado na fase de levantamento de requisitos e às cláusulas contratuais, provocando prejuízo aos usuários dos serviços.	A Contratada será declarada inidônea para licitar ou contratar com a Administração Pública, sem prejuízo às penalidades decorrentes da inexecução total ou parcial do contrato, o que poderá acarretar a rescisão do Contrato, sem prejuízo das demais penalidades previstas na Lei nº 8.666, de 1993.
11	Comprometer intencionalmente o sigilo das informações armazenadas nos sistemas da contratante.	A Contratada será declarada inidônea para licitar ou contratar com a Administração Pública, sem prejuízo às penalidades decorrentes da inexecução total ou parcial do contrato, o que poderá acarretar a rescisão do Contrato, sem prejuízo das demais penalidades previstas na Lei nº 8.666, de 1993.
12	Comprometer intencionalmente o sigilo das informações armazenadas nos sistemas da contratante.	A Contratada será declarada inidônea para licitar ou contratar com a Administração Pública, sem prejuízo às penalidades decorrentes da inexecução total ou parcial do contrato, o que poderá acarretar a rescisão do Contrato, sem prejuízo das demais penalidades previstas na Lei nº 8.666, de 1993.
13	Não atender ao indicador de nível de serviço IAE (Indicador de Atraso de Entrega de OF)	Aplicar-se-á glosa de 0,33% por dia de atraso sobre o valor da OF, nos casos do valor de IAE entre 0,1 a 1,50.
		Aplicar-se-á multa de 2% sobre o valor OF, nos casos do valor de IAE acima de 1,5.
14	Não cumprir qualquer outra obrigação contratual não citada nesta tabela.	Advertência. Em caso de reincidência ou configurado prejuízo aos resultados pretendidos com a contratação, aplicar-se-á multa de 0,5% do valor total do Contrato.

Tabela 6 - Termos de serviço a serem observados pela CONTRATADA e penalizações aplicáveis

7.5. **Do pagamento**

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

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

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

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

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

7.5.4.1. 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.

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

7.5.6. O setor competente para proceder o pagamento deve verificar se a Nota Fiscal/Fatura apresentada expressa os elementos necessários e essenciais do documento, tais como:

7.5.6.1. o prazo de validade;

7.5.6.2. a data da emissão;

7.5.6.3. os dados do contrato e do órgão contratante;

7.5.6.4. o período de prestação dos serviços;

7.5.6.5. o valor a pagar; e

7.5.6.6. eventual destaque do valor de retenções tributárias cabíveis.

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

7.5.7.1. não produziu os resultados acordados;

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

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

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

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

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

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

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

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

7.5.14.1. 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.

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

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

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

EM = I x N x VP, sendo:
EM = Encargos moratórios;
N = Número de dias entre a data prevista para o pagamento e a do efetivo pagamento;
VP = Valor da parcela a ser paga.
I = Índice de compensação financeira diário= 0,00016438, assim apurado:

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

8. **ESTIMATIVA DE PREÇOS DA CONTRATAÇÃO**

8.1. Conforme descrito na tabela a seguir, o valor total estimado para esta contratação é de **R$ 1.978.501,77 (um milhão, novecentos e setenta e oito mil quinhentos e um reais e setenta e sete centavos),** sendo, portanto, o máximo aceito pelo Ministério**.**

GRUPO	ITEM	CÓDIGO CATSER	DESCRIÇÃO DO BEM	MEDIDA	QTD.	VALOR UNIT.	VALOR TOTAL (36 meses)
1	1	27740	Extensão do suporte técnico, licenciamento e atualização de versão da Solução de Balanceamento de Carga de Servidores e Solução de Segurança Web - F5 Networks BIG IP i2800 Best Bundle, por 36 meses	Unidade	2	**217.440,96**	**1.304.645,76**
	2	27502	Expansão do licenciamento da Solução de Balanceamento de Carga de Servidores e Solução de Segurança Web - módulo F5 BIG-IP Virtual Edition, com suporte técnico e atualização de versão por 36 meses	Unidade	1	**224.618,67**	**673.856,01**
VALOR TOTAL 36 MESES							**R$ 1.978.501,77**

Tabela 7 - Valor estimado

8.2. Considerando que o valor estimado da contratação não ultrapassa o limite estabelecido no inc. I do art. 2º da Instrução Normativa SGD/ME nº 5, de 11 de janeiro de 2021, bem assim que não se trata de pregão para registro de preços de que cuida o inc. II do art. 2º da referida norma, o presente procedimento licitatório fica dispensado da necessidade de submissão prévia à Secretaria de Governo Digital do Ministério da Economia.

9. **ADEQUAÇÃO ORÇAMENTÁRIA E CRONOGRAMA FÍSICO-FINANCEIRO**

9.1. **Adequação Orçamentária**

9.2. Gestão/Unidade: 810002 - Setorial Orçamentaria e Financeira - MMFDH

9.3. Fonte de Recursos: 0100

9.4. Ação: 2000 – Administração da Unidade

9.5. PTRES: 174791

9.6. PO: 000F - Integração de Aquisição de Tecnologia da Informação

9.7. Programa de Trabalho: 14.122.0032.2000.0001

9.8. A Secretaria do Tesouro Nacional (STN) instituiu, a partir de 2018, o elemento de despesa 40 - Serviços de Tecnologia da Informação e Comunicação (Pessoa Jurídica). As mudanças referem-se à exclusão do elemento 39 (Outros serviços de terceiros) para classificar as despesas de Tecnologia da Informação e Comunicação, as quais passaram a ser exclusivas do elemento 40.

9.9. O quadro a seguir apresenta as naturezas de despesas explicitamente relacionadas a serviços de Operações de Infraestrutura e atendimento ao usuário de TIC, conforme Manual SIAFI Web.

ITEM	DESCRIÇÃO	NATUREZA DE DESPESA	DESCRIÇÃO
1	Extensão do suporte técnico, licenciamento e atualização de versão da Solução de Balanceamento de Carga de Servidores e	33904012	Serviços de Garantia de Equipamentos de TIC

	Solução de Segurança Web - F5 Networks BIG IP i2800 Best Bundle, por 36 meses		
2	Expansão do licenciamento da Solução de Balanceamento de Carga de Servidores e Solução de Segurança Web - módulo F5 BIG-IP Virtual Edition, com suporte técnico e atualização de versão por 36 meses	33904006	Locação de softwares

9.10. **Estimativa de impacto econômico financeiro**

9.10.1. O item 1 tem previsão de emissão da ordem de serviço logo após a assinatura do contrato.

9.10.2. O item 2 terá sua ordem de serviço emitida após o término de adequações no DataCenter do MMFDH.

10. **DA VIGÊNCIA DO CONTRATO**

10.1. A vigência do contrato será de 36 (trinta e seis) meses, contados a partir da data de sua assinatura, *podendo ser prorrogado por interesse das partes até o limite de 60 (sessenta) meses, na* prorrogável na forma do art. 57, § 1°, da Lei n° 8.666/93. .

10.2. A vigência contratual perpassará mais de um exercício financeiro, haja vista a necessidade de embasar contratualmente a vigência do licenciamento e do serviço de suporte técnico, que serão de 36 (trinta e seis) meses.

10.3. Portanto, já que o prazo não trará obrigação financeira futura para a Administração, mas sim gerará vantagem econômica na contratação, e considerando que a cotação de preço por prazo estendido proporciona a diminuição do valor de fornecimento, convencionou-se por definir a vigência em 36 (trinta e seis) meses.

11. **DO REAJUSTE DOS PREÇOS**

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

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

11.3. No caso de atraso ou não divulgação do índice de reajustamento, o CONTRATANTE pagará à CONTRATADA a importância calculada pela última variação conhecida, liquidando a diferença correspondente tão logo seja divulgado o índice definitivo. Fica a CONTRATADA obrigada a apresentar memória de cálculo referente ao reajustamento de preços do valor remanescente, sempre que este ocorrer.

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

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

11.6. Na ausência de previsão legal quanto ao índice substituto, as partes elegerão novo índice oficial, para reajustamento do preço do valor remanescente, por meio de termo aditivo.

11.7. O reajuste será realizado por apostilamento.

12. **DOS CRITÉRIOS DE SELEÇÃO DO FORNECEDOR**

12.1. **Da natureza dos bens e/ou serviços**

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

12.1.2. Ao amparo da Lei nº 10.520, de 2002, e do Decreto nº 3.555, de 8 de agosto de 2000, o objeto afigura-se à definição de **"SERVIÇO COMUM"**, ou seja, cujos padrões de desempenho e qualidade possam ser objetivamente definidos pelo edital, por meio de especificações usuais no mercado, senão vejamos:

12.1.3. Conforme advoga Marçal Justen Filho, *in verbis*: "*bem ou serviço comum é aquele que se apresenta sob identidade e características padronizadas e que se encontra disponível, a qualquer tempo, num mercado próprio".*

12.1.4. Portanto, a definição de "bens e serviços comuns" inclui o simples, o padronizado, o rotineiro e ainda os que possam ser objetivamente descritos, sendo este o entendimento do Tribunal de Contas da União. Podendo, portanto, ser licitado por meio da modalidade Pregão.

12.2. **Do Tipo e Critério de Julgamento da Proposta**

12.2.1. Na forma do art. 23 da IN SGD/ME nº 01/2019, são apresentados a seguir os critérios técnicos para avaliação e julgamento das propostas para a fase de **SELEÇÃO DO FORNECEDOR**, observando-se as disposições

normativas e legais aplicáveis às contratações públicas.

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

12.2.3. A licitante classificada e habilitada provisoriamente em primeiro lugar deve preencher os preços do(s) modelo(s) de proposta de preços ANEXO V - MODELO DE PROPOSTA do(s) item(ns) em que for vencedor, conforme lances.

12.2.4. No caso de entender tais documentos como insuficientes para a análise, poderá o pregoeiro, suportado pelo grupo técnico de apoio, solicitar complementação, e/ou realizar diligência(s) para obter informações mais detalhadas sobre os produtos ofertados, conforme previsto no parágrafo § 3º do Art. 43 da Lei nº 8.666/93.

12.3. **Justificativa para a Aplicação do Direito de Preferência e Margens de Preferência**

12.3.1. Não se aplica a esta Licitação o Decreto nº 7.174, de 12 de maio de 2010.

12.3.2. Não haverá tratamento diferenciado e simplificado para as microempresas e empresas de pequeno porte. Em conformidade com inc. III do art. 49 da Lei Complementar nº 123/06, tal tratamento não se mostra vantajoso para a administração pública por representar possibilidade de prejuízo ao conjunto ou complexo do objeto a ser contratado, no que diz respeito ao ponto fundamental que é a manutenção da padronização da aquisição por grupos para atender a solução. Assevera essa questão, o artigo 15 da Lei nº 8.666/93 e a Súmula nº 247/TCU.

12.3.3. Lei no 8.666, de 21 de junho de 1993 e suas alterações.

12.3.4. Lei nº 10.520, de 17 de julho de 2002 que institui a modalidade Pregão.

12.3.5. Lei Complementar nº 123, de 14 de dezembro de 2006, que institui o Estatuto Nacional da Microempresa e da Empresa de Pequeno Porte.

12.3.6. Lei nº 7.596, de 10 de abril de 1987.

12.3.7. Decretos nº 10.183, de 20 de setembro de 2019; 10.024, de 20 de setembro de 2019 e 7.892, de 23 de janeiro de 2013.

12.3.8. 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.

12.3.9. IN/SLTI/MPOG nº 01/2019, que trata da contratação de serviços de Tecnologia da Informação (TI).

12.3.10. Nota Técnica nº 01/2008 - SEFTI/TCU - Estabelece o conteúdo mínimo do Termo de Referência ou Termo de Referência para contratação de serviços de Tecnologia da Informação e Comunicações – TIC.

12.3.11. Nota Técnica nº 02/2008 - SEFTI/TCU - Estabelece o uso do pregão para aquisição de bens e serviços de Tecnologia da Informação.

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

12.4.1. A habilitação técnica será feita por intermédio de atestados ou declarações de capacidade técnica.

12.4.2. O atestado de capacidade técnica deverá ser fornecido em nome do licitante, e ser expedido por pessoa jurídica de direito público ou privado, com a comprovação de que a empresa tenha fornecido objeto compatível em quantidade e especificidade com o objeto licitado.

12.4.3. Será exigido, para a comprovação de execução de objeto equivalente ao deste Termo de Referência, que a licitante vencedora apresente documento que ateste o fornecimento de 01 (um) equipamento similar para o respectivo item, caso a licitante obtenha menor preço em relação ao item.

12.4.4. O atestado deverá ser obrigatoriamente emitido por pessoa jurídica de direito público ou privado, devendo ainda ser emitido em papel timbrado e conter:

a) Razão Social, CNPJ e Endereço Completo da Empresa Emitente;

b) Razão Social da Contratada;

c) Número e vigência do contrato, se for o caso;

d) Objeto do contrato;

e) Declaração de que foram atendidas as expectavas do cliente quanto ao cumprimento de cronogramas pactuados;

f) Local e Data de Emissão;

g) Identificação do responsável pela emissão do atestado, Cargo, Contato (telefone e correio eletrônico);

h) Assinatura do responsável pela emissão do atestado;

i) Devem ser originais ou autenticados, se cópias, e legíveis.

13. **DA GARANTIA DE EXECUÇÃO**

13.1. O adjudicatário, no prazo de por 90 (noventa) dias após a assinatura do Termo de Contrato ou aceite do instrumento equivalente, prestará garantia no valor correspondente a 3% (três por cento) do valor do Contrato, que será liberada de acordo com as condições previstas neste Edital, conforme disposto no art. 56 da Lei nº 8.666, de 1993, desde que cumpridas as obrigações contratuais.

13.2. Caberá ao contratado optar por uma das seguintes modalidades de garantia:

13.2.1. caução em dinheiro ou em títulos da dívida pública, devendo estes 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;

13.2.2. seguro-garantia;

13.2.3. fiança bancária.

13.3. A garantia em dinheiro deverá ser efetuada em favor da Contratante, na Caixa Econômica Federal, com correção monetária, em favor do contratante.

13.4. No caso de alteração do valor do contrato, ou prorrogação de sua vigência, a garantia deverá ser readequada ou renovada nas mesmas condições.

13.5. 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 10 (dez) dias úteis, contados da data em que for notificada.

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

13.7. A garantia prestada pelo contratado será liberada ou restituída após a execução do contrato e, quando em dinheiro, atualizada monetariamente. (artigo 56, §4º da Lei nº 8666/93).

14. **DA SUBCONTRATAÇÃO**

14.1. Pela natureza e baixa complexidade do objeto, não será admitida a subcontratação do objeto licitatório.

15. **DISPOSIÇÕES GERAIS**

15.1. Fazem parte deste Termo de Referência os seguintes Anexos:

15.1.1. ANEXO I - Especificações Técnica

15.1.2. ANEXO I - Item 1 – Extensão do suporte técnico, licenciamento e atualização de versão da Solução de Balanceamento de Carga de Servidores e Solução de Segurança Web - F5 Networks BIG IP i2800 Best Bundle, por 36 meses.

15.1.3. ANEXO I - Item 2 - licenciamento da Solução de Balanceamento de Carga de Servidores e Solução de Segurança Web - módulo F5 BIG-IP Virtual Edition.

15.1.4. ANEXO II - TERMO DE COMPROMISSO DE MANUTENÇÃO DE SIGILO

15.1.5. ANEXO III - MODELO DE TERMO DE INTEGRIDADE

15.1.6. ANEXO IV - MODELO DE TERMO DE CIÊNCIA

15.1.7. ANEXO V - MODELO DE PROPOSTA

16. **DA EQUIPE DE PLANEJAMENTO DA CONTRATAÇÃO E DA APROVAÇÃO**

16.1. A Equipe de Planejamento da Contratação foi instituída pela Portaria nº 23, de setembro de 2022 (3206603).

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

INTEGRANTE TÉCNICO	INTEGRANTE REQUISITANTE	INTEGRANTE ADMINISTRATIVO
(Assinado eletronicamente) **HENRIQUE ALCÂNTARA VELOSO MOTA**	*(Assinado eletronicamente)* **DAVID SANTOS ABREU**	*(Assinado eletronicamente)* **TATIANA FERANANDES DA SILVA**

AUTORIDADE MÁXIMA DA ÁREA DE TIC

(Assinado eletronicamente)
ARTUR HENRIQUE CASTRO DE ANDRADE
Coordenador-Geral de Tecnologia da Informação

AUTORIDADE COMPETENTE

APROVO o presente Termo de Referência, mediante competência contida inciso I do art. 7º da Portaria 6, de 12 de janeiro de 2021, conforme dispõe o inciso II do art. 14 do Decreto Nº 10.024, de 20 de setembro de 2019.

(*Assinado Eletronicamente)*
LORENA FERRER C. R. POMPEU
Subsecretária de Orçamento e Administração

ANEXO I - ESPECIFICAÇÕES TÉCNICAS

ANEXO I – Item 1 – Extensão do suporte técnico, licenciamento e atualização de versão da Solução de Balanceamento de Carga de Servidores e Solução de Segurança Web - F5 Networks BIG IP i2800 Best Bundle, por 36 meses.

Trata-se da atualização dos dois Appliances F5 Networks BIG IP i2800 Best Bundle existentes no Ministério, com suporte técnico na modalidade 24x7 (vinte e quatro horas por dia, sete dias por semana).

Serviço de Suporte, garantia e atualização

Para fins de especificação do serviço, e considerando que a descrição trata de aspectos gerais sobre a forma de execução, destaca-se que os requisitos elencados a seguir são correspondentes aos itens:

A Contratada deverá prover garantia, suporte técnico, e atualização de versões das licenças fornecidas, pelo prazo de trinta meses, contados da data do recebimento definitivo dessas licenças;

O serviço inclui a instalação inicial das licenças contratadas e entrega do ambiente em efetivo funcionamento, para emissão do recebimento definitivo pelo Contratante;

Inclui todas as atualizações de versões, pequenas atualizações de release e reparos de defeitos (bug fixing patches);

Os serviços de suporte técnico aos produtos deverão incluir, dentre outros:

Orientações sobre uso, configuração e instalação do software ofertado;

Questões sobre compatibilidade e interoperabilidade do produto ofertado (hardware e software);

Interpretação da documentação do software ofertado;

Orientações para identificar a causa de uma falha de software;

Orientação para solução de problemas de “performance” e “tuning” das configurações do software ofertado;

Orientação quanto às melhores práticas para implementação do software adquirido;

Apoio na recuperação de ambientes em caso de panes ou perda de dados;

Apoio para execução de procedimentos de atualização para novas versões do software instalado;

A contratada deverá gerar relatório mensal, analítico e sintético, indicando todos os eventos relevantes ocorridos durante o período de execução do mesmo a ser entregue até o 5 (quinto) dia útil do mês subsequente.

Durante o período de garantia, suporte técnico e manutenção, a Contratada deverá atender às solicitações do Ministério, em qualquer horário e prazos estabelecidos, respeitando as condições e os níveis de serviços no qual serão contados a partir da abertura do chamado e será classificado conforme as severidades especificadas a seguir:

SEVERIDADE ALTA: Aplicado quando há indisponibilidade do ambiente tecnológico;

SEVERIDADE MÉDIA: Aplicado quando há falha no uso dos softwares, estando ainda disponíveis, porém apresentando problemas ou instabilidade;

SEVERIDADE BAIXA: Aplicado para instalação, configuração, manutenção preventivas, aplicações de atualização e esclarecimento técnico relativo ao uso das ferramentas.

Os prazos máximos para o atendimento dos chamados obedecerão ao disposto na tabela a seguir, contados a partir da data e hora de abertura do chamado:

Severidade	Atendimento	Solução definitiva
Alta	2 (duas) horas	4 (quatro) horas
Média	4 (quatro) horas	12 horas
Baixa	12 (doze) horas	24 (vinte e quatro) horas

Tabela 1 - Prazos dos chamados

Para os chamados de severidade ALTA (paralisação de pelo menos 1 (uma) das funcionalidades elencadas nas especificações técnicas), o início do atendimento deverá ocorrer no máximo em 2 (duas) horas corridas, a contar da abertura do chamado e a solução deverá ocorrer em até 4 (quatro) horas corridas a contar do início do atendimento.

Para os chamados severidade MÉDIA (degradação na performance, funcionamento ou serviço da solução), o início do atendimento deverá ocorrer no máximo em 4 (quatro) horas corridas, a contar da abertura do chamado e a solução deverá ocorrer em até 12 (doze) horas corridas a contar do início do atendimento.

Para os chamados severidade BAIXA (quando há comprometimento do desempenho), o início do atendimento deverá ocorrer no máximo em 12 (doze) horas corridas, a contar da abertura do chamado e a solução deverá ocorrer em até 24 (vinte e quatro) horas corridas a contar do início do atendimento.

Para os chamados de qualquer severidade, a critério do Ministério, poderá ser agendado o melhor horário para atendimento.

O fechamento de qualquer chamado só poderá ocorrer mediante consulta prévia ao Ministério quanto à efetiva solução do problema.

Qualquer chamado fechado, sem anuência do Ministério ou sem que o problema tenha sido resolvido, será reaberto e os prazos serão contados a partir da abertura original do chamado, inclusive para efeito de aplicação das sanções previstas.

A Contratada manterá cadastro das pessoas indicadas pelo Ministério que poderão efetuar abertura e autorizar o fechamento de chamados.

Ao término de atendimentos relacionados à assistência técnica da garantia, a Contratada deverá apresentar Relatório de Atendimento contendo data e hora da abertura do chamado, data e hora do início e do término do atendimento, identificação do defeito, nome do técnico responsável pela execução da garantia, providências adotadas e outras informações pertinentes. O Relatório deverá ser assinado por técnico do Ministério.

O atendimento deve ser efetuado em língua portuguesa.

A Contratada deverá fornecer relatório de atendimento técnico, referente a cada chamado, contendo no mínimo as seguintes informações:

Data e hora da abertura do chamado;

Data e hora do início do atendimento;

Responsável pelo atendimento da solicitação;

Motivo da ocorrência (indicação do defeito);

Status do chamado (aberto, em tratamento, fechado, etc.);

Data e hora do fechamento do chamado;

Solução adotada (resolução).

O atendimento de suporte para a solução deverá ser do tipo 24 x 7 (vinte e quatro horas por dia, sete dias por semana), e deverá ser realizado por profissionais especializados.

Não haverá limite para o número de chamados de suporte técnico.

O descumprimento dos prazos de nível de serviço de atendimento implicará na aplicação das sanções administrativas previstas no contrato.

Nos casos em que as manutenções necessitarem de paradas do ambiente, o Ministério deverá ser imediatamente notificado para que se proceda a aprovação da manutenção, ou para que seja agendada nova data, a ser definida pelo Contratante, para execução das atividades de manutenção.

ANEXO I – Item 2 - licenciamento da Solução de Balanceamento de Carga de Servidores e Solução de Segurança Web - módulo F5 BIG-IP Virtual Edition.

Características Gerais

Os VIRTUAL APPLIANCES deverão ser compatíveis com a plataforma operacional que será disponibilizada pelo MMFDH de acordo com o subitem enumerado a seguir:

Sistema de Virtualização Microsoft Hyper-V Server 2016 ou versões superiores, a critério do MMFDH;

O MMFDH disponibilizará os equipamentos que atuarão como servidores físicos hospedeiros para os VIRTUAL APPLIANCES;

Cada VIRTUAL APPLIANCE deverá ser capaz de balancear o tráfego de entrada e saída para a Internet de 1 Gbps (um gigabits por segundo) ou superior, de tráfego IP oriundo de clientes externos e internos em enlaces de comunicação de redes distintas, de diferentes operadoras de telecomunicações, sem a necessidade da utilização do protocolo BGP ou qualquer outro protocolo de roteamento;

Os VIRTUAL APPLIANCES deverão operar de forma redundante em topologia de alta disponibilidade, ou seja, na eventualidade da falha de um dos VIRTUAL APPLIANCES, outro APPLIANCE deverá automaticamente assumir, de forma transparente, todas as funções executadas pelo APPLIANCE defeituoso, com sincronismo de configurações e sem perda das sessões que estiverem em curso;

Todos os VIRTUAL APPLIANCES fornecidos deverão estar em linha na data de sua entrega, não sendo aceitos VIRTUAL APPLIANCES que tenham sido descontinuados ou com data de descontinuidade anunciada;

Todos os softwares integrantes das soluções ofertadas, inclusive firmware e sistema operacional dos VIRTUAL APPLIANCES, deverão ser fornecidos na versão mais nova comercializada na data da abertura das Propostas;

Deverão ser fornecidos em conjunto com as soluções ofertadas, todos os acessórios, softwares e opcionais necessários para o correto funcionamento do VIRTUAL APPLIANCES;

Suportar e garantir a instalação em ambiente de alta disponibilidade;

Assegurar que a solução deverá ser capaz de trabalhar no modo Ativo/Standby, com virtual appliance da mesma marca e modelo;

Fornecer uma solução que opere no modo Ativo/Ativo, mantendo o status das conexões. Aceita-se como Ativo/Ativo a utilização de dois endereços Virtuais, onde cada endereço fica ativo em um elemento e standby no outro;

Assegurar que a operação da solução de 2 ou mais appliances virtuais, quando implementada em ambiente redundante suporte sincronismo de sessão entre os dois membros. A falha do virtual appliance principal não deverá causar a interrupção das sessões balanceadas;

A solução deve possuir escalabilidade, podendo crescer na forma de cluster adicionando novos appliances virtuais ou físicos inclusive de modelos diferentes;

Possuir suporte a IPv6;

A solução deve suportar múltiplas tabelas de rotas independentes;

Possuir capacidade para gerenciar os recursos disponíveis de acordo com as funções habilitadas nos equipamentos SLB, GSLB, Aceleração Web, etc.

A solução deve possuir múltiplos domínios de roteamento em IPv4 e IPv6;

Possuir ferramenta online web gratuita na qual seja possível carregar as configurações e receber diagnóstico da solução com informações sobre atualizações, melhores práticas, estado da solução e informações preventivas.

Possuir suporte à funcionalidade de VXLAN, essencial para integração com o ambiente de virtualização (Software Defined Network).

Gerenciamento

Implementar uma configuração de endereçamento IP estático ou dinâmico (DHCP/BOOTP) para o gerenciamento;

Implementar o SNTP (Simple Network Time Protocol) ou NTP (Network Time Protocol);

Permitir acesso in-band via SSH;

Manter internamente múltiplos arquivos de configurações do sistema;

Utilizar SCP ou HTTPS como mecanismo de transferência de arquivos de configuração e Sistema Operacional;

Possuir auto-complementação de comandos na CLI;

Possuir ajuda contextual;

Interface por linha de comando (CLI – Command Line Interface) que possibilite a configuração dos equipamentos;

Possuir, no mínimo, Três níveis de usuários na GUI – Super-Usuário, Usuário com permissões reduzidas, e usuário Somente Leitura;

Os usuários de gerência deverão poder ser autenticados em bases remotas. No mínimo RADIUS, LDAP e TACACS+ deverão ser suportados;

Deverá ser possível receber da base RADIUS, LDAP e TACACS+ o nível de acesso (Grupo ou Permissões);

Possuir Interface Gráfica via Web;

A interface Gráfica deverá permitir a atualização do sistema operacional e/ou a instalação de patches ou Hotfixes sem o uso da linha de comando;

A interface gráfica deverá permitir a configuração de qual partição o equipamento deverá dar o boot;

Possuir um comando, via CLI, que mostre o tráfego de utilização das interfaces (bps e pps);

Suportar a rollback de configuração e imagem;

Possuir e fornecer MIBs compiláveis na plataforma HP Open View Network Node Manager;

Possuir e fornecer geração de mensagens de syslog para eventos relevantes ao sistema;

Possuir configuração de múltiplos syslog servers para os quais o equipamento irá enviar as mensagens de syslog;

Possuir armazenamento de mensagens de syslog em dispositivo interno ao equipamento;

A interface Gráfica deverá permitir a reinicialização do equipamento;
Reinicialização do equipamento por comando na CLI;
Possuir recurso de gerência via SNMP e implementar SNMPv1, SNMPv2c e SNMPV3;
Possuir traps SNMP;
Possui suporte a monitoração utilizando RMON através de pelo menos 4 grupos: statistics, history, alarms e events
Os logs de sistema devem ter a opção de ser armazenados internamente ao sistema ou em servidor externo;
Implementar Debugging: CLI via console e SSH;
Deve possuir suporte a Link Layer Discovery Protocol (LLDP);
Deve ser possível enviar, pelo menos, as seguintes informações via LLDP: Port ID, TTL, Port Description, System Name, System Description, Management Address, Port VLAN ID, Port and Protocol VLAN ID, VLAN Name, Protocol Identity, Link Aggregation, Maximum Frame Size;
A Solução deve ter a capacidade de permitir a criação de MIBs customizadas;
A Solução deve ter suporte a sFlow;
Distribuição de carga e otimização das aplicações
Suportar todas as aplicações comuns de um Switch Layer 7, como:
Server Load-Balancing;
Firewall Load-Balancing;
Proxy Load-Balancing;
Suportar Balanceamento apenas em direção ao servidor, onde a resposta do servidor real é enviada diretamente ao cliente;
A solução deve permitir o encapsulamento, em camada 3, do tráfego entre o balanceador e o servidor para tráfego IPv4 e IPv6, quando o balanceamento é realizado apenas em direção ao servidor, onde a resposta do servidor real é enviada diretamente ao cliente;
Permitir a clonagem de pools, de forma que a solução envie uma cópia do tráfego para um pool adicional, como por exemplo um pool de IDSs ou Sniffers, para fins de análise de tráfego de rede ou mesmo para identificação de padrões de acesso não permitidos ou indicações de atividade maliciosas ou ataques de rede;
Possuir recursos para balancear servidores com qualquer hardware, sistema operacional e tipo de aplicação;
A solução deve possuir recurso de ativação de grupo prioritário, no qual o administrador pode especificar a quantidade mínima de servidores que devem estar disponíveis em cada grupo e a prioridade dos grupos.
Caso o número de servidores disponíveis fique menor do que o estipulado pelo administrador, a solução deve automaticamente distribuir o tráfego para o próximo grupo com maior prioridade não afetando o serviço.
Caso o número de servidores disponíveis volte ao valor mínimo estipulado pelo administrador, a solução deve automaticamente retirar o grupo com menor prioridade de balanceamento, voltando ao estado original.
Possuir capacidade de abrir um número reduzido de conexões TCP com o servidor e inserir os HTTP requests gerado pelos clientes nestas conexões, reduzindo a necessidade de estabelecimento de conexões nos servidores e aumentando a performance do serviço;
Suportar os seguintes métodos de balanceamento:
- Round Robin;
- Least Connections;
- Weighted Percentage (por peso);
- Servidor ou equipamento com resposta mais rápida baseado no tráfego real;
- Weighted Percentage dinâmico (baseado no número de conexões)
- Dinâmico, baseado em parâmetros de um determinado servidor ou equipamento, coletados via SNMP ou WMI;
A solução deve permitir aplicar criptografia de cookies para a proteção dos cookies utilizados pela aplicação web;
Possuir recursos para balancear as sessões novas, mas preservar sessões existentes no mesmo servidor, implementando persistência de sessão dos seguintes tipos:
- Por cookie: inserção de um novo cookie na sessão;
- Por cookie: utilização do valor do cookie da aplicação, sem adição de cookie;
- Por endereço IP destino;
- Por endereço IP origem;
- Por sessão SSL;
- Através da análise da URL acessada.;
- Através da análise de qualquer parâmetro no header HTTP;
- Através da análise do MS Terminal Services Session (MSRDP)
- Através da análise do SIP Call ID ou Source IP;
- Através da análise de qualquer informação da porção de dados (camada 7);
A solução deve utilizar Cache Array Routing Protocol (CARP) no algoritmo de HASH;
O equipamento oferecido deverá suportar os seguintes métodos de monitoramento dos servidores reais:
- Layer 3 – ICMP;
- Conexões TCP e UDP pela respectiva porta no servidor;
- Devem existir monitores predefinidos para, no mínimo, os seguintes protocolos: ICMP, HTTP, HTTPS, Diameter, FTP, SASP, SMB, RADIUS, MSSQL, NNTP, ORACLE, RPC, LDAP, IMAP, SMTP, POP3, SIP, Real Server, SOAP, SNMP e WMI;
Possuir recursos para balanceamento de carga de servidores SIP para VoIP (equipamento SIP PROXY);
Possuir recursos para limitar o número de sessões estabelecidas com cada servidor real;
Possuir recursos para limitar o número de sessões estabelecidas com cada servidor virtual;
Possuir recursos para limitar o número de sessões estabelecidas com cada grupo de servidores;
Possuir recursos para limitar o número de sessões estabelecidas com cada servidor físico:

Realizar Network Address Translation (NAT);
Realizar Proteção contra Denial of Service (DoS);
Realizar Proteção contra Syn flood;
Realizar Limpeza de cabeçalho HTTP;
A solução deve permitir o controle da resposta ICMP por servidor virtual;
Possuir recursos para que a configuração seja baseada em perfis, permitindo uma fácil administração;
Possuir capacidade de geração e gestão de perfis hierarquizados, permitindo maior facilidade na administração de políticas similares;
Permitir a criação de Virtual Servers com endereço IPv4 e os servidores reais com endereços IPv6;
Possuir recursos para executar compressão de conteúdo HTTP, para reduzir a quantidade de informações enviadas ao cliente;
Deve permitir compressão tipo GZIP e Deflate;
Definir qual tipo de compressão será habilitada (gzip1 a gzip9, deflate);
Possuir capacidade para definir compressão especificamente para certos tipos de objetos;
Possuir recursos para fazer aceleração de SSL, onde os certificados digitais são instalados no equipamento e as requisições HTTP são enviadas aos servidores sem criptografia;
Garantir que na aceleração de SSL, tanto a troca de chaves quanto a criptografia dos dados seja realizada com aceleração em hardware, para não onerar o sistema, este item somente é válido para solução em appliance;
Deve possuir capacidade de importação dos certificados e chaves criptográficas, para transações seguras entre cliente/servidor, podendo assim operar em modo “man in the middle”, ou seja, descriptografar, otimizar e re-criptografar o tráfego SSL sem comprometer a segurança da conexão SSL estabelecida previamente entre cliente/servidor. Caso haja falha na leitura da conexão SSL, esta deverá, se assim definido, prosseguir em regime de passthrough.
A solução deve possuir a funcionalidade de espelhamento de conexões SSL.
A solução deve possuir a capacidade de redirecionar o SSL Offload (troca de chaves) de determinado serviço para outro appliance físico que tenha mais capacidade para tratamento SSL. Dessa forma deve ser possível otimizar recursos executando tarefas que exigem muito desempenho para serem tratadas em hardware especializado.
Possuir recursos para configurar o equipamento para recriptografar em SSL a requisição ao enviar para o servidor, permitindo as demais otimizações em ambiente 100% criptografado;
Todas as funcionalidades de inspeção, proteção e aceleração de tráfego criptografado através de SSL/TLS especificadas neste edital devem estar disponíveis quando a conexão segura for estabelecida usando:
Autenticação do servidor por parte do cliente, através da verificação da validade do certificado digital fornecido pelo lado servidor durante o processo de estabelecimento do túnel SSL/TLS;
Autenticação do cliente por parte do servidor, através da solicitação e verificação da validade do certificado digital fornecido pelo cliente durante o processo de estabelecimento do túnel SSL/TLS;
Ambas as autenticações acima mencionadas ocorrendo de forma simultânea;
Ao realizar inspeção, proteção, OffLoad e aceleração de tráfego criptografado através de SSL/TLS, a solução deverá ser capaz de:
Encaminhar ao servidor real via cabeçalho HTTP ou de forma transparente, todo o certificado digital utilizado pelo lado cliente para se autenticar perante o servidor durante o processo de estabelecimento do túnel SSL/TLS;
Encaminhar ao servidor real via cabeçalho HTTP campos específicos do certificado digital utilizado pelo cliente para se autenticar perante o servidor durante o processo de estabelecimento do túnel SSL/TLS;
A solução deve permitir aplicar criptografia de cookies para a proteção dos cookies utilizados pela aplicação web;
Possuir recursos para fazer aceleração de SSL, onde os certificados digitais são instalados no equipamento e as requisições POP3S, IMAPSe SMTPS são enviadas aos servidores sem criptografia;
A solução deve possuir diversos recursos relacionados ao uso de criptografia com o objetivo de otimizar e minimizar o impacto na performance das aplicações. Dentre eles deve ser possível configurar parâmetros como:
SSL session cache Timeout;
Session Ticket;
OCSP (Online Certificate Status Protocol) Stapling;
Dynamic Record Sizing;
ALPN (Application Layer Protocol Negotiation);
Perfect Forward Secrecy;
Suportar a utilização de memória RAM como cache de objetos HTTP, para responder às requisições dos usuários sem utilizar recursos dos servidores;
Possuir capacidade, no uso do recurso de cache, em definir quais tipos de objeto serão armazenados em cache e quais nunca devem ser cacheados;
Garantir que o recurso de cache possa ajustar quanta memória será utilizada para armazenar objetos;
Suporte a otimização do protocolo TCP para ajustes a parâmetros das conexões clientes e servidor;
A solução deve suportar Internet Content Adaptation Protocol (ICAP);
Deve ser capaz de realizar DHCP relay;
Deve possuir relatórios das aplicações, com pelos menos os seguintes gráficos:
- Tempo de resposta da aplicação;
- Latência;
- Conexões para conjunto de servidores, servidores individuais;
- Por URL;
A ferramenta de relatórios deve possuir pelo menos os seguintes filtros para a geração dos gráficos:
Servidores virtuais
Servidores balanceados

URLs
Países de origem, baseados em geolocalização (GEOIP)
Dispositivos de origem do cliente (user agent)
Deve possuir framework unificado para configuração da aplicação
Deve possuir criptografia IPSEC para comunicação entre os balanceadores;
Quando licenciada, a solução deve ter a capacidade de realizar cache transparente das respostas DNS;
A Solução deve ter a capacidade de permitir a criação de MIBs customizadas;
A Solução deve ter suporte a sFlow;
A solução deve possuir múltiplos domínios de roteamento em IPv4 e IPv6;
A solução deve permitir que cada domínio de roteamento utilize BGP, OSPF e RIP em IPv4 e IPv6;
A solução deve suportar Equal Cost Multipath (ECMP);
A solução deve realizar Bidirectional Forward Detection (BFD);
A solução deve ter suporte a Stream Control Transmission Protocol (SCTP);
Deve ter suporte a Transport Layer Security (TLS) Server Name Indication (SNI);
A solução deve possuir monitor HTTP/HTTPS com autenticação NTLM embutida, que permita verificar se o HTTP/HTTPS está operando assim como a plataforma de autenticação;
A solução deve ter suporte a TLS 1.2, SHA 2 Cipher e SHA256 hash;
A solução deve ter suporte a criptografia Perfect Forward Secrecy não apenas para troca de chaves RSA.
A solução deve ser capaz de colocar em fila as requisições TCP que excedam a capacidade de conexões do grupo de servidores ou de um servidor. O balanceador não deverá descartar as conexões que excedam o número de conexões do servidor ou do grupo de servidores:
- Deve ser possível configurar o tamanho máximo da fila;
- Deve ser possível configurar o tempo máximo de permanência na fila;
A solução deve realizar Controle de Banda Estático para grupos de aplicações e rede;
A solução deve realizar Controle de Banda Dinâmico por aplicação e usuário;
A solução deve realizar Controle de Banda baseado em domínio de roteamento;
Permitir tráfego por parâmetros de QoS (Quality of Service) ou rate-shaping, com pelo menos 2 (duas) filas para priorização de tráfego baseada na camada de aplicação; Através dessa priorização de tráfego e restrição de largura de banda deverá ser possível permitir um melhor nível de serviço para clientes preferenciais em detrimento dos demais clientes. A solução deve permitir a priorização de tráfego de entrada para determinadas aplicações.
A solução deve permitir a criação de túneis IP por domínio de roteamento utilizando GRE, IPIP, EtherIP, PPP;
A solução deve permitir a criação de túneis IP transparente utilizando GRE e IPIP;
Fornecer recursos para o uso de servidores (reals) no mesmo Virtual Server;
Possuir suporte ao protocolo SPDY e HTTP 2.0;
O equipamento deve possuir suporte ao espelhamento de conexões FTP, Telnet, HTTP, UDP, SSL.
O equipamento deverá permitir a sincronização das configurações:
- De forma automática;
- Manualmente, forçando a sincronização apenas no momento desejado;
Permitir a configuração das interfaces de alta disponibilidade do cluster (heartbeat), com opções para:
Compartilhar a rede de heartbeat com a rede de dados; e
Utilizar uma rede exclusiva para o heartbeat.
Permitir que regras customizadas em linguagem aberta possam ser utilizadas para customizar a distribuição dinâmica de tráfego e aumentar a proteção contra ataques;
A solução deve possuir linguagem de programação open-source que permita a manipulação do tráfego de entrada e saída, viabilizando assim a alteração de parâmetros no cabeçalho e no corpo das mensagens.
Essa linguagem de programação deve permitir a importação de pacotes, garantindo assim que a agilidade e flexibilidade no compartilhamento dos scripts.
Permitir a criação de políticas através de interface gráfica web para manipulação de tráfego através de lógica para pelo menos os seguintes operadores:
GEOIP, http-basic-auth, http-cookie, http-header, http-host, http-method, http-referer, http-set-cookie, http-status, http-uri e http-version.
Deve ser possível tomar as seguintes ações através dessas políticas:
Bloqueio de tráfego
Reescrita e manipulação de URL
Registro de tráfego (log)
Adição de informação no cabeçalho HTTP
Redirecionamento do tráfego para um membro específico
Selecionar uma política específica para Aplicação Web
A solução deverá ser capaz de fazer log de todas as sessões, onde os registros deverão conter:
Endereço IP de origem;
Porta TCP ou UDP de origem;
Endereço IP de destino;
Porta TCP ou UDP de destino;
Protocolo de camada 4 (TCP ou UDP);
Data e hora da mensagem;
URL acessada;

A solução deve possuir políticas de uso de senhas administrativas tais como: nível de complexidade, período de validade e travamento de conta devido a erros múltiplos de login de forma nativa ou no mínimo integrado a uma base Active Directory.
A solução deve suportar controle de versão da política de configuração de forma a permitir fazer roll back de políticas aplicadas.
A solução deve ser capaz de analisar a performance de aplicações web.
A solução deve possuir relatórios das aplicações.
Deve prover métricas de aplicações como: Transações por Segundo; Tempo de latência do cliente e servidor; Throughput de requisição e resposta; Sessões
A solução deverá gerar informações para permitir análises históricas e auxiliar nos processos de manutenções preventivas, de troubleshooting, de planejamento de capacidade e de análise da experiência dos usuários finais no acesso das aplicações.
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.
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.
A geração de informações históricas deverá permitir:
O detalhamento do tempo de resposta total de carregamento de uma URL e ou Página;
Permitir a correlação de métricas de uso de rede com o comportamento das aplicações.
Proteção contra ataques de aplicação:
A solução deve operar nos modos ativo-ativo e ativo-standby;
O equipamento oferecido deverá proteger a infraestrutura web de ataques contra a camada de aplicação (Camada 7);
Deve possuir tecnologia para mitigação de DDoS em camada 7 baseado em analise comportamental, usando o aprendizado.
Não deve haver a necessidade de intervenção de usuário para configurar thresholds DoS pois esses valores devem ser auto-ajustáveis e adpatativos de acordo com mudanças.
A solução deve possuir a capacidade de automaticamente capturar tráfego no formato TCP Dump relativos a ataques DoS L7, Web Scraping e força bruta permitindo uma análise mais aprofundada por parte do administrador.
A solução deve suportar o uso de firewall camada 3-4 junto com firewall camada 7 no mesmo equipamento/appliance para evitar problemas com o aumento da latência.
O equipamento oferecido deverá possuir a certificação ICSA para Firewall de Aplicação (Web Application Firewall);
Permitir a utilização de um modelo positivo de segurança para proteger contra ataques conhecidos aos protocolos HTTP e HTTPS e às aplicações web acessíveis através destes.
Possuir política de segurança de aplicações web pré-configurada na solução.
Permite a criação de políticas diferenciadas por aplicação e por URL, onde cada aplicação e URL poderão ter políticas totalmente diferentes;
Permitir a criação de políticas diferenciadas por aplicação.
Permite 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;
A solução deverá se integrar a soluções de análise (Scanner) de vulnerabilidade do site. O resultado desta análise deve ser utilizado para configurar as políticas do equipamento;
A solução deve permitir a integração com soluções de análise de vulnerabilidades (Scanner) de terceiros como por exemplo: Trustwave App Scanner (Cenzic), White Hat Sentinel, IBM AppScan, Qualys, Quotium Seeker, HP Webinspect.
A solução deve permitir a inspeção de upload de arquivos para os servidores de aplicação;
Essa inspeção pode ser feito via integração ICAP. Deve ser possível integrar com diferentes softwares de Antivírus;
Deve se integrar com o software de Antivírus existente no ambiente da Contratante.
Permitir que regras customizadas em linguagem aberta possam ser utilizadas para customizar e aumentar a proteção contra ataques recentes;
Permitir a integração com Firewall de Database de outros fabricantes.
A solução deve se integrar com outras soluções de segurança e análise de logs de outros fabricantes.
O fabricante da solução deve disponiibilizar também a comercialização como serviço na nuvem (WAFaaS), incluindo o serviço de migrar as regras/políticas existentes do Datacenter para a nuvem.
Deve possuir tecnologia de detecção de anomalias baseado nos IDs dos dispositivos, permitindo a detecção de DoS, ataques de força bruta e ataques de sequestro de sessão. Deve ser possível filtar relatórios por IDs de dispositivos.
A solução deve permitir incluir em blacklist os endereços IPs que repetidamente falharem a desafios no browser. Portanto o sistema não precisa usar recursos para mitigar trafego enviado por esses endereços Ips. Ao entrar em Blacklist o sistema automaticamente bloqueia os pacotes enviados por esse endereço por um período de tempo.
A solução deve suportar e fazer a proteção do tráfego em cima de protocolo WebSocket.
A solução deve possibilitar o uso de multiplas formas de logging remoto ao mesmo tempo para a mesma aplicação. Portanto dever ser possível por exemplo logar os requests válidos num servidor de SIEM e os requests inválidos em outro servidor de SIEM de outra marca e modelo.
A solução deverá possuir funcionalidade de proteção positiva e segura contra ataques, como:
Acesso por Força Bruta;
Ameaças Web AJAX/JSON;
DoS e DDoS camada 7;
Buffer Overflow;
Cross Site Request Forgery (CSRF);
Cross-Site Scripting (XSS);
SQL Injection;
Parameter tampering

Cookie poisoning;
HTTP Request Smuggling;
Manipulação de campos escondidos;
Manipulação de cookies;
Roubo de sessão através de manipulação de cookies;
Sequestro de sessão;
Força bruta no browser
XML bombs/DoS
Checagem de consistência de formulários;
Checagem do cabeçalho do “user-agent” para identificar clientes inválidos.
A solução deve suportar o uso de páginas de login AJAX/JSON tanto com configuração manual como descoberta automatica
Deverá ser capaz de identificar e bloquear ataques através de:
Regras de verificação personalizadas – política de segurança configurada.
Assinaturas, com atualização periódica da base pelo fabricante;
As assinaturas devem ser atualizadas durante o período do contrato sem que seja necessário nenhum custo a mais por parte da CONTRATANTE na aquisição de novas licenças ou subscrições. Deve fazer parte da solução de WAF ofertada.
Prevenir contra vazamento de dados sensíveis (mensagens de erro HTTP, códigos das aplicações, entre outros) dos servidores de aplicação, retirando os dados ou mascarando a informação nas páginas enviadas aos usuários.
Permitir a customização da resposta de bloqueio.
Permitir a liberação temporária ou definitiva (white-list) de endereços IP bloqueados por terem originados ataques detectados pela solução.
Deve permitir limitar o número de conexões e requisições por IP de origem para cada endereço IP Virtual.
Deve permitir adicionar, automaticamente e manualmente, em uma lista de bloqueio, os endereços IP de origem que ultrapassarem o limite estabelecido, por um período de tempo determinado através de configuração.
Deve permitir criar lista de exceção (white list) por endereço IP específico ou faixa de sub-rede.
A solução deve suportar o modelo de segurança positiva definido pelo OWASP, pelo menos o que consta no TOP 10.
Permitir o uso do parâmetro HTTP X-Forwarded-For como parte da política de controle.
Deverá implantar, no mínimo, as seguintes funcionalidades:
Proteção contra Buffer Overflow;
Checagem de URL;
Checagem de métodos HTTP utilizados (GET, POST, HEAD, OPTIONS, PUT, TRACE, DELETE, CONNECT);
Proteção contra envios de comandos SQL escondidos nas requisições enviadas a bases de dados (SQL Injection);
Proteção contra Cross-site Scripting;
Funcionalidade de Cookie Encryption;
Checagem de consistência de formulários;
Checagem do cabeçalho “user-agent” para identificar clientes inválidos.
Implementar as seguintes funcionalidades:
Cloaking – Proteção contra exposição de informações do ambiente e servidores internos como:
Sistema operacional e servidor web com impressão digital;
Esconder qualquer mensagem de erro HTTP dos usuários;
Remover as mensagens de erro às páginas que serão enviadas aos usuários;
Permitir a utilização de uma página HTML informativa e personalizável como HTTP Response aos bloqueios.
Deve ser possível verificar o endereço de origem do pacote IP no cabeçalho IP e no parâmetro X-forwarded-for (XFF).
Deve suportar a criação de políticas por geo-localização, permitindo que o tráfego de determinado(s) País/Países seja(m) bloqueado(s).
Possuir mecanismo de aprendizado automático capaz de identificar todos os conteúdos das aplicações, incluindo URLs, parâmetros URLs, campos de formulários, o que se espera de cada campo (tipo de dado, tamanho de caracteres), cookies, arquivos XML e elementos XML.
O equipamento oferecido deverá possuir uma funcionalidade de criação automática de políticas, onde a política de segurança é criada e atualizada automaticamente baseando-se no tráfego real observado à aplicação;
O perfil aprendido de forma automatizada pode ser ajustado, editado ou bloqueado;
O equipamento oferecido deverá possuir proteção baseada em assinaturas para prover proteção contra ataques conhecidos.
Deverá ser possível desabilitar algumas assinaturas específicas em determinados parâmetros, como uma exceção a regra geral;
A atualizações de assinaturas deverão passar por um período configurável de testes, ondes nenhuma requisição que viole a assinatura será bloqueada, apenas informada no relatório. Este processo deve ser automatizado, não sendo necessário criar regras específicas a cada atualização de assinatura;
O equipamento oferecido deverá permitir o bloqueio de ataques DoS na camada 7, possuindo também a opção de apenas registrar o ataque, sem tomar nenhuma ação de bloqueio;
O equipamento oferecido deverá possuir as seguintes formas de detecção de ataques DoS na camada de aplicação:
- Número de requisições por segundo enviados a uma URL específica;
- Número de requisições por segundo enviados de um IP específico;
- Detecção através de código executado no cliente com o objetivo de detectar interação humana ou comportamento de robôs (bots);
- Número máximo de transações por segundo (TPS) de um determinado IP;
- Aumento de um determinado percentual do número de transações por segundo (TPS);
- Aumento do stress do servidor de aplicação;

O equipamento oferecido deverá permitir o bloqueio de ataques de força bruta de usuário/senha em páginas de acesso (login) que protegem áreas restritas. Este bloqueio deve limitar o número máximo de tentativas e o tempo do bloqueio deverá ser configurável;
O equipamento oferecido deverá permitir o bloqueio de determinados endereços IPs que ultrapassarem um número máximo de violações por minuto. O período de bloqueio deverá ser configurável e durante este período todas as requisições do cliente serão bloqueadas automaticamente;
O equipamento oferecido deverá permitir o bloqueio de robôs (bots) que acessam a aplicação através de detecção automática, não dependendo de cadastros manuais. Robôs conhecidos do mercado, como Google, Yahoo e Microsoft Bing deverão ser liberados por padrão;
O equipamento oferecido deverá permitir o cadastro de robôs que podem acessar a aplicação;
Possuir política de segurança de aplicações pré-configuradas no equipamento para pelo menos as seguintes aplicações:
- IBM Lotus Domino;
- Microsoft ActiveSync v1.0, v2.0;
- Microsoft OWA in Exchange 2003, 2007, 2010;
- Microsoft SharePoint 2003, 2007, 2010;
- Oracle 10g Portal;
- Oracle Application 11i;
- Oracle PeopleSoft Portal;
- SAP NetWeaver;

O equipamento oferecido deverá implementar proteção ao JSON (JavaScript Object Notation);
Possuir firewall XML integrado – suporte a filtro e validação de funções XML específicas da aplicação;
Implementar a segurança de web services, através dos seguintes métodos:
- Criptografar/Decriptografar partes das mensagens SOAP;
- Assinar digitalmente partes das mensagens SOAP;
- Verificação de partes das mensagens SOAP;

Prevenir o vazamento de informações, permitindo o bloqueio ou a remoção dos dados confidenciais;
Prevenir que erros de aplicação ou infraestrutura sejam mostrados ao usuário;
Deverá ter integração, via ICAP, com servidor de antivírus para verificação dos arquivos a serem carregados nos servidores;
Permitir o uso do parâmetro HTTP X-Forwarded-For como parte da política de controle;
Deverá proteger o protocolo FTP com pelo menos os seguintes métodos:
- Determinar os comandos FTP permitidos;
- Requests FTP anônimos;
- Checar compliance com o protocolo FTP;
- Proteger contra ataques de força bruta nos logins;

Deverá proteger o protocolo SMTP com pelo menos os seguintes métodos:
- A comunicação deve ser aderente a RFC 2821;
- Limitar o número de mensagens;
- Validar registro SPF do DNS;
- Determinar quais métodos SMTP podem ser utilizados;

Deverá armazenar os log localmente ou exportar para Syslog server;
Deverá proteger contra atraques CSRF (Cross-Site Request Forgery), podendo ser possível especificar quais URLs serão examinadas;
Deverá possuir controle de fluxo por aplicação permitindo definir o fluxo de acesso de uma URL para outra da mesma aplicação. Dessa forma qualquer tentativa de acesso a um determido site que não siga o fluxo passando pelas URLs pré-definidas deverá ser bloqueado como uma tentativa de acesso ilegal.
A solução deve fornecer relatórios consolidados de ataques com pelo menos os seguintes dados: Resumo geral com as políticas ativas, anomalias e estatísticas de tráfego, Ataques DoS, Ataques de Força Bruta, Ataques de Robôs, Violações, URL, Endereços IP, Países, Severidade e PCI Compliance.
Deverá permitir o agendamento de relatórios a serem entregues por email;
Fornecer os seguintes Gráficos de alertas por:
- Política de segurança;
- Tipos de ataques;
- Violações;
- URL;
- Endereços IP;
- Países;
- Severidade;
- Código de resposta;
- Métodos;
- Protocolos;
- Vírus;
- Usuário;
- Sessão;

Deverá exportar as requisições que contém os ataques, pelo menos nos formatos PDF e binário
Deve possuir relatório em tempo real sobre ataques DoS L7, atualizado automaticamente.
A solução deve mostrar o impacto de ataques DoS L7 na performance e memória do servidor.
Os logs devem indicar o momento de início e final de um ataque DoS L7.

Possuir método de mitigação de DoS L7 baseado em: CAPTCHA ; Descarte de todas as requisições de um determinado IP e/ou país suspeito; Geolocalização, incluindo a prevenção com CAPTCHA para países suspeitos que ultrapassarem os thresholds; Defesa proativa contra Bot, através da injeção de um desafio JavaScript para detectar se é um usuário legítimo ou robô;
A solução deve permitir que ao detectar um falso positivo, o administrador aceite a requisição e atualize a política automaticamente.
A solução ao se integrar com um Scanner de vulnerabilidade deve mostrar quais a vulnerabilidades podem ser resolvidas automaticamente (pela própria solução de WAF) e quais podem ser resolvidas manualmente, pelo próprio administrador. No caso de resolução manual, deve ainda mostrar um guia com os passos necessários para resolver aquela vulnerabilidade, inclusive com a avisos de possíveis consequências na aplicação Web.
A solução deve classificar o nível de violação de uma requisição, possuindo pelo menos 5 níveis, onde o nível 5 é referente a violação mais grave e portanto deve ter prioridade.
A solução deve possuir proteção de DDoS L7 baseado em análise comportamental, sem precisar de nenhuma configuração manual.
Suportar os protocolos HTTP/1.0, HTTP/1.1 e HTTP/2.0.
Suportar codificação HTML "application/x-www-form-urlencoded".
Suportar Cookies v0 e v1.
Suportar codificação fragmentada (chunked encoding) em requisições e respostas.
Suportar compressão de requisições e respostas.
Suportar validação de protocolo, como:
Possibilidade de restringir uso de métodos;
Possibilidade de restringir protocolos e versões de protocolos;
Strict (per-RFC) Request Validation;
Validar caracteres URL-encoded; e
Validação de codificação fora de padrão %uXXYY.
Suportar restrições de HTML, como:
Tamanho do nome de parâmetros;
Tamanho dos valores de parâmetros; e
Combinação de tamanho de parâmetros (nome e valores).
Suportar POST no upload de arquivo.
Permitir configurar ou oferecer restrições para tamanho individual de arquivo.
Permitir customizar a lógica na inspeção de upload de arquivos.
Suporte para os métodos Basic, Digest e NTLM para autenticação.
Suporte para autenticação por back end tipo LDAP e Microsoft Active Directory.
Capacidade de filtrar cabeçalhos, corpo e status de respostas.
Suportar as seguintes técnicas de detecção:
URL-decoding;
Terminação Null Byte String;
Paths auto-referenciados;
Case de caracteres misturados;
Uso excessivo de espaços em branco;
Remoção de comentários;
Decodificação de entidades HTML; e
Caracteres de escape.
Possuir registro de logs com as seguintes características:
Em cada registro de log de acesso deve ser inserido um identificador de transação HTTP que deve ser único, envolvendo o par requisição/resposta;
Os registros de log de acesso e eventos devem ser armazenados em arquivo ou em banco de dados que permita a exportação ou em outro formato aberto como 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;
Permitir configurar a retenção dos logs por tempo e volume; e
Ter capacidade para detecção, remoção ou codificação de dados sensíveis do log.
A solução deverá gerar relatórios com as seguintes características:
Permitir a filtragem por data ou hora, endereço IP e tipo de incidente;
Permitir a geração de relatórios sob demanda ou pré-programados periodicamente (diário e semanal); e
Permitir a geração de relatórios em formatos PDF/A (versão aberta) e HTML.
Possuir as seguintes características de gerenciamento:
Facilidade para liberação de regras aprendidas automaticamente que estejam gerando grande quantidade de falso positivo;
Facilidade para transformar um ataque detectado e considerado falso positivo como regra do firewall;
Facilidade para aplicar diferentes regras para diversas aplicações;
Capacidade para customizar regras de negação de serviço;
Capacidade para combinar detecção e prevenção na construção das regras; e
Capacidade para desfazer a aplicação de uma regra.
Possuir mecanismos que garantam a capacidade de gerenciamento do equipamento sob condições de alto tráfego.
A solução deve apresentar perfil de aprendizagem automática com:
Capacidade de aprendizagem automática sem intervenção humana; e
Capacidade de inspeção das regras criadas automaticamente.
Permitir o gerenciamento da configuração com as seguintes características:

Gerenciamento por autenticação dos usuários e as autorizações baseadas em perfis (roles); e
Capacidade de gerenciamento remoto dos equipamentos.
Apresentar logs e relatórios administrativos com as seguintes características:
Capacidade para identificar e notificar falhas do sistema ou perda de performance;
Capacidade de agregação de informações para simplificar a revisão das atividades do dispositivo; e
Capacidade para gerar estatísticas de serviço e sistema.
Possuir suporte a XML:
Para proteção de WebServices;
Em conformidade com a especificação WS-I básico; e
Com capacidade de restringir métodos do WebService via definição em WSDL.
Suportar funções de camuflagem (cloaking), como:
Esconder qualquer mensagem de erro http dos usuários; e
Remover as mensagens de erro das paginas que serão enviadas aos usuários.
Proteger a aplicação Web contra robôs sofisticados através da combinação de desafios enviados ao browser do usuário e tecnicas avançadas de analise comportamental.
A solução deve ecnriptar dados e credenciais na camada de aplicação, sem ter a necessidade de atualizar a aplicação.
Essas informações devem ser encriptadas para proteger o login e as credenciais dos usuários e com isso os dados da aplicação.
Deve aprender automaticamente o comportamento da aplicação e combinar o comportamento heurístico do trafego com o stress do servidor de aplicação para determinar uma condição de DDoS.
Ao detectar uma condição de DDoS, assinaturas dinâmicas devem ser automaticamente criadas e implementadas em tempo real para proteção da aplicação.
Deve possuir uma proteção proativa contra ataques automatizados por robôs e outras ferramentas de ataque.
Deve proteger informações sensíveis e confidenciais da interceptação por terceiros, através da criptografia de dados quando ainda no browser do usuário.
Deve proteger esses dados criptografados de malwares e keyloggers.
Deve possuir proteção contra ataques DDoS, através da análise de comportamento de trafego usando técnicas de analise de dados e Machine Learning.
Através da analise continua de carga e monitoração de saúde de servidores, deve ser possível identificar anomalias e mitiga-las.
Deve ajudar a previnir contra ataques de Credential Stuffing, onde bases de credenciais expostas na Internet são usados para tentativa de acesso de outras aplicações Web.

Serviço de Instalação e Configuração

A Licitante vencedora será inteiramente responsável pela migração da solução atual para a nova solução, de forma a não comprometer o funcionamento dos sistemas, recursos ou equipamentos atualmente em operação.
Serão contemplados todos os serviços de instalação física de todos os componentes adquiridos, desde a montagem dos equipamentos até a energização dos mesmos.
Deverá ser fornecido documentação de toda a implementação e configuração dos produtos adquiridos.
Após no máximo 10 (dez) dias da assinatura do contrato, deverá ser realizada uma reunião presencial no Contratante, com a participação de no mínimo 1 (um) preposto da Contratada e os representantes da equipe do Contratante, com o objetivo de elaborar o plano de migração.
A Contratada deverá apresentar, para aprovação do Contratante, o plano detalhado de migração, especificando os procedimentos e cronograma a serem adotados.
O Contratante fará análise e validação do plano detalhado de migração, em até 5 (cinco) dias úteis, apontado as devidas correções no documento, ficando a Contradada responsável por ajustar o plano em até 7 (sete) dias úteis, conforme as alterações apontadas pela Contratante.
Fica a critério do Contratante, definir o horário de instalação e configuração dos equipamentos, podendo tais procedimentos serem executados em feriados ou finais de semana e em horário noturno.
A Contratada não poderá realizar terceirização dos serviços objeto deste termo de referência, sendo responsável pela execução do serviço objeto desta contratação.

ANEXO II - TERMO DE COMPROMISSO DE MANUTENÇÃO DE SIGILO

TERMO DE COMPROMISSO DE MANUTENÇÃO DE SIGILO

INTRODUÇÃO

O Termo de Compromisso de Manutenção de Sigilo registra o comprometimento formal da Contratada em cumprir as condições estabelecidas no documento relativas ao acesso e utilização de informações sigilosas da Contratante em decorrência de relação contratual, vigente ou não.

Referência: Art. 18, Inciso V, alínea "a" da IN SGD/ME Nº 1/2019.

Pelo presente instrumento o <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 do 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 pelo 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 nº 12.527, de 18/11/2011 e os Decretos nº 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 do 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 do 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 ao CONTRATANTE dos documentos comprobatórios.

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

A vigência deste Termo independe do prazo de vigência do contrato assinado.

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 pelo 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 - Havendo necessidade legal devido a Programas de Governo, a CONTRATADA assume o compromisso de assinar Termo de Sigilo (ou equivalente) adicional relacionado ao Programa, prevalecendo as cláusulas mais restritivas em benefício do CONTRATANTE.

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

I – O 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 pelo 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 a 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

O CONTRATANTE elege o foro da <CIDADE DO CONTRATANTE>, onde está localizada a sede do 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 _____ de 20____

De acordo.

CONTRATANTE	CONTRATADA
_____ <Nome> Matrícula: <Matr.>	_____ <Nome> <Qualificação>
Testemunhas	
Testemunha 1 _____ <Nome> <Qualificação>	Testemunha 2 _____ <Nome> <Qualificação>

ANEXO III - MODELO DE TERMO DE INTEGRIDADE

TERMO DE INTEGRIDADE

Termo de Integridade e Ética:

Eu,_____, representante legal da empresa_____, regularmente inscrita no CNPJ sob o n._____, declaro, para os devidos fins, que a empresa/organização ora qualificada não pratica e nem permite que pratiquem, sob sua esfera de atuação, atos contrários às leis, normas, regras e regulamentos vigentes no ordenamento jurídico brasileiro, que importem lesão à Administração Pública Nacional ou Estrangeira, nos termos do art. 5º da Lei nº 12.846, de 1º de agosto de 2013 - Lei Anticorrupção.

Outrossim, declaro que a empresa envida os melhores esforços para prevenir, mitigar e erradicar condutas inadequadas da sua atuação e se determina de acordo com as melhores práticas do mercado.

Reconheço que o que subscrevo é verdade, sob as penas da lei.

LOCAL, DATA.

Assinatura
Cargo
CPF

ANEXO IV - MODELO DE TERMO DE CIÊNCIA

TERMO DE CIÊNCIA

INTRODUÇÃO

< O Termo de Ciência visa obter o comprometimento formal dos empregados da contratada diretamente envolvidos na contratação quanto ao conhecimento da declaração de manutenção de sigilo e das normas de segurança vigentes no Órgão/Entidade>.
< No caso de substituição ou inclusão de empregados da contratada, o preposto deverá entregar ao Fiscal Administrativo do Contrato os Termos de Ciência assinados pelos novos empregados envolvidos na execução dos serviços contratados>.

Referência: Art. 18, Inciso V, alínea "b" da IN SGD/ME Nº 1/2019.

1 – IDENTIFICAÇÃO

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

2 – CIÊNCIA

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

Funcionários da Contratada

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

<Local>, <dia> de <mês> de <ano>.

ANEXO V - MODELO DE PROPOSTA

MODELO DE PROPOSTA

PROPOSTA
PREGÃO ELETRÔNICO N. __/_____
OBJETO:_____
EMPRESA: _____
CNPJ: _____
ENDEREÇO: _____
TELEFONE: _____
E-MAIL: _____

AO
MINISTÉRIO DA MULHER, DA FAMÍLIA E DOS DIREITOS HUMANOS

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

GRUPO	ITEM	DESCRIÇÃO	MARCA	MODELO	Indicar a origem do produto (nacional ou importado)	UN.	QUANT.	PREÇO UNITÁRIO R$	PREÇO TOTAL R$
1	1	Extensão do suporte técnico, licenciamento e atualização de versão da Solução de Balanceamento de Carga de Servidores e Solução de Segurança Web - F5 Networks BIG IP i2800 Best Bundle, por 36 meses				Un	2		
	2	Expansão do licenciamento da Solução de Balanceamento de Carga de Servidores e Solução de Segurança Web - módulo F5 BIG-IP Virtual Edition.				Un	1		
	PREÇO TOTAL POR EXTENSO:								

Declaramos que o item constante desta proposta corresponde exatamente às especificações descritas no Termo de Referência do Edital, às quais aderimos formalmente.

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

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

PRAZO DE ENTREGA DO OBJETO: _____ (por extenso) dias (observar o disposto no Edital).

Declaramos que:

a) os equipamentos ofertados, caso necessário, receberão atendimento de garantia na rede de assistência autorizada pelo fabricante;

b) informaremos os preços unitários dos equipamentos, das peças e dos demais componentes que integram o objeto da licitação sempre que solicitado pela CONTRATANTE, para fins de registro patrimonial;

c) serão fornecidas peças de reposição originais durante todo o período de garantia, podendo também ser utilizadas peças de tecnologia mais recente, também originais, de desempenho igual ou superior.

É OBRIGATÓRIA A COMPROVAÇÃO A QUE SE REFERE O SUBITEM ___ DO ITEM ___ DO EDITAL.

TABELA DE CONFORMIDADE TÉCNICA

Para cada um dos itens no qual o licitante deseja fazer proposta deve ser preenchido separadamente as tabelas apresentadas abaixo.

IDENTIFICAÇÃO DO ITEM: Ex: ITEM 01 - Extensão do suporte técnico, licenciamento e atualização de versão da Solução de Balanceamento de Carga de Servidores e Solução de Segurança Web - F5 Networks BIG IP i2800 Best Bundle, por 36 meses.				
DESCRIÇÃO DOS REQUISITOS MÍNIMOS PARA Trata-se da atualização dos dois Appliances F5 Networks BIG IP i2800 Best Bundle existentes no Ministério, com suporte técnico na modalidade 24x7 (vinte e quatro horas por dia, sete dias por semana).		**PÁGINA**	**ITEM**	**OBSERVAÇÃO**
PROCESSADOR				
1.1	A Contratada deverá prover garantia, suporte técnico, e atualização de versões das licenças fornecidas, pelo prazo de trinta meses, contados da data do recebimento definitivo dessas licenças;			
...				
...				
...				

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

_____

Assinatura do representante legal da empresa

_____

Nome do representante legal da empresa

Documento assinado eletronicamente por **Henrique Alcântara Veloso Mota**, **Integrante Técnico**, em 16/12/2022, às 18:41, conforme horário oficial de Brasília, com fundamento no **§ 3º do art. 4º do Decreto nº 10.543, de 13 de novembro de 2020**.

Documento assinado eletronicamente por **David Santos Abreu**, **Integrante Requisitante**, em 16/12/2022, às 19:21, conforme horário oficial de Brasília, com fundamento no **§ 3º do art. 4º do Decreto nº 10.543, de 13 de novembro de 2020**.

Documento assinado eletronicamente por **Artur Henrique Castro de Andrade**, **Coordenador(a)-Geral de Tecnologia da Informação**, em 19/12/2022, às 08:36, conforme horário oficial de Brasília, com fundamento no **§ 3º do art. 4º do Decreto nº 10.543, de 13 de novembro de 2020**.

Documento assinado eletronicamente por **Lorena Ferrer Cavalcanti Randal Pompeu**, **Subsecretário(a) de Orçamento e Administração**, em 19/12/2022, às 10:55, conforme horário oficial de Brasília, com fundamento no **§ 3º do art. 4º do Decreto nº 10.543, de 13 de novembro de 2020**.

3317323 00135.214051/2021-24

MINISTÉRIO DA MULHER, DA FAMÍLIA E DOS DIREITOS HUMANOS
DIVISÃO DE CONTRATOS
SCS Quadra 09 - Lote C, Ed. Parque Cidade Corporate, Torre-A, 10º Andar
Brasília, DF. CEP 70308-200. - http://www.mdh.gov.br

MINUTA DE CONTRATO 01/2022 - RETIFICADA - DICON/CCGA/CGL/SOAD/SE/MMFDH

MINUTA

TERMO DE CONTRATO Nº XX/XXXX QUE EI REPRESENTADA PELO MINISTÉRIO DA MI DIREITOS HUMANOS E A EMPRESA XXXXXX.

A União, representada pelo **MINISTÉRIO DA MULHER, DA FAMÍLIA E DOS DIREITOS HUMANOS**, por intermédio da **SUBSECRETARIA DE ORÇAMENTO E ADMINISTRAÇÃO**, com sede no Setor Comercial Sul - B, Quadra 9, Lote C, Edifício Parque Cidade Corporate, 10º andar, Torre A, CEP 70308-200, na cidade de Brasília/ DF, inscrito no CNPJ sob o n.º 27.136.980/0008-87, neste ato representado pela Senhor (a) **XXXXXXXXXXXXXXXXX**, Matrícula SIAPE: XXXXXXXXX, designada por meio da Portaria n.º XXXXXXXXXXXXX, publicada na XXXXX, do Diário Oficial da União – DOU, de XXXXXXXXX, por Subdelegação de Competência fixada no art. 1º, inciso I, da Portaria nº XXXXXXXXXX, publicada na XXXXXXXXX, do Diário Oficial da União – DOU, de XXXXXXX, doravante denominada **CONTRATANTE**, e a empresa xxxxxxxxxx, inscrita no CNPJ/MF sob o nº : XXXXXXX, com sede na XXXXXX, doravante denominada **CONTRATADA**, neste ato representada pelo Senhor(a) **XXXXXX,** tendo em vista o que consta no Processo nº 00135.214051/2021-24, e em observância às disposições da Lei nº 8.666, de 21 de junho de 1993, da Lei nº 10.520, de 17 de julho de 2002, da Lei nº 8.248, de 22 de outubro de 1991, do Decreto nº 7.892, de 23 de janeiro de 2013, do Decreto nº 9.507, de 21 de setembro de 2018, do Decreto nº 7.174, de 12 de maio de 2010, da Lei nº 13.709, de 14 de agosto de 2018, da Lei 12.305, de 02 de agosto de 2010, da Lei nº 8.078, de 11 de setembro de 1990, da Lei nº 9.784, de 29 de janeirode 1999, da Lei nº 12.846, de 1º de agosto de 2013, da Lei nº 7.596, de 10 de abril de 1987, do Decreto nº 8.538 de 06 de outubro de 2015, do Decreto nº 10.183, de 20 de setemro de 2019, do Decreto nº 10.024, de 20 de setembro de 2019, do Decreto nº 7.174, de 12 de maio de 2010, Decreto nº 10.222, de 05 de fevereiro de 2020, Decreto nº 9.637, de 26 de dezembro de 2018, da Instrução Normativa SGD/ME nº 1, de 4 de Abril de 2019, Instrução Normativa SEGES/ME nº 53, de 8 de Julho de 2020, da Instrução Normativa nº 73, de 05 de agosto de 2020 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 Eletrônico nº XXXXXXX, UASG: 81005, mediante as cláusulas e condições a seguir enunciadas:

1. **CLÁUSULA PRIMEIRA - OBJETO**

1.1. O objeto do presente instrumento é a contratação de Modernização da Solução de Balanceamento de Carga de Servidores e Solução de Segurança Web existente, incluindo renovação do suporte técnico e expansão do licenciamento, conforme condições, quantidades e exigências estabelecidas no Termo de Referência e seus anexos.

1.2. Este Termo de Contrato vincula-se ao Edital do Pregão, identificado no preâmbulo e à proposta vencedora, independentemente de transcrição.

1.3. Discriminação do objeto:

Grupo	Item	CATSER	Descrição	Medida	Qtd.	Valor Unit.	Valor Total
1	1	27740	Extensão do suporte técnico, licenciamento e atualização de versão da Solução de Balanceamento de Carga de Servidores e Solução de Segurança Web - F5 Networks BIG IP i2800 Best Bundle, por 36 meses	Unid.	2	**R$ 0,00**	**R$ 0,00**
	2	27502	Expansão do licenciamento da Solução de Balanceamento de Carga de Servidores e Solução de Segurança Web - módulo F5 BIG-IP Virtual Edition, com suporte técnico e atualização de versão por 36 meses	Unid.	1	**R$ 0,00**	**R$ 0,00**
VALOR TOTAL - 36 (TRINTA E SEIS) MESES						**R$ 0,00**	

Tabela 1 - Relação dos serviços e bens

2. **CLÁUSULA SEGUNDA - VIGÊNCIA**

2.1. A vigência do contrato será de 36 (trinta e seis) meses, contados a partir da data de sua assinatura, podendo ser prorrogado por interesse das partes até o limite de 60 (sessenta) meses, na forma do art. 57, § 1°, da Lei n° 8.666/93.

3. **CLÁUSULA TERCEIRA - PREÇO**

3.1. O valor total do contrato é de R$ 1.978.501,77 (um milhão, novecentos e setenta e oito mil quinhentos e um reais e setenta e sete centavos).

GRUPO	ITEM	CÓDIGO CATSER	DESCRIÇÃO DO BEM	MEDIDA	QTD.	VALOR UNIT	VALOR TOTAL

1	1	27740	Extensão do suporte técnico, licenciamento e atualização de versão da Solução de Balanceamento de Carga de Servidores e Solução de Segurança Web - F5 Networks BIG IP i2800 Best Bundle, por 36 meses	Unidade	2	**434.881,92**	**1.304.645,76**
	2	27502	Expansão do licenciamento da Solução de Balanceamento de Carga de Servidores e Solução de Segurança Web - módulo F5 BIG-IP Virtual Edition, com suporte técnico e atualização de versão por 36 meses	Unidade	1	**673.856,01**	**673.856,01**
VALOR TOTAL 36 MESES							**R$ 1.978.501,77**

3.2. No valor acima estão incluídas todas as despesas ordinárias diretas e indiretas decorrentes da execução do objeto, inclusive tributos e/ou impostos, encargos sociais, trabalhistas, previdenciários, fiscais e comerciais incidentes, taxa de administração, frete, seguro e outros necessários ao cumprimento integral do objeto da contratação.

4. **CLÁUSULA QUARTA – DOTAÇÃO ORÇAMENTÁRIA**

4.1. As despesas decorrentes desta contratação estão programadas em dotação orçamentária própria, prevista no orçamento da União, para o exercício de 2022, na classificação abaixo:

Empenho	PTRES	Elemento de Despesa	Quantidade	Valor Total R$

4.2. No(s) exercício(s) seguinte(s), as despesas correspondentes correrão à conta dos recursos próprios para atender às despesas da mesma natureza, cuja alocação será feita no início de cada exercício financeiro.

5. **CLÁUSULA QUINTA – PAGAMENTO**

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

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

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

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

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

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

5.7. Havendo erro na apresentação da Nota Fiscal ou nos 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.

5.8. O setor competente para proceder o pagamento deve verificar se a Nota Fiscal/Fatura apresentada expressa os elementos necessários e essenciais do documento, tais como:

5.8.1. o prazo de validade;

5.8.2. a data da emissão;

5.8.3. os dados do contrato e do órgão contratante;

5.8.4. o período de prestação dos serviços;

5.8.5. o valor a pagar; e

5.8.6. eventual destaque do valor de retenções tributárias cabíveis.

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

5.9.1. não produziu os resultados acordados;

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

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

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

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

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

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

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

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

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

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

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

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

EM = I x N x VP, sendo:
EM = Encargos moratórios;
N = Número de dias entre a data prevista para o pagamento e a do efetivo pagamento;
VP = Valor da parcela a ser paga.
I = Índice de compensação financeira diário= 0,00016438, assim apurado:

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

6. **CLÁUSULA SEXTA - DA LEI ANTICORRUPÇÃO**

6.1. As partes CONTRATANTES/CELEBRANTES DO CONTRATO comprometem-se a observar os preceitos legais instituídos pelo ordenamento jurídico brasileiro no que tange ao combate à corrupção, em especial a Lei nº 12.846, de 1º de Agosto de 2013, e, no que forem aplicáveis, os seguintes tratados internacionais: Convenção sobre o Combate da Corrupção de Funcionários Públicos Estrangeiros em Transações Comerciais Internacionais (Convenção da OCDE) - promulgada pelo Decreto nº 3.678, de 30 de novembro de 2000; a Convenção Interamericana Contra a Corrupção (Convenção da OEA) - promulgada pelo Decreto nº 4.410, de 7 de outubro de 2002; e a Convenção das Nações Unidas Contra a Corrupção (Convenção das Nações Unidas) - promulgada pelo Decreto nº 5.687, de 31 de janeiro de 2006.

6.2. A **CONTRATADA**, declara, por si e por seus administradores, funcionários, representantes e outras pessoas que agem em seu nome, direta ou indiretamente, estar ciente dos dispositivos contidos na Lei nº 12.846/2013; (ii) se obriga a tomar todas as providências para fazer com que seus administradores, funcionários e representantes tomem ciência quanto ao teor da mencionada Lei nº 12.846/2013.

PARÁGRAFO PRIMEIRO – A **CONTRATADA**, no desempenho das atividades objeto deste CONTRATO, compromete-se perante ao **CONTRATANTE** a abster-se de praticar ato(s) que possa(m) constituir violação à legislação aplicável ao presente instrumento pactual, incluindo aqueles descritos na Lei nº 12.846/2013, em especial no seu artigo 5º.

PARÁGRAFO SEGUNDO - Qualquer descumprimento das regras da Lei Anticorrupção e suas regulamentações, por parte da **CONTRATADA**, em qualquer um dos seus aspectos, poderá ensejar:

I - Instauração do Procedimento de Apuração da Responsabilidade Administrativa – PAR, nos termos do Decreto nº 8.420/2015 e Instrução Normativa CGU nº 13/2019, com aplicação das sanções administrativas porventura cabíveis;

II – Ajuizamento de ação com vistas à responsabilização na esfera judicial, nos termos dos artigos 18 e 19 da Lei nº 12.846/2013.

PARÁGRAFO TERCEIRO - A **CONTRATADA** obriga-se a conduzir os seus negócios e práticas comerciais de forma ética e íntegra em conformidade com os preceitos legais vigentes no país.

7. **CLÁUSULA SÉTIMA – REAJUSTE DOS PREÇOS**

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

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

7.3. No caso de atraso ou não divulgação do índice de reajustamento, o CONTRATANTE pagará à CONTRATADA a importância calculada pela última variação conhecida, liquidando a diferença correspondente tão logo seja divulgado o índice definitivo. Fica a CONTRATADA obrigada a apresentar memória de cálculo referente ao reajustamento de preços do valor remanescente, sempre que este ocorrer.

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

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

7.6. Na ausência de previsão legal quanto ao índice substituto, as partes elegerão novo índice oficial, para reajuste dos preços do valor remanescente, por meio de termo aditivo.

7.7. O reajuste será realizado por apostilamento.

8. **CLÁUSULA OITAVA – GARANTIA DE EXECUÇÃO**

8.1. O adjudicatário, no prazo de por 90 (noventa) dias após a assinatura do Termo de Contrato ou aceite do instrumento equivalente, prestará garantia no valor correspondente a 3% (três por cento) do valor do Contrato, que será liberada de acordo com as condições previstas neste Edital, conforme disposto no art. 56 da Lei nº 8.666, de 1993, desde que cumpridas as obrigações contratuais.

8.2. Caberá ao contratado optar por uma das seguintes modalidades de garantia:

8.2.1. caução em dinheiro ou em títulos da dívida pública, devendo estes 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;

8.2.2. seguro-garantia;

8.2.3. fiança bancária.

8.3. A garantia em dinheiro deverá ser efetuada em favor da Contratante, na Caixa Econômica Federal, com correção monetária, em favor do contratante.

8.4. No caso de alteração do valor do contrato, ou prorrogação de sua vigência, a garantia deverá ser readequada ou renovada nas mesmas condições.

8.5. 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 10 (dez) dias úteis, contados da data em que for notificada.

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

0.1. A garantia prestada pelo contratado será liberada ou restituída após a execução do contrato e, quando em dinheiro, atualizada monetariamente. (artigo 56, §4º da Lei nº 8666/93).

9. **CLÁUSULA NONA – ENTREGA E RECEBIMENTO DO OBJETO**

9.1. As condições de entrega e recebimento do objeto são aquelas previstas no Termo de Referência, anexo ao Edital.

10. **CLÁUSULA DÉCIMA – REGIME DE EXECUÇÃO DOS SERVIÇOS E FISCALIZAÇÃO**

10.1. O regime de execução dos serviços a serem executados pela CONTRATADA, os materiais que serão empregados e a fiscalização pela CONTRATANTE são aqueles previstos no Termo de Referência, anexo do Edital.

11. **CLÁUSULA DÉCIMA PRIMEIRA - OBRIGAÇÕES DA CONTRATANTE E DA CONTRATADA**

11.1. As obrigações da CONTRATANTE e da CONTRATADA são aquelas previstas no Termo de Referência, anexo do Edital.

12. **CLÁUSULA DÉCIMA SEGUNDA – SANÇÕES ADMINISTRATIVAS**

12.1. As sanções relacionadas à execução do contrato são aquelas previstas no Termo de Referência, anexo do Edital.

13. **CLÁUSULA DÉCIMA TERCEIRA – RESCISÃO**

13.1. O presente Contrato poderá ser rescindido:

13.1.1. 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;

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

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

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

13.4. O termo de rescisão, sempre que possível, será precedido de:

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

13.4.2. Relação dos pagamentos já efetuados e ainda devidos;

13.4.3. Indenizações e multas.

14. **CLÁUSULA DÉCIMA QUARTA– VEDAÇÕES E PERMISSÕES**

14.1. É vedado à CONTRATADA interromper a execução dos serviços sob alegação de inadimplemento por parte da CONTRATANTE, salvo nos casos previstos em lei.

14.2. 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.

14.2.1. 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.

14.2.2. 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.

15. **CLÁUSULA DÉCIMA QUINTA – ALTERAÇÕES**

15.1. Eventuais alterações contratuais reger-se-ão pela disciplina do art. 65 da Lei nº 8.666, de 1993.

15.2. 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.

15.3. 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.

16. **CLÁUSULA DÉCIMA SEXTA – DOS CASOS OMISSOS**

16.1. 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 de licitações e contratos administrativos 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.

17. **CLÁUSULA DÉCIMA SÉTIMA – PUBLICAÇÃO**

17.1. Incumbirá à CONTRATANTE providenciar a publicação deste instrumento, por extrato, no Diário Oficial da União, no prazo previsto na Lei nº 8.666, de 1993.

18. **CLÁUSULA DÉCIMA OITAVA – FORO**

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

Para firmeza e validade do pactuado, o presente Termo de Contrato foi lavrado e disponibilizado, eletronicamente, por meio do Sistema Eletrônico de Informações – SEI, assinado pelos contraentes.

XXXXXXXXXXXXXXXX
Subsecretário (a) de Orçamento e Administração
Ministério da Mulher, da Família e dos Direitos Humanos
Contratante

xxxxxxxxxxxxxxxxxxxx
Representante Legal
xxxxxxxxxxxxxx
Contratada

Documento assinado eletronicamente por **Charliane Ferreira de Mesquita**, **Coordenador(a)**, em 15/12/2022, às 18:39, conforme horário oficial de Brasília, com fundamento no **§ 3º do art. 4º do Decreto nº 10.543, de 13 de novembro de 2020**.

A autenticidade deste documento pode ser conferida no site https://sei.mdh.gov.br/autenticidade, informando o código verificador **3317323** e o código CRC **A5D729E8**.

Estudo Técnico Preliminar

1. Informações Básicas

Número do processo: 00135.214051/2021-24

2. Descrição da necessidade

2.1. O papel da Tecnologia como instrumento indutor do desenvolvimento social e econômico de um país é cada vez mais fundamental. A Tecnologia da Informação vem assumindo uma importância cada vez maior para que se possa ampliar o acesso ao conhecimento e facilitar a comunicação, de forma cada vez mais efetiva com o cidadão.

2.2. À medida que o uso de informações e sistemas crescem não há como deixar de se abordar o item segurança e disponibilidade que, em se tratando de empresas particulares e/ou órgãos públicos, deixa de ser um ponto apenas importante para se tornar vital. Informações sigilosas roubadas, websites destruídos, informações apagadas de um banco de dados, entre outras ações, costumam resultar em prejuízos financeiros e morais que muitas vezes não podem ser reparados.

2.3. Neste sentido, no mundo globalizado que vivemos, a Tecnologia da Informação cumpre papel primordial: disponibilizar ao corpo técnico do Ministério, e às coligadas e subordinadas, as ferramentas adequadas para o tratamento e segurança das informações, da gestão financeira de fundos e de projetos apoiados pelo MMFDH, de apoio a pesquisa, enfim, da governança ambiental.

2.4. Ao longo dos anos o Ministério da Mulher, da Família e dos Direitos Humanos - MMFDH tem investido em recursos de tecnologia da informação e comunicação, de forma a assegurar o desempenho de suas atividades institucionais, possibilitando o tratamento de um grande e variado conjunto de informações.

2.5. No que tange à segurança da informação, nos últimos anos, o MMFDH realizou investimentos na criação de seu ambiente seguro. Tais investimentos, além de permitir um atendimento adequado à população, foi orientado à manutenção da credibilidade deste Ministério perante a sociedade. O MMFDH atento ao contínuo crescimento dos incidentes de segurança e a evolução das ameaças à sua rede tecnológica, vem buscando dar continuidade ao elevado nível de proteção de sua rede de dados, minimizando os incidentes no âmbito de sua estrutura organizacional.

2.6. Atualmente, mais de noventa por cento de todo o tráfego da Internet é criptografado por meio dos protocolos SSL/TLS (SSL: Certificado digital utilizado pelo protocolo https para poder manter as seguranças em conexões na internet e entre sistemas. Utiliza-se de criptografia para manter a segurança para que a comunicação entre um cliente e um servidor ocorra de forma segura. Entretanto, muitos cibercriminosos fazem o uso da criptografia para ocultar conteúdo malicioso ou extrair informações sigilosas de pessoas ou corporações podendo comprometer a integridade, a disponibilidade e a confidencialidade das informações. O desencapsulamento do tráfego SSL pelo BIG-IP para a posterior inspeção aumenta significativamente a segurança da rede do MMFDH ao possibilitar a análise desse tipo de tráfego permitindo a entrada e a saída apenas do tráfego benigno e desejado.

2.7. Ressalta-se que Balanceamento de Carga é uma tecnologia que permite que os usuários de Internet (externos e internos) realizem suas solicitações de acesso às aplicações web corporativas e estas sejam distribuídas entre os servidores de aplicações da rede do MMFDH, garantindo a alta disponibilidade e desempenho. Outra característica importante que a solução de Balanceamento de Carga provê é a segurança das aplicações. O conjunto de recursos de balanceamento inclui o melhor controle e a melhor distribuição dos recursos computacionais da infraestrutura, fazendo que os usuários sejam atendidos com velocidade e segurança. Além disso, a solução conta com módulo de relatórios onde se pode extrair informações gerenciais sobre os acessos às aplicações corporativas do MMFDH.

2.8. Ainda, há ganho de performance das aplicações, uma vez que esses equipamentos são os responsáveis por verificar a disponibilidade dos servidores e balancear a carga de requisições entre eles. Dessa forma, é possível diminuir o tempo de resposta para os serviços solicitados e aumentar a disponibilidade e o desempenho dos servidores suportados pela solução.

2.9. Outro fator importante, que corrobora com a necessidade de garantir uma infraestrutura de desempenho atualizada, é o contínuo aumento do acesso público aos serviços e às informações prestadas pelo órgão, oriundas das políticas de Transformação Digital e da necessidade do atendimento virtual e trabalho remoto, haja vista as políticas de isolamento social, necessárias ao enfrentamento da pandemia da COVID-19.

2.10. O balanceamento de carga do sistema BIG-IP é necessário para distribuir de forma igualitária as requisições a uma mesma aplicação hospedada em dois ou mais hosts servidores resultando em um melhor aproveitamento dos recursos de hardware e da rede e ainda, em conjunto com o Firewall através do serviço SD-Wan Fortinet, priorizar o tráfego das aplicações que são de maior relevância para o MMFDH por meio de configurações aplicadas de qualidade de serviço (QOS) otimizando a utilização dos links de internet contratados junto as operadoras SERPRO e NETWORLD TELECOMUNICAÇÕES DO BRASIL LTDA.

2.11. O equipamento está configurado como Default Gateway da rede e concentra ambos os links de Internet deste Ministério, fazendo com que as funções de “QoS”, balanceamento de aplicações (Application Controller) e balanceamento de links WAN sejam imprescindíveis para possibilitar o monitoramento e o controle do tráfego de rede. A utilização controlada de recursos de forma a priorizar as aplicações críticas, restringir as aplicações não críticas e bloquear as indesejáveis reflete diretamente no ciclo de investimento, prolongando os períodos entre as aquisições necessárias para atualizar a infraestrutura de rede (upgrades). Por sua vez, a função de balanceamento permite implantar soluções resilientes a falhas para acesso às aplicações internas e externas, melhorando a disponibilidade e a qualidade dos serviços de TI.

2.12. A solução BIG-IP atua também como um Proxy reverso aumentando significativamente a segurança dos acessos oriundos de áreas consideradas hostis como a Internet aos nossos servidores Web, que hospedam aplicações como o SEI, SISGEN. SINIR, MONITORAR, etc. O Firewall executa uma primeira inspeção de todas as requisições a essas aplicações e, se permitidas, as encaminha para a inspeção final executada pelo BIG-IP. Posteriormente, as requisições válidas são finalmente encaminhadas para o Virtual Server no BIG-IP, responsável pelo serviço.

2.13. Diante de um eventual ataque de DoS[1] ou DDoS[2] , o balanceador contém o ataque por empregar processamento em hardware, o que confere maior velocidade e segurança. Desta forma, a integridade de servidores e serviços permanece preservada.

3. Área requisitante

Área Requisitante	Responsável
COORDENAÇÃO GERAL DE TECNOLOGIA DA INFORMAÇÃO - CGTI	DAVID SANTOS ABREU

4. Necessidades de Negócio

4.1. Identificação das necessidades de negócio

4.1.1. No ambiente de redes de computadores, sempre se estará sujeito a falhas do sistema, indisponibilizando os recursos oferecidos que muitas vezes são de extrema importância para seus usuários. Neste sentido, a concepção de um sistema de alta disponibilidade envolve o uso de técnicas que se aplicam a prevenção de falhas, a tolerância a falhas, a remoção de falhas e a predição de faltas (AVIZIENIS, 2004).

4.1.2. A tolerância a falhas diz respeito à propriedade de um sistema continuar a fornecer um serviço correto para o qual foi projetado, mesmo quando submetido à faltas de hardware e software. Esta propriedade pode ser obtida pela aplicação de técnicas de redundância específicas, tais como de hardware e de software.

4.2. Redundância

4.2.1. A redundância é definida como a capacidade de um sistema em superar a falha de um de seus componentes através do uso de recursos redundantes. Para isso, um sistema depende de recursos alternativos, além do principal, e que estejam disponíveis para assumir o sistema assim que um evento de falha ocorrer.

4.2.2. A redundância é um termo muito usual e não se aplica apenas a redes de computadores. Ela pode ser embarcada em vários sistemas, como: energia, aviação, máquinas industriais e outros. A finalidade de um recurso redundante é suprir integral ou parcialmente os serviços, visando sempre que as funções mínimas do sistema estejam em funcionamento

4.3. Contingência

4.3.1. Definição de contingência como possibilidade de um acontecimento futuro de uma condição existente, incerteza sobre as condições operacionais envolvidas e a resolução destas condições dependerem de eventos futuros. Ou seja, a possibilidade de um fato ocorrer ou não, com uma situação de risco existente, com certo grau de probabilidade de acontecer. Portanto, quando se

projeta um sistema, deve-se definir em conjunto um plano de contingência, plano este que deve visar manter o funcionamento do sistema, caso ocorra uma falha, quando este estiver executando tal processo de contingenciamento. Para isso, faz-se necessário um estudo de cada um dos processos em particular, quais os riscos envolvidos em cada um deles, de como afetariam o sistema, quais seriam os mais impactantes, quais as áreas mais críticas, o que poderia paralisar o sistema, e o tempo de restabelecimento para cada fase, pois são questões que norteiam o plano de contingência.

4.3.2. Medidas preventivas e planejadas que suportem, por exemplo, falhas de software, hardware, base de dados, energia, temperatura, perda do link de comunicação e de causas naturais, devem estar incluídas no plano de contingenciamento, ou seja, ações imediatas, para serem executadas, visando o restabelecimento dos serviços, mesmo que parcialmente, diminuindo o tempo de paralisação caso ocorra uma falha. O plano de contingência deve ter alta disponibilidade de informações de monitoramento. Ser implantado de um modo seguro e eficiente, que possa gerenciar/solucionar os problemas ocorridos, e se possível, ser proativo e disponibilizem a solução da falha independentemente de ações externas, minimizando os impactos, e apenas mantendo relatório dos fatos ocorridos.

4.4. Disponibilidade

4.4.1. Disponibilidade é definida pelo tempo em que um sistema de rede deve estar disponível para seus usuários. Ela pode ser mensurada em relação ao tempo em que o sistema está em falha (downtime), com o tempo que deve estar disponível. Dependendo do plano de contingência criado para suprir falhas que possam indisponibilizar o sistema, o tempo disponível pode variar em horas, dias, meses ou até anos. Uma pequena variação na porcentagem pode considerar uma grande diferença de tempo. Por isso, é importante estimar a disponibilidade mínima da rede, a fim de montar seu plano de contingência. A disponibilidade pode ser enquadrada em três classes, Disponibilidade Básica, Alta Disponibilidade e Disponibilidade Contínua.

4.5. Balanceamento de Carga

4.5.1. Por ser um dos pontos mais críticos e vulneráveis a falha, a multiplicação de links wan é muito comum em planos de contingência. Dependendo do projeto e a disponibilidade dos recursos dos equipamentos utilizados, o balanceamento de carga entre os links pode ser implementado. Com o balanceamento de carga, pode-se aproveitar os recursos do sistema redundante, ao invés de ficarem ociosos até que ocorra uma falha.

4.5.2. A função de balanceamento entre os links wan é distribuir o tráfego de dados entre eles. Dependendo de sua aplicação, o balanceamento aumenta o desempenho da rede somando a banda dos links, aumentando a capacidade do sistema podendo inclusive prover redundância entre os links. O balanceamento pode ser relativo ao tráfego que entra na rede e ao tráfego que sai, ela pode ser em nível de pacotes, fluxos, destinos, e entre outras possibilidades.

4.6. Serviço de Suporte, garantia e atualização

4.6.1. Para fins de especificação do serviço, e considerando que a descrição trata de aspectos gerais sobre a forma de execução, destaca-se que os requisitos elencados a seguir são correspondentes aos itens:

4.6.2. A Contratada deverá prover garantia, suporte técnico, e atualização de versões das licenças fornecidas, pelo prazo de 36 (trinta e seis meses), contados da data do recebimento definitivo dessas licenças;

4.6.2.1. O prazo de garantia de 36 (trinta e seis meses) é padrão e comum para contratações de tecnologia da informação, principalmente quando se trata de bens de alto valor, como são os equipamentos cuja garantia é parte do objeto do presente estudo e acompanha o padrão do fabricante. O caso em apreço trata, entre outros, de extensão de **Licenças** e garantia durante 36 meses, o que, do ponto de vista econômico-financeiro, e até mesmo processual, é muito vantajoso para o Ministério, já que possibilita a obtenção de preços mais atrativos, sem a necessidade de prorrogações contratuais e de concessão de reajustes.

4.6.3. O serviço inclui a instalação inicial das licenças contratadas e entrega do ambiente em efetivo funcionamento, para emissão do recebimento definitivo pelo Contratante;

4.6.4. Inclui todas as atualizações de versões, pequenas atualizações de release e reparos de defeitos (bug fixing patches);

4.6.5. Os serviços de suporte técnico aos produtos deverão incluir, dentre outros:

4.6.5.1. Orientações sobre uso, configuração e instalação do software ofertado;

4.6.5.2. Questões sobre compatibilidade e interoperabilidade do produto ofertado (hardware e software);

4.6.5.3. Interpretação da documentação do software ofertado;

4.6.5.4. Orientações para identificar a causa de uma falha de software;

4.6.5.5. Orientação para solução de problemas de “performance” e “tuning” das configurações do software ofertado;

4.6.5.6. Orientação quanto às melhores práticas para implementação do software adquirido;

4.6.5.7. Apoio na recuperação de ambientes em caso de panes ou perda de dados;

4.6.5.8. Apoio para execução de procedimentos de atualização para novas versões do software instalado;

4.6.5.9. A contratada deverá gerar relatório mensal, analítico e sintético, indicando todos os eventos relevantes ocorridos na solução de balanceamento, o qual deverá ser entregue ao fiscal do contrato até o 5 (quinto) dia útil do mês subsequente.

4.6.6. Durante o período de garantia, suporte técnico e manutenção, a Contratada deverá atender às solicitações do Ministério, em qualquer horário e prazos estabelecidos, respeitando as condições e os níveis de serviços no qual serão contados a partir da abertura do chamado e será classificado conforme as severidades especificadas a seguir:

4.6.6.1. SEVERIDADE ALTA: Aplicado quando há indisponibilidade do ambiente tecnológico;

4.6.6.2. SEVERIDADE MÉDIA: Aplicado quando há falha no uso dos softwares, estando ainda disponíveis, porém apresentando problemas ou instabilidade;

4.6.6.3. SEVERIDADE BAIXA: Aplicado para instalação, configuração, manutenção preventivas, aplicações de atualização e esclarecimento técnico relativo ao uso das ferramentas.

4.6.6.4. Os prazos máximos para o atendimento dos chamados obedecerão ao disposto na tabela a seguir, contados a partir da data e hora de abertura do chamado:

Severidade	Atendimento	Solução definitiva
Alta	2 (duas) horas	4 (quatro) horas
Média	4 (quatro) horas	12 horas
Baixa	12 (doze) horas	24 (vinte e quatro) horas

Tabela 1 - Prazos dos chamados

4.6.6.5. Para os chamados de severidade ALTA (paralisação de pelo menos 1 (uma) das funcionalidades elencadas nas especificações técnicas), o início do atendimento deverá ocorrer no máximo em 2 (duas) horas corridas, a contar da abertura do chamado e a solução deverá ocorrer em até 4 (quatro) horas corridas a contar do início do atendimento.

4.6.6.6. Para os chamados severidade MÉDIA (degradação na performance, funcionamento ou serviço da solução), o início do atendimento deverá ocorrer no máximo em 4 (quatro) horas corridas, a contar da abertura do chamado e a solução deverá ocorrer em até 12 (doze) horas corridas a contar do início do atendimento.

4.6.6.7. Para os chamados severidade BAIXA (quando há comprometimento do desempenho), o início do atendimento deverá ocorrer no máximo em 12 (doze) horas corridas, a contar da abertura do chamado e a solução deverá ocorrer em até 24 (vinte e quatro) horas corridas a contar do início do atendimento.

4.6.6.8. Para os chamados de qualquer severidade, a critério do Ministério, poderá ser agendado o melhor horário para atendimento.

4.6.6.9. O fechamento de qualquer chamado só poderá ocorrer mediante consulta prévia ao Ministério quanto à efetiva solução do problema.

4.6.6.10. Qualquer chamado fechado, sem anuência do Ministério ou sem que o problema tenha sido resolvido, será reaberto e os prazos serão contados a partir da abertura original do chamado, inclusive para efeito de aplicação das sanções previstas.

4.6.6.11. A Contratada manterá cadastro das pessoas indicadas pelo Ministério que poderão efetuar abertura e autorizar o fechamento de chamados.

4.6.6.12. Ao término de atendimentos relacionados à assistência técnica da garantia, a Contratada deverá apresentar Relatório de Atendimento contendo data e hora da abertura do chamado, data e hora do início e do término do atendimento, identificação do defeito, nome do técnico responsável pela execução da garantia, providências adotadas e outras informações pertinentes. O Relatório deverá ser assinado por técnico do Ministério.

4.6.6.13. O atendimento deve ser efetuado em língua portuguesa.

4.6.7. A Contratada deverá fornecer relatório de atendimento técnico, referente a cada chamado, contendo no mínimo as seguintes informações:

4.6.7.1. Data e hora da abertura do chamado;

4.6.7.2. Data e hora do início do atendimento;

4.6.7.3. Responsável pelo atendimento da solicitação;

4.6.7.4. Motivo da ocorrência (indicação do defeito);

4.6.7.5. Status do chamado (aberto, em tratamento, fechado, etc.);

4.6.7.6. Data e hora do fechamento do chamado;

4.6.7.7. Solução adotada (resolução).

4.6.7.8. O atendimento de suporte para a solução deverá ser do tipo 24 x 7 (vinte e quatro horas por dia, sete dias por semana), e deverá ser realizado por profissionais especializados.

4.6.7.9. Não haverá limite para o número de chamados de suporte técnico.

4.6.7.10. O descumprimento dos prazos de nível de serviço de atendimento implicará na aplicação das sanções administrativas previstas no contrato.

4.6.7.11. Nos casos em que as manutenções necessitarem de paradas do ambiente, o Ministério deverá ser imediatamente notificado para que se proceda a aprovação da manutenção, ou para que seja agendada nova data, a ser definida pelo Contratante, para execução das atividades de manutenção.

4.7. Descrição das Necessidades de Negócio

4.7.1. O objeto desta contratação está alinhado com o Plano Diretor de Tecnologia da Informação e Comunicação – PDTIC 2022-2023 e a contratação de certificação é uma ação estruturante e essencial ao funcionamento do Ministério e relaciona-se também com as necessidades finalísticas.

Objetivos Estratégicos - CICLO 2019 - 2023 (SEI 2396898 e 2396900) Fonte: https://www.gov.br/mdh/pt-br/acesso-a-informacao/governanca/planejamento-estrategico	
ID	**Objetivos Estratégicos**
P1	Assegurar transparência e sistematização de informações para o aperfeiçoamento de políticas de direitos humanos
A3	Prover recursos orçamentários, financeiros e tecnológicos de forma eficiente
A4	Buscar a inovação dos serviços e processos com foco na simplificação, eficiência e melhoria da qualidade

Estratégia de Governo Digital - 2020 a 2022 Fonte: https://www.gov.br/governodigital/pt-br/EGD2020	
Objetivo 11	Garantia da segurança das plataformas de governo digital e de missão crítica
Iniciativa 11.1	Garantir, no mínimo, 99% de disponibilidade das plataformas compartilhadas de governo digital, até 2022.
Iniciativa 11.3	Definir padrão mínimo de segurança cibernética a ser aplicado nos canais e nos serviços digitais, até 2022.

ALINHAMENTO AO PDTIC 2022-2023 (SEI 2838829) Fonte: https://www.gov.br/mdh/pt-br/acesso-a-informacao/tecnologia-da-informacao			
ID	**Ação do PDTIC**	**ID**	**Meta do PDTIC associada**
A078	EQUIPAMENTO SEGURANÇA REDE	M07	Aprimorar a Segurança Física e do Ambiente quanto ao Controle do Acesso, Armazenamento e Disponibilidade da informação

ALINHAMENTO AO PAC 2022 (SEI 2648557) Fonte: https://www.gov.br/mdh/pt-br/acesso-a-informacao/licitacoes-e-contratos/pac-2022	
Item	**Descrição**
310	EQUIPAMENTO SEGURANÇA REDE

5. Necessidades Tecnológicas

5.1. Identificação das necessidades tecnológicas

5.1.1. Disponibilizar soluções de Segurança de TIC;

5.1.2. Atender à Política de Segurança da Informação nos Órgãos e Entidades da Administração Pública Federal;

5.1.3. Garantir a qualidade, o desempenho e a alta disponibilidade das informações e dos equipamentos do MMFDH;

5.1.4. Garantir a continuidade dos serviços aos usuários do MMFDH;

5.1.5. Manter a infraestrutura de alto desempenho adequada para o tráfego de informações e sistemas críticos de TIC;

5.1.6. Manter o licenciamento em conformidade com o parque tecnológico;

5.1.7. Manter o parque tecnológico atualizado e padronizado;

5.1.8. Obter atualizações, correções e evoluções durante o período de vigência do contrato;

5.1.9. Manter a disponibilidade, integridade, confidencialidade e autenticidade dos dados e informações.

5.1.10. Contratar suporte técnico, licenciamento e atualização de versão dos equipamentos F5 Networks BIG IP i2800 Best Bundle, por 36 meses.

5.1.11. Serviço de instalação e configuração.

5.1.11.1. Contemplar instalação e configuração na aquisição da solução, a fim de mantê-los em plenas condições de uso no início da vigência contratada. Exigir que o conhecimento da operação da solução seja repassado à equipe do MMFDH que irá executar atividades relacionadas aos produtos contratados.

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

6.1. Requisitos de Negócio

6.1.1. Atender às necessidades no Ministério para o serviço de suporte técnico e garantia por empresa especializada, contemplando a solução de tratamento e entrega de dados do MMFDH:

6.1.2. Garantir o acesso seguro aos recursos de Tecnologia da Informação para a prestação de serviços digitais do MMFDH.

6.1.3. Prover acesso seguro aos sistemas administrativos e corporativos utilizados pelo MMFDH (SEI, correio eletrônico, Internet, dentre outros) para o desempenho de suas funções.

6.1.4. Prover acesso de boa qualidade aos recursos providos externamente a rede do MMFDH através do tratamento e melhor utilização da capacidade oferecida pelos links de internet.

6.1.5. Prover acesso de boa qualidade priorizando o tráfego das aplicações classificadas como essenciais para alcançar os objetivos primários do Órgão.

6.1.6. Os serviços de manutenção corretiva, assistência e suporte técnico para os dois equipamentos já existentes no Ministério contemplarão a substituição de equipamentos e/ou módulos e/ou componentes (fontes, “fans” e sfp) que apresentem defeito durante a vigência da garantia.

6.1.7. O Suporte deverá ser especializado, podendo ser executado remotamente ou localmente dependendo da criticidade. A avaliação do chamado quanto a criticidade será feita pelo Ministério;

6.1.8. A documentação produzida durante a execução dos serviços, seja em papel ou meio eletrônico, será de propriedade do MMFDH e não deverá ser divulgado sem sua expressa autorização.

6.2. Requisitos temporais

6.2.1. A entrega das licenças deverá ocorrer em até 5 (cinco) dias úteis, contados da data da emissão de Ordem de Serviço por parte da CONTRATANTE.

6.2.2. Caso se veja impossibilitada de cumprir com o prazo estipulado no item anterior, a empresa CONTRATADA deverá, por escrito, solicitar prorrogação do prazo e apresentar justificativas.

6.2.3. O pedido de prorrogação, com indicação do novo prazo, quando for o caso, deverá ser encaminhado à fiscalização do CONTRATANTE, que poderá, de modo justificado, acolher ou não o pedido. Vencidos os prazos de entrega ou de prorrogação e não cumprida a obrigação de entrega, o CONTRATANTE oficiará a empresa CONTRATADA acerca do transcurso da data limite, passando o inadimplemento, sendo aplicáveis as sanções previstas no Termo de Referência e demais instrumentos legais.

6.2.4. Não há necessidade de fornecimento de mídias físicas para o licenciamento a ser adquirido.

6.2.5. As licenças e chaves de ativação necessárias deverão ser enviadas via e-mail para e-mail a ser definido pela CGTI. Somente será considerado entregue após confirmação de recebimento pela CONTRATANTE.

6.2.6. As licenças fornecidas deverão estar cobertas por garantia integral pelo período mínimo de 36 (trinta e seis) meses a contar da data do recebimento.

6.2.7. Problema no licenciamento, caso comprovado, deverá ser sanado dentro dos tempos estipulados. Quando não for possível solucionar o problema no prazo estipulado, caso autorizado pela Contratante, deverá ser fornecido outra licença de igual configuração ou superior, até resolução definitiva do problema.

6.2.8. Considerando que os recursos fornecidos pela solução a ser contratada são imprescindíveis à execução diária das atividades deste Ministério e que, se paralisados, podem pôr em risco a continuidade das atividades da Administração, não se mostra sensato exigir que sua vigência fique limitada a 12 (doze) meses, já que a prática administrativa é de prorrogar contratos desta natureza pelo período máximo permitido em lei (60 meses). Portanto, é notável a vantagem para a Administração Pública adotar vigência superior a 12 (doze)meses para serviços de natureza continua, uma vez que o interesse real é de contratá-los por maior período. Dessa maneira, além de permitir maior competitividade, reduz os custos administrativos e mitiga os riscos de indisponibilidade dos serviços de TIC por problemas que possam surgir nos processos de renovações contratuais.

6.2.9. Assim, a vigência do contrato será de 36 (trinta e seis) meses a partir da data de assinatura do contrato, prorrogável na forma do art. 57, § 1°, da Lei n° 8.666/93.

6.3. Requisitos de Arquitetura Tecnológica

6.3.1. Não aplicável a esta contratação.

6.4. Requisitos de Segurança

6.4.1. Aumentar o nível de segurança da operação de tecnologia do Contratante;

6.4.2. O serviço terá a participação e cooperação da Área de TI do Contratante durante toda a duração do contrato;

6.4.3. A Contratada irá prestar auxílio à equipe de Segurança da Informação do Contratante no suporte direto à solução contratada.

6.4.4. Todos os profissionais devem ser credenciados junto à Contratante, para que sejam autorizados a retirar e a entregar documentos, bem como prestar serviços em qualquer dependência da Contratante;

6.4.5. A Contratada deverá observar e respeitar, rigorosamente, todas as normas e procedimentos de segurança implementados no ambiente de Tecnologia da Informação do MMFDH, assim como as suas atualizações;

6.4.6. Deve ser mantido sigilo sobre todos os ativos de informações e de processos que se refiram ao Contratante, conforme TERMO DE COMPROMISSO e TERMO DE CIÊNCIA, que comporão o presente processo;

6.4.7. A Contratada não poderá divulgar quaisquer informações a que tenha acesso em virtude dos trabalhos a serem executados ou de que tenha tomado conhecimento em decorrência da execução do objeto, sem autorização, por escrito, da Contratante, sob pena de aplicação das sanções cabíveis;

6.4.8. Observância às diretrizes estabelecidas pela Política de Segurança da Informação e Comunicações do Contratante e demais normas sobre o assunto, no que couber.

6.4.9. Segurança da Informação durante o teletrabalho.

6.5. Requisitos Legais

6.5.1. Lei Federal nº 8.666/1993: Institui normas para licitações e contratos da Administração Pública e dá outras providências;

6.5.2. Lei Federal nº 10.520/2002: Institui no âmbito da União, Estados, Distrito Federal e Municípios, modalidade de licitação denominada pregão, para aquisição de bens e serviços comuns, e dá outras providências;

6.5.3. 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;

6.5.4. Decreto nº 7.174/2010: Regulamenta a contratação de bens e serviços de informática e automação pela administração pública federal;

6.5.5. Decreto nº 10.222 de 5 de fevereiro de 2020: A presente Estratégia Nacional de Segurança Cibernética - E-Ciber é orientação manifesta do Governo federal à sociedade brasileira sobre as principais ações por ele pretendidas, em termos nacionais e internacionais, na área da segurança cibernética e terá validade no quadriênio 2020-2023.

6.5.6. Decreto nº 9.637, de 26 de dezembro de 2018: Institui a Política Nacional de Segurança da Informação, dispõe sobre a governança da segurança da informação, e altera o Decreto nº 2.295, de 4 de agosto de 1997, que regulamenta o disposto no art. 24, caput, inciso IX, da Lei nº 8.666, de 21 de junho de 1993, e dispõe sobre a dispensa de licitação nos casos que possam comprometer a segurança nacional.

6.5.7. Instrução Normativa SGD/ME nº 01/2019: 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;

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

6.6. Requisitos Sociais, Ambientais e Culturais

6.6.1. É dever da Contratada observar entre outras: o menor impacto sobre recursos naturais como flora, fauna, ar, solo e água; preferência para materiais, tecnologias e matérias-primas de origem local; maior eficiência na utilização de recursos naturais como água e energia; maior geração de empregos, preferencialmente com mão de obra local; maior vida útil e menor custo de manutenção do bem e da obra; uso de inovações que reduzam a pressão sobre recursos naturais; e origem ambientalmente regular dos recursos naturais utilizados nos bens, serviços e obras. O ambiente físico da Contratada para fins de execução do serviço deve ser compatível com o disposto na NR17 do Ministério do Trabalho e Emprego – MTE e na recomendação técnica DSST nº 01/2005 do Ministério do Planejamento, Desenvolvimento e Gestão, no que couber.

6.6.2. O objeto a ser contratado deve estar adequado a Política Nacional de Resíduos Sólidos (PNRS), Lei Nº 12.305/2010, foi aprovada em agosto de 2010, dispondo sobre seus princípios, objetivos e instrumentos, bem como sobre as diretrizes relativas à gestão integrada e ao gerenciamento de resíduos sólidos, incluindo os perigosos, às responsabilidades dos geradores e do poder público e aos instrumentos econômicos aplicáveis, no que couber.

7. Estimativa da demanda - quantidade de bens e serviços

7.1. O Departamento de Informática do MMFDH, é responsável direto por fomentar, regulamentar, desenvolver e avaliar as ações estratégicas de Tecnologia da Informação e Comunicação - TIC, vem em constante atualização, visto que seus sistemas e serviços possuem valor inestimado, e é muito importante que os investimentos em tecnologia da informação sejam priorizados no sentido de garantir a segurança e a disponibilidade dos dados e informações em conjunto com as melhores práticas de mercado.

7.2. O MMFDH conta hoje com uma Solução, com dois equipamentos de Balanceamento de Carga de Servidores e Solução de Segurança Web F5 Net works BIG IP i2800 Best Bundle, adquirida no final do ano 2018 através do Contrato 35/2018 (SEI nº 0566612) e o suporte e garantia dessa solução de balanceamento findou em dezembro de 2021, mas o equipamento ainda possui considerável vida útil, sendo assim, é essencial que se verifique a viabilidade da renovação desse suporte.

7.3. Com o fim do prazo de vigência do referido contrato e inexistência de suporte e manutenção dos equipamentos adquiridos, foi iniciado planejamento da contratação que evidenciou a viabilidade para contratar os serviços de atualização e suporte para os equipamentos.

7.4. Solução de Tratamento e Entrega de Dados

7.4.1. Trata-se da atualização dos dois Appliances F5 Networks BIG IP i2800 Best Bundle existentes no Ministério, com suporte técnico na modalidade 24x7 (vinte e quatro horas por dia, sete dias por semana).

Imagem 1 - Quantidade de equipamentos instalados no Datacenter do MMFDH em 30/06/2022.

7.4.2. Especificações técnicas e descrições da solução existente estão detalhadas no Anexo - A deste Estudo Técnico Preliminar.

7.4.3. A necessidade de dois balanceadores é devido a alta disponibilidade (H.A – high availability) capacidade de garantir a continuidade dos serviços utilizados, mesmo em ocasiões de falhas, quando uma falha é identificada, seja no software, seja na conexão física, o dispositivo alternativo pode passar a operar, assumindo todas as funções do equipamento inoperante, ou seja, é necessário para fins de redundância e contingência.

7.5. Relação da quantidade estimada x quantidade necessária

7.5.1. Apresenta-se a seguir o quadro contendo a solução a ser contemplada com a contratação proposta.

GRUPO	ITEM	DESCRIÇÃO	QTDE.
Único	1	Extensão do suporte técnico, licenciamento e atualização de versão da Solução de Balanceamento de Carga de Servidores e Solução de Segurança Web - F5 Networks BIG IP i2800 Best Bundle, por 36 meses	2
	2	Expansão do licenciamento da Solução de Balanceamento de Carga de Servidores e Solução de Segurança Web - módulo F5 BIG-IP Virtual Edition.	1

Tabela 3 - Quantitativo

7.5.2. O item 1 da tabela supre se refere à extensão de suporte técnico, licenciamento e atualização de versão da Solução de Balanceamento de Carga de Servidores e Solução de Segurança Web - F5 Networks BIG IP i2800 Best Bundle, tendo em vista, os dois balanceadores utilizados por este Ministério, conforme imagem 1, do item 2.4.1.

7.5.3. O item 2 do quadro indica a necessidade de expansão das funcionalidades em uso, haja vista a evolução tecnológica ocorrida desde a formalização do Contrato n° 35/2018, ocorrida no segundo semestre do ano 2018.

7.5.4. Portanto, é necessária uma nova contratação para garantir a continuidade e disponibilidade da solução de Balanceamento de Carga no ambiente do MMFDH, caso não haja, os equipamentos adquiridos ficarão sem suporte e manutenção.

8. Levantamento de soluções

8.1. Identificação das Soluções

8.1.1. A análise comparativa de soluções, nos termos do inc. II do art. 11 da IN-01/2019/SGD, visa elencar as alternativas de atendimento à demanda, considerando, além do aspecto econômico, os aspectos qualitativos em termos de benefícios para o alcance dos objetivos da contratação.

8.1.2. Para atendimento da demanda posta, existem alternativas disponíveis no mercado, que possibilitam desde a renovação do suporte da solução existente, até a substituição completa da solução, seja pela aquisição de novos equipamentos, seja pela contratação na modalidade de serviço, sem a propriedade dos equipamentos.

8.1.3. Para atender a necessidade de suporte técnico da solução de tratamento e entrega de dados do MMFDH, levantou-se as seguintes alternativas:

Id	Descrição da solução
1	Contratação de nova Solução de Balanceamento de Carga de Servidores e Solução de Segurança Web, no formato de serviço, com fornecimento de equipamentos, licenças e suporte.
2	Aquisição de nova solução de Balanceamento de Carga de Servidores e Solução de Segurança Web, de forma genérica e aberta ao mercado, com garantia e suporte.
3	Modernização da Solução de Balanceamento de Carga de Servidores e Solução de Segurança Web existente, incluindo renovação do suporte técnico e expansão do licenciamento.
4	Utilização de Solução de Balanceamento de Carga de Servidores e Solução de Segurança Web disponível no Portal do Software Público.

Tabela 4 - Identificação de Soluções

9. Análise comparativa de soluções

9.1.1. Observância das alternativas às políticas, premissas e especificações técnicas vigentes

Requisito	ID do cenário	SIM	NÃO	NÃO SE APLICA
	1	X		
	2	X		

A Solução encontra-se implantada em outro órgão ou entidade da Administração Pública Federal?				
	3	X		
	4		X	
A Solução está disponível no Portal do Software Público Brasileiro?	1		X	
	2		X	
	3		X	
	4		X	
A Solução é um software livre ou software público?	1		X	
	2		X	
	3		X	
	4			X
A Solução é aderente às políticas, premissas e especificações técnicas definidas pelos Padrões e-PING, e-MAG, ePWG?	1	X		
	2	X		
	3	X		
	4			X
A Solução é aderente às regulamentações da ICPBrasil? (quando houver necessidade de certificação digital)	1	X		
	2	X		
	3	X		
	4			X
	1			X
	2			X

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

9.1.2. No intuito de complementar a presente análise, foi feita consulta ao site da Secretaria de Governo Digital, Órgão Central do SISP, a fim de se identificar eventual Catálogo de Soluções de TIC com Condições Padronizadas (https://www.gov.br/governodigital/pt-br/contratacoes/catalogo-de-solucoes-de-tic).

9.1.3. Para a solução que se pretende contratar, não foi formalizado instrumento com condições padronizadas.

10. Registro de soluções consideradas inviáveis

10.1. Conforme previsto no parágrafo 1º do art. 11 da IN SGD/ME N° 1/2019, as soluções identificadas e consideradas inviáveis deverão ser registradas no Estudo Técnico Preliminar da Contratação (breve descrição e justificativa), dispensando-se a realização dos respectivos cálculos de custo total de propriedade.

10.2. De acordo com a análise realizada, é considerada inviável a solução constante do **Cenário 4 - Utilização de solução disponível no Portal do Software Público.**

10.3. Trata-se da utilização das soluções disponíveis no Portal do Software Público, para atendimento da necessidade posta.

10.4. Em consulta Portal do Software Público (https://www.gov.br/governodigital/pt-br/software-publico/catalogo/catalogo), não foram identificados softwares com as características necessárias à solução desejada. Portanto, para o fornecimento de Solução de Balanceamento de Carga de Servidores e Solução de Segurança Web, incluindo suporte técnico, garantia e atualização, não é possível a utilização de software público. É necessária a contratação de empresa especializada na solução.

10.5. Pelo motivo apresentado, a solução não é viável, pelo farto de não existir software no portal capaz de atender as necessidades do MMFDH.

11. Análise comparativa de custos (TCO)

11.1. Análise Comparativa de Soluções

11.1.1. A proteção física e lógica da informação deve ser provida por ferramentas especializadas, seguras, consolidadas e, acima de tudo, que preservem a confidencialidade, a integridade e a disponibilidade da informação.

11.2. Cálculo dos Custos Totais de Propriedade

11.2.1. Em observância ao disposto na Instrução Normativa SGD/ME nº 1, de 4 de abril de 2019, apresenta-se a seguir a avaliação das soluções viáveis do ponto de vista técnico e funcional, e a capacidade de cada uma delas para atender aos requisitos da contratação:

Solução Viável 1 - Cenário 1	
Descrição	Contratação de nova solução de tratamento e entrega de dados, no formato de serviço, com fornecimento de equipamentos, licenças e suporte.
	Trata-se de contratação no formato de serviço, por intermédio do qual a Contratada fornece os equipamentos, licenças e serviços, sem a transferências de propriedade para o Ministério. Para tanto, o Contratante realiza pagamentos mensais à Contratada, de acordo com os níveis mínimos de serviço acordados.

Análise da Solução	**Pontos Positivos da Solução:** • Utilização de equipamentos novos, modernos e atualizados, de primeiro uso; • Não haverá transferência de propriedade dos equipamentos para o Ministério, portanto, não haverá, no âmbito da Pasta, preocupação com trâmites burocráticos para apropriação dos equipamentos ao patrimônio público, tampouco com cálculos e acompanhamento da depreciação dos bens. Tem-se, pois, um ganho para o órgão em relação às obrigações patrimoniais, o que dará liberdade aos servidores da respectiva área para empreenderem esforços em outras frentes. **Pontos Negativos da Solução:** • Maior complexidade na gestão contratual, por se tratar de serviços; • Preocupação com renovação anual de contrato, em face da burocracia envolvida em tal ação; • Maior preocupação por ocasião do final da vigência improrrogável do contrato, já que, sendo os equipamentos da propriedade da contratada, ao final da avença ela fará a retirada dos bens do ambiente do Ministério, e este somente terá restabelecido o serviço por ocasião de novo certame licitatório; • Não aproveitamento dos equipamentos já existente do Ministério. • Preço estimado para a contratação substancialmente mais elevado.

Custo Total de Propriedade – Memória de Cálculo

Para fins de comparativo preliminar de preços, foi identificada solução cujo objeto possui características técnicas similares àquelas esperadas para este cenário, sendo, pois, o **Contrato n° 15/2019 - UASG 413001, da Agência Nacional de Telecomunicações (2912363), Termo Aditivo 02/2022, vigência 18/02/2022 a 17/02/2023.**

O objeto do Contrato é a "Prestação de serviço técnico, especializado em WAF, com fornecimento de equipamento, pelo período de 12 meses".

O valor mensal atualizado do Contrato n° 15/2019 é de R$ 97.069,25 (noventa e sete mil sessenta e nove reais e vinte e cinco centavos), sendo total anual de R$ 1.164.831,00 (um milhão, cento e sessenta e quatro mil oitocentos e trinta e um reais).

Na análise em questão, foi considerado como balizador o valor anual do contrato, de modo a projetar a expectativa preliminar de preço de eventual nova contratação

Neste cenário, a solução pretendida possuiria **valor anual de R$ 1.164.831,00** (um milhão, cento e sessenta e quatro mil oitocentos e trinta e um reais).

Solução Viável 2 - Cenário 2

Descrição	Aquisição de nova solução de Balanceamento de Carga de Servidores e Solução de Segurança Web, com garantia e suporte.
	Trata-se da aquisição de nova solução de mercado, desenhada "do zero", para atendimento das necessidades hoje supridas pela solução anteriormente contratada e atualmente em uso. Para tanto, seria desprezado o investimento já realizado pelo Ministério, tanto na tecnologia hoje em uso, quanto na capacitação e preparação dos servidores e colaboradores.

Análise da Solução	**Pontos Positivos da Solução:** • Utilização de equipamentos novos, modernos e atualizados, de primeiro uso; • Equipamentos serão adquiridos, isto é, serão incorporados ao patrimônio público a cargo do MMFDH; • Remota possibilidade de interrupção dos serviços após a finalização do contrato, ainda que não se tenha concluído novo certamente para renovação dos serviços de garantia e suporte técnico. **Pontos Negativos da Solução:** • Necessidade de trâmites burocráticos com a apropriação dos bens ao patrimônio do órgão; • Preço estimado significativo, não se apresenta como uma das soluções mais baratas disponíveis. • Não aproveitamento dos equipamentos já existente do Ministério.

Custo Total de Propriedade – Memória de Cálculo

Para fins de comparativo preliminar de preços, foi feita consulta, tendo sido identificadas soluções contratadas, de dois fabricantes distintos, cujos objetos possuem características técnicas similares àquelas esperadas para este cenário, e cujos valores são consolidados a seguir, constituindo uma média estimativa:

Empresa	**Órgão**	**Data da Compra**	**Valor para 12 meses**
Citrix Systems	TJ-RJ UASG - 30100 - PE 46/2021 (2912365) - (Itens 1, 2, 3, 4, 7)	01/09/2021	612.852,84
Alsar Tecnologia em Redes	AGU - 110102 - PE 02/2021 (3182519) - (Item 1)	23/12/2021	898.000,00
Média aritmética			**755.426,42**

Na análise em questão, foi considerada como baliza a média aritmética dos valores anuais das contratações obtidas, de modo a projetar a expectativa preliminar de preço de eventual nova contratação.

Os valores anuais utilizados como referência foram obtidos da seguinte forma:

- PE 46/2021 - TJ/RJ (2912365), cuja reunião dos itens 1, 2, 3, 4 e 7 corresponde ao objeto de estudo deste cenário. Para obtenção da estimativa anual preliminar foram somados os valores correspondentes aos itens supracitados, tendo sido divido o resultado por 51 (quantidade de meses do contrato) e multiplicado por 12 (quantidade de meses anuais), conforme tabela a seguir:

Item	**Nome do Material**	**Quant.**	**Valor Unit.**	**Valor Total**
1	APPLIANCE BALANCEADOR DE APLICAÇÃO	2	485.000,00	970.000,00
2	SOLUÇÃO DE GERENCIAMENTO	1	100.000,00	100.000,00

3	SERVIÇO DE IMPLANTAÇÃO/MIGRAÇÃO DA SOLUÇÃO	1	44.624,45	44.624,45
4	SERVIÇO DE SUPORTE TÉCNICO (51 meses)	1	500.000,00	500.000,00
7	SERVIÇO DE GARANTIA DA SOLUÇÃO (51 meses)	1	990.000,00	990.000,00
TOTAL CONTRATADO PARA 51 MESES = "A"				2.604.624,45
VALOR PROPORCIONAL RELATIVO A 1 MÊS "B" = (A/51)				51.071,07
VALOR PROPORCIONAL RELATIVO A 12 MESES "C" = (B*12)				**612.852,84**

- PE 02/2021 - AGU (3182519), cujo item 1 corresponde ao objeto de estudo deste cenário, com valor de R$ 898.000,00.

Portanto, neste cenário, e considerando a média aritmética dos valores obtidos, a solução pretendida possuiria **valor anual de R$ 755.426,42 (setecentos e cinquenta e cinco mil quatrocentos e vinte e seis reais e quarenta e dois centavos).**

Solução Viável 3 - Cenário 3	
Descrição	**Modernização da Solução de Balanceamento de Carga de Servidores e Solução de Segurança Web existente, incluindo renovação do suporte técnico e expansão do licenciamento.**
Análise da Solução	Trata-se da modernização da solução existente, por intermédio da renovação do suporte e garantia dos equipamentos já adquiridos, associada à expansão das funcionalidades, para adequação tecnológica do ambiente atual do Ministério. Esta forma de contratação é comumente utilizada na Administração Pública Federal, por possuir grandes vantagens como preservação do investimento já realizado, redução de custos com novas aquisições, otimização da força de trabalho, e aproveitamento do conhecimento técnico já adquirido na utilização da tecnologia de balanceamento existente no Ministério. **Pontos Positivos da Solução:** • Infraestrutura de TIC existente adequada para suportar os serviços providos. • Continuidade dos serviços e ferramentas utilizadas pelos usuários do Órgão. • Segurança dos equipamentos servidores, seus componentes e de suas aplicações. • Integridade dos dados e informações disponibilizadas. • Aprimoramento da camada de proteção contra fraudes e ameaças digitais. • Valor da contratação ser mais vantajoso para o Ministério **Pontos Negativos da Solução:**

	• Limitação do tempo de extensão da garantia, haja vista a "idade" dos equipamentos, considerando que já se passaram 36 meses desde a sua produção, o que, com eventual renovação, elevará o seu tempo de vida útil a 72 meses.

Custo Total de Propriedade – Memória de Cálculo

Para fins de comparativo preliminar de preços, foi identificada solução cujo objeto dos itens 1 e 2 possui características técnicas similares àquelas esperadas para este cenário, sendo, pois, o **Pregão Eletrônico nº 12/2021 - UASG 440001, do Ministério do Meio Ambiente (2912367)**.

O objeto do certame é a "Contratação de empresa especializada na prestação de serviços de garantia, suporte e manutenção técnica on-site para solução de tratamento e entrega de dados BIG-IP F5 e licenciamento do módulo IP Intelligence por 36 (trinta e seis) meses".

Os valores anuais utilizados como referência foram obtidos da seguinte forma:

ITEM	DESCRIÇÃO	UND	QTD	VALOR UNITÁRIO	TOTAL
1	Renovação de Garantia e Suporte para a solução de tratamento e entrega de dados F5 BIG-IP (3 anos)	Serviço por equipamento	2	198.000,00	396.000,00
2	Manutenção especializada 24x7 para solução de tratamento e entrega de dados F5 BIG-IP	Serviço mensal	36	8.250,00	297.000,00
TOTAL CONTRATADO PARA 36 MESES = "A"					693.000,00
VALOR PROPORCIONAL RELATIVO A 1 MÊS "B" = (A/36)					19.250,00
VALOR PROPORCIONAL RELATIVO A 12 MESES "C" = (B*12)					**231.000,00**

Neste cenário, a solução pretendida possuiria **valor anual de R$ 231.000,00 (duzentos e trinta e um mil reais).**

Tabela 5 - Comparação Solução Balanceamento de Carga de Servidores e Solução de Segurança Web

11.2.2. Expansão do licenciamento da Solução existente.

11.2.2.1. Os cenários detalhados no item 3.2.2 (Soluções 1, 2 e 3) tratam da análise relativa às soluções de balanceamento que possuem o potencial de atender à demanda existente e às possíveis formas de manter suas funcionalidades, seja contratando em forma de serviço, de aquisição de nova solução, ou ainda, estendendo-se o suporte técnico e garantia dos bens já adquiridos.

11.2.2.2. Por outro lado, o Ministério possui hoje a necessidade de incrementar a solução existente, de modo que passe a contemplar também os serviços em nuvem, conforme detalhado no Anexo - A deste Estudo Técnico Preliminar.

11.2.2.3. Sendo assim, apresenta-se a seguir a estimativa preliminar para o item 2 do presente estudo.

11.2.2.4. Importante destacar que, para a correta composição dos preços preliminares da contratação ora em estudo, o valor obtido na tabela a seguir será acrescido aos valores de todos os cenários cujas soluções são viáveis, criando, assim, uma solução fidedigna ao que se tem como adequada para atender à necessidade atual do Ministério.

Expansão do Licenciamento	
Descrição	**Complementação do objeto das Soluções Viáveis, com o incremento do licenciamento do módulo F5 BIG-IP Virtual Edition.**
Análise da Solução	Trata-se da expansão do licenciamento já existente, de forma a agregar funcionalidades de segurança, desempenho, disponibilidade e abordagem a ameaças avançadas nos serviços de nuvem. Portanto, para otimização do uso da ferramenta, e considerando que o Ministério já possui contrato de serviços de computação em nuvem, bem como tem previsão de ampliar essa contratação, será incluído no certame a expansão para o licenciamento do módulo F5 BIG-IP Virtual Edition.

Custo Total de Propriedade – Memória de Cálculo

Para fins de estimativa preliminar de preços, foi identificada contratação cujo objeto possui características técnicas similares àquelas do módulo F5 BIG-IP Virtual Edition, objeto do item 2 do presente estudo (tabela do item 2.5.1), sendo, pois, o **Pregão Eletrônico nº 16/2021 - UASG 200334, da Escola Superior do Ministério Público da União (2912368)**, que será utilizado como paradigma.

O objeto do certame é a "Renovação da garantia e suporte técnico para a solução de tratamento de dados e acelerador de aplicações F5 BIG-IP Virtual Edition, por um período de 36 (trinta e seis meses).

ITEM	DESCRIÇÃO	QTD	VALOR UNITÁRIO	TOTAL
1	Extensão de Garantia e Direitos de Atualização do Tipo ‘Standard’ para Cluster de VE Best Bundle 5G (part number F5-SVC- BIGVE+STDL13) e IP Intelligence (part number F5-SBS-BIGVEIPI23YR) por 36 (trinta e seis) meses.	1	276.825,00	276.825,00
2	Serviço de Suporte Técnico Mensal – Especializado - 24x7 Ilimitado por 36 meses	1	214.290,00	214.290,00
TOTAL CONTRATADO PARA 36 MESES = "A"				491.115,00
VALOR PROPORCIONAL RELATIVO A 1 MÊS "B" = (A/36)				13.642,08
VALOR PROPORCIONAL RELATIVO A 12 MESES "C" = (B*12)				**163.704,96**

Neste cenário, a solução pretendida possuiria **valor anual de R$ 163.704,96 (cento e sessenta e três mil setecentos e quatro reais e noventa e seis centavos).**

Tabela 6 - Comparação Expansão do Licenciamento

11.3. Portanto, face à criticidade dessas aplicações e ao crescimento exponencial dos serviços em nuvem, é imprescindível que se tenha à disposição do Ministério um contrato de suporte e manutenção para os equipamentos citados, garantindo o balanceamento, a segurança e a otimização do tráfego destinado aos Sistemas e Aplicações de Tecnologia da Informação do MMFDH, aliado à garantia da disponibilidade e segurança do tráfego para os serviços em nuvem.

11.4. Ainda, considerando os avanços tecnológicos, é imprescindível que sejam avaliadas opções de expansão e modernização da solução existente.

11.5. Para fins de composição do Mapa Comparativo dos Cálculos Totais de Propriedades, e de modo que se obtenha um preço estimado fidedigno, o valor relativo à expansão será acrescido às estimativas obtidas para cada cenário, conforme a seguir:

11.5.1. Solução Viável 1 - **R$ 1.164.831,00** (Valor anual estimado para contratação de nova solução, no formato de serviço) **+ R$ 163.704,96** (valor anual estimado para expansão do licenciamento) **= R$ 1.328.535,96 (um milhão, trezentos e vinte e oito mil quinhentos e trinta e cinco reais e noventa e seis centavos).**

11.5.2. Solução Viável 2 - **R$ 755.426,42** (Valor anual estimado para aquisição de nova solução, no formato de hardware) **+ R$ 163.704,96** (valor anual estimado para expansão do licenciamento) **= R$ 919.131,38 (novecentos e dezenove mil cento e trinta e um reais e trinta e oito centavos).**

11.5.3. Solução Viável 3- **R$ 231.000,00** (Valor anual estimado para extensão do licenciamento existente) **+ R$ 163.704,96** (valor anual estimado para expansão do licenciamento) **= R$ 394.704,96 (trezentos e noventa e quatro mil setecentos e quatro reais e noventa e seis centavos).**

11.6. Os dados mencionados no item acima são apenas uma estimativa, visto que os valores reais só poderão ser confirmados após a conclusão do processo licitatório.

11.7. MAPA COMPARATIVO DOS CÁLCULOS TOTAIS DE PROPRIEDADE (TCO)

11.8. Considerando-se os valores obtidos preliminarmente nos itens 5.3 a 5.6.3 supra, apresenta-se a seguir os custos totais de propriedade para a renovação e expansão do licenciamento.

Descrição da Solução	**Estimativa de TCO ao longo dos anos**			**Total estimado**
	Ano 1	**Ano 2**	**Ano 3**	
Solução Viável 1	R$ 1.328.535,96	R$ 1.328.535,96	R$ 1.328.535,96	R$ 3.985.607,88
Solução Viável 2	R$ 919.131,38	R$ 919.131,38	R$ 919.131,38	R$ 2.727.394,14
Solução Viável 3	R$ 394.704,96	R$ 394.704,96	R$ 394.704,96	R$ 1.184.114,88

Tabela 9 - Quantitativo estimado ao longo dos anos

11.9. Considerando o comparativo acima, o resultado dos estudos demonstra que, ao longo de 3 anos, é certamente mais vantajosa a Modernização da Solução de Balanceamento de Carga de Servidores e Solução de Segurança Web existente, incluindo renovação do suporte técnico e expansão do licenciamento.

11.10. Desse modo, fica evidenciado que a melhor alternativa para a contratação proposta é a renovação e expansão do licenciamento atual, visto que, além de possibilitar a manutenção de toda a solução atualizada em suas últimas versões disponíveis, garante a preservação do investimento já feito.

11.11. Tendo em vista a situação orçamentária, dentre outras questões técnicas, a contratação pretensa será formalizada para o período de 36 (trinta e seis) meses.

12. Descrição da solução de TIC a ser contratada

12.1. Solução Viável 3 - Modernização da Solução de Balanceamento de Carga de Servidores e Solução de Segurança Web existente, incluindo renovação do suporte técnico e expansão do licenciamento.

12.1.1. Trata-se da contratação de extensão do suporte técnico, licenciamento e atualização de versão da Solução de Balanceamento de Carga de Servidores e Solução de Segurança Web - F5 Networks BIG IP i2800 Best Bundle existente, de modo que passe a contar com as licenças mais atuais e estáveis disponibilizadas pelo fabricante, bem como seja restabelecido o serviço de suporte técnico e garantia, na modalidade 24 x 7 (vinte e quatro horas, sete dias por semana).

12.1.2. Ainda, tem-se a expansão do licenciamento, de modo a contemplar os serviços em nuvem hoje em uso pelo Ministério, mantendo-se segurança e disponibilidade do acesso, tanto ambiente local quanto ao ambiente em nuvem.

12.1.3. A solução proposta se compõe de um grupo com dois itens, conforme a seguir:

Grupo	Item	Descrição	Unid. Medida	Quant.
1	1	Extensão do suporte técnico, licenciamento e atualização de versão da Solução de Balanceamento de Carga de Servidores e Solução de Segurança Web - F5 Networks BIG IP i2800 Best Bundle, por 36 meses	Unid.	2
	2	Expansão do licenciamento da Solução de Balanceamento de Carga de Servidores e Solução de Segurança Web - módulo F5 BIG-IP Virtual Edition, com suporte técnico e atualização de versão por 36 meses	Unid.	1

Tabela 10 - Solução escolhida

12.1.3.1. A solução proposta para o item 1 trata de serviço de suporte técnico e atualização de versão das licenças hoje instalada nos equipamentos. Para este item, será entregue pela futura contratada um certificado que comprove a atualização das licenças do F5 Networks BIG IP i2800 Best Bundle para a última versão estável disponibilizada pelo fabricante à época da contratação, pelo período 36 meses.

12.1.3.2. A solução proposta para o item 2 trata do fornecimento, no formato de subscrição, de licenciamento do módulo de Balanceamento de Carga de Servidores e Solução de Segurança Web. Para este item, será entregue pela futura contratada um certificado de licenciamento do módulo F5 BIG-IP Virtual Edition por 36 meses.

12.1.4. Destaca-se que o fabricante da solução a ser contratada possui renome internacional, e opera de forma global, havendo, no Brasil, mais de uma dezena de representante autorizados a comercializar seus produtos, conforme pode ser observado no site da empresa em: https://www.f5.com/partners/find-a-partner?partnerLocation=Brazil&partnerPage=1.

12.2. Justificativa da solução escolhida

12.2.1. Tendo em vista as análises constantes do presente documento, constata-se que o objeto que melhor atende à necessidade é a Contratação de Modernização da Solução de Balanceamento de Carga de Servidores e Solução de Segurança Web existente, incluindo renovação do suporte técnico e expansão do licenciamento.

12.2.2. Essa solução garante a distribuição uniforme da carga de conexões geradas pelos usuários dos sistemas, permitindo otimizar utilização de recursos, maximizar o desempenho e minimizar o tempo de resposta, evitando a sobrecarga dos servidores das aplicações. Além disso, a solução possui diversas camadas de segurança para proteção dos ativos de informações publicados externamente. Importa ressaltar que a solução, apesar de disponibilizar mais camadas de segurança, não se confunde com as soluções de antivírus, visto que essas possuem aplicação totalmente diversa de uma solução de balanceamento.

12.2.3. O MMFDH já adquiriu no passado solução deste tipo e a utiliza até hoje. Com a continuidade da utilização da solução de balanceamento, espera-se que todos os serviços disponibilizados para a sociedade possam continuar a serem prestados com eficiência e eficácia, mantendo o ambiente tecnológico do órgão o mais distribuído e seguro possível, aumentando assim, a sua capacidade operacional.

12.2.4. A contratação também contempla a garantia para os equipamentos, atualização de novas versões de software e suporte técnico para toda solução, por um período de 36 (trinta e seis) meses.

12.2.5. A forma de contratação aqui proposta é comumente utilizada na Administração Pública Federal, por possuir grandes vantagens como preservação do investimento já realizado, redução de custos com aquisição de plataformas diversas e com

integração de ferramentas, otimização da força de trabalho, e aproveitamento do conhecimento técnico já adquirido na utilização da tecnologia de balanceamento existente no Ministério.

12.2.6. A solução escolhida mantém todos os recursos da ferramenta já existente no Ministério, a qual fornece disponibilidade, o desempenho e a segurança, conforme tabela abaixo:

Recuso	Descrição do Recurso
BIG-IP Access Policy Manager	Protege, simplifica e protege o acesso do usuário a aplicativos e dados
BIG-IP Advanced Firewall Manager	Protege sua rede contra ameaças recebidas, incluindo ataques DDOS complexos
BIG-IP Advanced WAF	Protege aplicativos com análise comportamental, defesa de bot e criptografia de camada de aplicativo
BIG-IP Carrier-Grade NAT (CGNAT)	Gerenciamento de endereços IP IPv4/IPv6 rápido, escalável e seguro como parte de um conjunto de funções consolidadas
BIG-IP DNS	Fornece hiperescala e segurança durante altos volumes de consulta e ataques DNS DDoS
BIG-IP Local Traffic Manager	Gerencia o tráfego de rede para que os aplicativos estejam sempre rápidos, disponíveis e seguros
BIG-IP Policy Enforcement Manager	Melhora o desempenho da rede por meio do gerenciamento eficaz de políticas
BIG-IP Service Proxy para Kubernetes	Fornece controle, segurança e visibilidade de sinalização de entrada/saída multiprotocolo para 5G nativo da nuvem
BIG-IP SSL Orchestrator	Maximiza a eficiência e a segurança da infraestrutura com criptografia/descriptografia e direcionamento de tráfego
Container Ingress Services	Fornece serviços de automação, orquestração e rede para implantações de contêiner

Tabela 11 - fonte: https://www.f5.com/products/big-ip-services

12.2.7. No aspecto qualitativo a solução escolhida mantem posicionado de forma satisfatória em pesquisa e consultoria em TI, podemos observar no Gartner.

Imagem 2 - Quadrante Mágico da Gartner em Application Delivery Controllers (ADC)

12.3. Benefícios a serem alcançados

Id	Benefício Esperado	Tipo
1	Regularidade do ambiente computacional do MMFDH, em obediência ao regime de proteção da propriedade intelectual;	Eficiência
2	Gerenciamento do parque tecnológico;	Eficácia
3	Suporte e direito de atualização contínua;	Efetividade
4	Ganho de colaboração e produtividade;	Economicidade
5	Melhor nível de segurança, integridade e consistência do tráfego de dados e informações no ambiente do Ministério;	Eficiência

6	Alta disponibilidade dos serviços e sistemas mantidos pelo MMFDH;	Eficácia
7	Diminuição de custos futuros, uma vez que contratos subsequentes poderão contemplar apenas a aquisição da opção de atualização dos softwares já adquiridos;	Efetividade

Tabela 12 - Benefícios Esperados

12.4. Necessidades de adequação do ambiente para execução contratual

a) Preparação e disponibilização de ambiente virtual adequado para receber a solução.

12.5. Recursos necessários à continuidade do negócio durante e após a execução do contrato

12.5.1. Recursos humanos

a) Os recursos humanos internos a serem alocados se referem aos fiscais técnico, administrativo e gestor do contrato que devem realizar suas atividades de acompanhamento e controle, conforme definido na IN nº 01/2019.

b) Técnico da contratada de Sustentação de Ambiente de TIC.

c) Servidores do Ministério serão alocados para realização de definições, acompanhamento e gestão da solução.

6.5.2. Recursos Materiais

6.5.2.1. Não será necessária a disponibilização de recurso material específico para receber a solução contratada.

12.6. Estratégia de continuidade contratual

12.6.1. Para assegurar a continuidade da solução, acionar-se-á as seguintes ações para os eventos apresentados na tabela abaixo.

ID	Evento	Ação Preventiva	Responsáveis	Ação de Contingência	Responsáveis
01	Inexecução do Contrato	Fiscalização adequada dos níveis de serviço	CGTI	Acionamento contratual	Gestor do Contrato
02	Encerramento ordinário do contrato	Realização de processo de renovação tempestiva.	Gestor do Contrato	Prorrogação do ajuste	CGTI
03	Encerramento sem possibilidade de renovação.	Realizar novo planejamento.	CGTI	Realizar novo processo de planejamento e contratação dos serviços.	CGTI

Tabela 13 - Eventos

13. Estimativa de custo total da contratação

Valor (R$): 625.704,96

13.1. Considerando-se os valores iniciais obtidos, apresenta-se a seguir o valor estimado para a contratação:

Grupo	Item	Descrição	Medida	Qtd.	Valor Total 12 Meses	Valor Total 36 Meses

1	1	Extensão do suporte técnico, licenciamento e atualização de versão da Solução de Balanceamento de Carga de Servidores e Solução de Segurança Web - F5 Networks BIG IP i2800 Best Bundle, por 36 meses	Unid.	2	462.000,00***	1.386.000,00
	2	Expansão do licenciamento da Solução de Balanceamento de Carga de Servidores e Solução de Segurança Web - módulo F5 BIG-IP Virtual Edition.	Unid.	1	163.704,96	491.114,88
VALOR TOTAL					**R$ 625.704,96**	**R$ 1.877.114,88**

Tabela 14 - Valor estimado para contração

(231.000,00 *2)

13.2. De acordo com os valores preliminares apresentados, estima-se que a contratação terá valor máximo anual de R$ 625.704,96 (seiscentos e vinte e cinco mil setecentos e quatro reais e noventa e seis centavos), e por 3 (três) anos **R$ 1.877.114,88 (Um milhão, oitocentos setenta e sete cento e quatorze e oitenta e oito reais).**

13.3. Destaca-se que esses valores correspondem a uma pesquisa inicial, para fins de definição da melhor ferramenta a ser licitada, do ponto de vista técnico-econômico.

14. Justificativa técnica da escolha da solução

14.1. Um dos meios de comunicação utilizado pelo Ministério, tanto para fins institucionais quanto para relacionamento com a sociedade, é a internet. A utilização deste meio de comunicação requer um mecanismo de constante atualização tecnológica e segurança operacional, com a finalidade de assegurar a continuidade e a manutenção dos serviços prestados. O presente processo visa a solução de Balanceamento de Carga de Servidores e Segurança para as Aplicações Web do Ministério da Mulher, Família e dos Direitos Humanos - MMFDH. Tendo em vista a relevância das informações coletadas, é de extrema importância que a infraestrutura computacional do Ministério acompanhe as mudanças e atualizações necessárias. Além disso, o Ministério necessita também que a infraestrutura garanta estabilidade, segurança, alta-disponibilidade e agilidade na utilização e no armazenamento de dados.

15. Justificativa econômica da escolha da solução

15.1. Sob o ponto de vista financeiro, a modernização pretendida permitirá ao Ministério agregar disponibilidade, desempenho e qualidade de serviços a todo o corpo funcional, dando um salto qualitativo na adoção de soluções que visam atender de forma eficiente e racional à demanda operacional interna.
15.2. Em suma, a contratação objetiva otimizar a solução da entrega de produtos a sociedade, com efetividade e racionalidade de gasto.

16. Benefícios a serem alcançados com a contratação

16.1. Satisfação dos clientes e usuários de serviço de TIC.

16.2. Infraestrutura de TIC adequada para suportar os serviços providos.

16.3. Continuidade dos serviços e ferramentas utilizadas pelos usuários do Órgão.

16.4. Disponibilidade, manutenção e suporte do licenciamento existente.

16.5. Segurança dos equipamentos servidores, seus componentes e de suas aplicações.

15.6. Integridade dos dados e informações disponibilizadas.

16.7. Aprimoramento da camada de proteção contra fraudes e ameaças digitais.

17. Providências a serem Adotadas

17.1. Ocorrerá a designação formal pelas autoridades competentes do gestor da execução contratual e fiscais responsáveis pela fiscalização técnica, administrativa e setorial, se for o caso, e seus substitutos.
17.2. O contrato será administrado pela Coordenação de Contratos e Gestão de Atas/CGL/SOAD/MMFDH.

18. Declaração de Viabilidade

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

18.1. Justificativa da Viabilidade

A Equipe de Planejamento da Contratação, devidamente nomeada pela Autoridade Competente, optou pela Solução do Cenário 3, conforme justificativas e benefícios contidos no tópico "6. Descrição de TIC a ser contratada".

Diante de todo o exposto, a Equipe de Planejamento da Contratação declara a **VIABILIDADE** da contratação da solução demandada.

Em cumprimento ao disposto no Art. 11 da Instrução Normativa SGD/ME N° 1/2019, o presente documento segue assinado pelos Integrantes Requisitante e Técnico da Equipe de Planejamento da Contratação, designada pela Portaria nº 23, de 29 de setembro de 2022 (SEI nº 3206603).

Por fim, propomos o encaminhamento do presente estudo técnico, para análise e considerações da autoridade competente.

19. Responsáveis

DAVID SANTOS ABREU
Coordenador

HENRIQUE ALCANTARA VELOSO MOTA
Assessor Técnico Especializado

ARTUR HENRIQUE CASTRO DE ANDRADE
Coordenador Geral de Tecnologia da Informação

LORENA FERRER C. R. POMPEU
Subsecretária de Orçamento e Administração

Lista de Anexos

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

- Anexo I - ANEXO A.pdf (1.34 MB)

Anexo I - ANEXO A.pdf

ANEXO A - ESPECIFICAÇÕES TÉCNICAS DA SOLUÇÃO EXISTENTE

Apresentam-se a seguir as evidências da solução existente, bem como dos serviços em nuvem em uso pelo Ministério:

Relatório demonstrando o tipo das licenças do F5 atualmente - Relatório MDH –

General Properties

License Type	Production
Licensed Date	Mar 12, 2021
Active Modules	• Local Traffic Manager, i2600(Perpetual) (XBJMBLB-PHLYNRS) • Rate Shaping • Carrier Grade NAT (AFM ONLY) • APM, Limited • Protocol Security Manager • Routing Bundle • DNSSEC • Anti-Virus Checks • Base Endpoint Security Checks • Firewall Checks • Network Access • Secure Virtual Keyboard • APM, Web Application • Machine Certificate Checks • Protected Workspace • Remote Desktop • App Tunnel • GTM Licensed Objects, Unlimited • DNS Rate Fallback, Unlimited • DNS Licensed Objects, Unlimited • GTM Rate Fallback, (UNLIMITED) • DNS Rate Limit, Unlimited QPS • GTM Rate, Unlimited • Max SSL, i2600 • Max Compression, i2600 • LTM to Best Upgrade, i28XX(Perpetual) (HGZHBBL-OWZBBOT) • BIG-IP, DNS (Max) • Application Security Manager, i2XXX • Advanced Firewall Manager, i2XXX • Access Policy Manager, Base, i28XX • DNSSEC • Anti-Virus Checks • Base Endpoint Security Checks • Firewall Checks • Network Access • Secure Virtual Keyboard • APM, Web Application • Machine Certificate Checks • Protected Workspace • Remote Desktop • App Tunnel • GTM Licensed Objects, Unlimited • DNS Rate Fallback, Unlimited • DNS Licensed Objects, Unlimited • GTM Rate Fallback, (UNLIMITED) • DNS Rate Limit, Unlimited QPS • GTM Rate, Unlimited • Carrier Grade NAT (AFM ONLY) • Protocol Security Manager • Routing Bundle • Performance Upgrade, i26XX to i28XX(Perpetual) (JJIMSIZ-AMVPQHF) • SSL, Forward Proxy, 2XXX/i2XXX(Perpetual) (OMZBKIN-MGKKKHS)
Optional Modules	• Access Policy Manager, Base, i26XX • Access Policy Manager, Max, i26XX • Advanced Firewall Manager, i2XXX • Advanced Protocols • Advanced Web Application Firewall, i2XXX • Anti-Bot Mobile, i2XXX • App Mode (TMSH Only, No Root/Bash) • Application Security Manager, i2XXX • ASM to AWF Upgrade, i2XXX

License F5:

General Properties

	• BIG-IP, DNS (1K) • BIG-IP, DNS and GTM Upgrade (1K TO MAX) • BIG-IP, Multicast Routing • BIG-IP, Privileged User Access, 100 Endpoints • BIG-IP, Privileged User Access, 1000 Endpoints • BIG-IP, Privileged User Access, 250 Endpoints • BIG-IP, Privileged User Access, 50 Endpoints • BIG-IP, Privileged User Access, 500 Endpoints • Carrier Grade NAT, i2XXX • DataSafe, i2XXX • DNS Services • External Interface and Network HSM • Intrusion Prevention System, i2XXX • IP Intelligence, 1Yr, 1600 • IP Intelligence, 1Yr, 2XXX/i2XXX/3600 • IP Intelligence, 3Yr, 1600 • IPS, 1Yr, i2XXX / i4XXX • IPS, 3Yr, i2XXX / i4XXX • Link Controller • RAX Module Add-on, i2600 • Routing Bundle • SM2 SM3 SM4, i-Series • SSL Orchestrator, 2XXX/i2XXX • URL Filtering, 1Yr, 2000s/i26XX • URL Filtering, 3Yr, 2000S/I26XX • VPN Users
Inactive Modules	• IP Intelligence, 3Yr, 2XXX/i2XXX/3600 (KLANHQT-LGSKZYX) • Subscription expired Nov 14, 2021

Relatório com os serviços em uso/contratados de nuvem - Relatório Trafego-o365 - SaaS:

Trafego-SaaS

Panorama : 2022/04/09 11:37:10 - 2022/05/09 11:37:09

Application Name	App Sub Category	Bytes
outlook-web-online	email	1.84 T
ms-teams-audio-video	office-programs	1.12 T
sharepoint-online	social-business	619.72 G
ms-onedrive-base	file-sharing	236.90 G
ms-teams	office-programs	136.74 G
ms-office365-base	office-programs	53.57 G
office365-enterprise-access	office-programs	33.13 G
sharepoint-online-downloading	social-business	9.32 G

e Relatório Trafego-VPN-Azure:

Trafego-VPN-Azure

Panorama : 2022/04/09 11:25:21 - 2022/05/09 11:25:20

Day Received	Source Zone	Destination Zone	Source address	Source Host Name	Destination address	Destination Host Name	Bytes Received	Bytes Sent	Bytes
Fri, Apr 29, 2022	Z-INT_INTERNA	Z-EXT-VPN-AZURE	10.102.9.180	10.102.9.180	172.16.168.6	172.16.168.6	102.47 M	6.73 G	6.84 G
	Z-INT_INTERNA	Z-EXT-VPN-AZURE	10.102.9.105	10.102.9.105	172.16.168.6	172.16.168.6	3.97 M	2.92 M	6.90 M
	Z-INT_INFOVIA-BLOCO_A	Z-EXT-VPN-AZURE	10.223.10.119	10.223.10.119	172.16.170.254	172.16.170.254	1.51 M	2.17 M	3.69 M
	Z-INT_INTERNA	Z-EXT-VPN-AZURE	10.102.11.124	10.102.11.124	172.16.168.6	172.16.168.6	383.58 k	359.98 k	743.56 k
	Z-EXT-VPN-AZURE	Z-EXT-VPN-AZURE	146.88.240.4	www.arbor-observatory.com	189.9.36.168	189.9.36.168	0	3.85 k	3.85 k
	Z-EXT-VPN-AZURE	Z-EXT-VPN-AZURE	185.151.107.102	unassigned-please-contact-hostmaster.uk/hub.net	189.9.36.168	189.9.36.168	0	3.20 k	3.20 k
	Z-EXT-VPN-AZURE	Z-EXT-VPN-AZURE	194.233.90.223	vm861101.contaboserver.net	189.9.36.168	189.9.36.168	0	1.32 k	1.32 k
	Z-EXT-VPN-AZURE	Z-EXT-VPN-AZURE	184.105.247.195	scan-14.shadowserver.org	189.9.36.168	189.9.36.168	0	1.27 k	1.27 k
	Z-EXT-VPN-AZURE	Z-EXT-VPN-AZURE	66.94.109.198	vm857988.contaboserver.net	189.9.36.168	189.9.36.168	0	1.26 k	1.26 k
	Z-EXT-VPN-AZURE	Z-EXT-VPN-AZURE	155.146.96.69	155.146.96.69	189.9.36.168	189.9.36.168	510	510	1.02 k
	Z-EXT-VPN-AZURE	Z-EXT-VPN-AZURE	92.204.248.74	92.204.248.74	189.9.36.168	189.9.36.168	0	915	915
	Z-EXT-VPN-AZURE	Z-EXT-VPN-AZURE	195.154.200.146	195-154-200-146.rev.poneytelecom.eu	189.9.36.168	189.9.36.168	0	901	901
	Z-EXT-VPN-AZURE	Z-EXT-VPN-AZURE	154.53.51.8	vm833344.contaboserver.net	189.9.36.168	189.9.36.168	0	885	885
	Z-EXT-VPN-AZURE	Z-EXT-VPN-AZURE	148.153.135.178	148.153.135.178	189.9.36.168	189.9.36.168	408	408	816
	Z-EXT-VPN-AZURE	Z-EXT-VPN-AZURE	209.141.33.68	the.dark.reign.of.gothic.rock.re	189.9.36.168	189.9.36.168	0	714	714
	Z-EXT-VPN-AZURE	Z-EXT-VPN-AZURE	103.74.107.141	103.74.107.141	189.9.36.168	189.9.36.168	0	707	707
	Z-EXT-VPN-AZURE	Z-EXT-VPN-AZURE	52.175.130.141	52.175.130.141	189.9.36.168	189.9.36.168	0	637	637
	Z-EXT-VPN-AZURE	Z-EXT-VPN-AZURE	62.210.13.20	62-210-13-20.rev.poneytelecom.eu	189.9.36.168	189.9.36.168	0	504	504
	Z-EXT-VPN-AZURE	Z-EXT-VPN-AZURE	194.31.98.142	194.31.98.142	189.9.36.168	189.9.36.168	0	485	485
	Z-EXT-VPN-AZURE	Z-EXT-VPN-AZURE	151.106.15.82	151.106.15.82	189.9.36.168	189.9.36.168	0	459	459
	Z-EXT-VPN-AZURE	Z-EXT-VPN-AZURE	92.118.39.130	92.118.39.130	189.9.36.168	189.9.36.168	0	459	459
	Z-EXT-VPN-AZURE	Z-EXT-VPN-AZURE	85.95.241.192	192.241.95.85.datacenter-services.ixirtelekom.com.tr	189.9.36.168	189.9.36.168	0	457	457
	Z-EXT-VPN-AZURE	Z-EXT-VPN-AZURE	51.158.145.218	51-158-145-218.rev.poneytelecom.eu	189.9.36.168	189.9.36.168	0	451	451
	Z-EXT-VPN-AZURE	Z-EXT-VPN-AZURE	51.79.82.87	ns570119.ip-51-79-82.net	189.9.36.168	189.9.36.168	0	447	447
	Z-EXT-VPN-AZURE	Z-EXT-VPN-AZURE	192.241.221.70	zg-0421d-133.stretchoid.com	189.9.36.168	189.9.36.168	0	427	427
Wed, Apr 27, 2022	Z-INT_INTERNA	Z-EXT-VPN-AZURE	10.102.9.180	10.102.9.180	172.16.168.6	172.16.168.6	158.03 M	2.16 G	2.32 G
	Z-INT_INFOVIA-BLOCO_A	Z-EXT-VPN-AZURE	10.223.10.119	10.223.10.119	172.16.170.254	172.16.170.254	2.10 G	19.52 M	2.12 G
	Z-INT_INTERNA	Z-EXT-VPN-AZURE	10.102.11.124	10.102.11.124	172.16.168.6	172.16.168.6	660.32 k	621.51 k	1.28 M
	Z-INT_INTERNA	Z-EXT-VPN-AZURE	10.102.9.180	10.102.9.180	172.16.170.254	172.16.170.254	165.32 k	389.55 k	554.87 k
	Z-EXT-VPN-AZURE	Z-EXT-VPN-AZURE	146.88.240.4	www.arbor-observatory.com	189.9.36.168	189.9.36.168	0	4 k	4 k
	Z-EXT-VPN-AZURE	Z-EXT-VPN-AZURE	157.245.63.226	157.245.63.226	189.9.36.168	189.9.36.168	0	1.51 k	1.51 k
	Z-INT_INTERNA	Z-EXT-VPN-AZURE	10.102.9.105	10.102.9.105	189.9.36.163	189.9.36.163	444	948	1.39 k
	Z-EXT-VPN-AZURE	Z-EXT-VPN-AZURE	216.218.206.119	scan-06m.shadowserver.org	189.9.36.168	189.9.36.168	0	1.37 k	1.37 k
	Z-EXT-VPN-AZURE	Z-EXT-VPN-AZURE	155.146.96.69	155.146.96.69	189.9.36.168	189.9.36.168	510	510	1.02 k
	Z-EXT-VPN-AZURE	Z-EXT-VPN-AZURE	148.153.135.178	148.153.135.178	189.9.36.168	189.9.36.168	510	510	1.02 k
	Z-EXT-VPN-AZURE	Z-EXT-VPN-AZURE	62.210.13.20	62-210-13-20.rev.poneytelecom.eu	189.9.36.168	189.9.36.168	0	997	997
	Z-EXT-VPN-AZURE	Z-EXT-VPN-AZURE	195.154.200.146	195-154-200-146.rev.poneytelecom.eu	189.9.36.168	189.9.36.168	0	902	902
	Z-EXT-VPN-AZURE	Z-EXT-VPN-AZURE	66.94.109.198	vm857988.contaboserver.net	189.9.36.168	189.9.36.168	0	836	836
	Z-EXT-VPN-AZURE	Z-EXT-VPN-AZURE	103.74.107.141	103.74.107.141	189.9.36.168	189.9.36.168	0	643	643
	Z-EXT-VPN-AZURE	Z-EXT-VPN-AZURE	147.203.255.20	147.203.255.20	189.9.36.168	189.9.36.168	0	613	613
	Z-EXT-VPN-AZURE	Z-EXT-VPN-AZURE	51.89.124.57	ip57.ip-51-89-124.eu	189.9.36.168	189.9.36.168	0	483	483
	Z-EXT-VPN-AZURE	Z-EXT-VPN-AZURE	209.141.33.68	the.dark.reign.of.gothic.rock.re	189.9.36.168	189.9.36.168	0	476	476
	Z-EXT-VPN-AZURE	Z-EXT-VPN-AZURE	51.75.241.203	ns3131524.ip-51-75-241.eu	189.9.36.168	189.9.36.168	0	464	464
	Z-EXT-VPN-AZURE	Z-EXT-VPN-AZURE	134.119.184.118	134.119.184.118	189.9.36.168	189.9.36.168	0	463	463
	Z-EXT-VPN-AZURE	Z-EXT-VPN-AZURE	93.175.194.189	93.175.194.189	189.9.36.168	189.9.36.168	0	462	462
	Z-EXT-VPN-AZURE	Z-EXT-VPN-AZURE	173.59.115.148	static-173-59-115-148.phlapa.fios.verizon.net	189.9.36.168	189.9.36.168	0	459	459
	Z-EXT-VPN-AZURE	Z-EXT-VPN-AZURE	92.204.248.74	92.204.248.74	189.9.36.168	189.9.36.168	0	459	459
	Z-EXT-VPN-AZURE	Z-EXT-VPN-AZURE	49.249.21.58	static-58.21.249.49-tataidc.co.in	189.9.36.168	189.9.36.168	0	458	458
	Z-EXT-VPN-AZURE	Z-EXT-VPN-AZURE	104.223.56.130	unassigned.quadranet.com	189.9.36.168	189.9.36.168	0	458	458
	Z-EXT-VPN-AZURE	Z-EXT-VPN-AZURE	38.105.208.130	38.105.208.130	189.9.36.168	189.9.36.168	0	458	458
Tue, Apr 26, 2022	Z-INT_INTERNA	Z-EXT-VPN-AZURE	10.102.9.180	10.102.9.180	172.16.168.6	172.16.168.6	169.30 M	3.05 G	3.22 G
	Z-INT_INFOVIA-BLOCO_A	Z-EXT-VPN-AZURE	10.223.10.119	10.223.10.119	172.16.170.254	172.16.170.254	2.48 M	3.48 M	5.97 M
	Z-INT_INTERNA	Z-EXT-VPN-AZURE	10.102.11.124	10.102.11.124	172.16.168.6	172.16.168.6	137.32 k	115.85 k	253.18 k
	Z-EXT-VPN-AZURE	Z-EXT-VPN-AZURE	202.150.191.14	202.150.191.14	189.9.36.168	189.9.36.168	0	6.65 k	6.65 k
	Z-EXT-VPN-AZURE	Z-EXT-VPN-AZURE	146.88.240.4	www.arbor-observatory.com	189.9.36.168	189.9.36.168	0	3.85 k	3.85 k

	Z-INT_INTERNA	Z-EXT-VPN-AZURE	10.102.9.105	10.102.9.105	189.9.36.163	189.9.36.163	592	1.26 k	1.85 k
	Z-EXT-VPN-AZURE	Z-EXT-VPN-AZURE	184.105.247.238	scan-13k.shadowserver.org	189.9.36.168	189.9.36.168	0	1.27 k	1.27 k
	Z-EXT-VPN-AZURE	Z-EXT-VPN-AZURE	155.146.96.69	155.146.96.69	189.9.36.168	189.9.36.168	510	510	1.02 k
	Z-EXT-VPN-AZURE	Z-EXT-VPN-AZURE	148.153.135.178	148.153.135.178	189.9.36.168	189.9.36.168	510	510	1.02 k
	Z-EXT-VPN-AZURE	Z-EXT-VPN-AZURE	209.141.33.68	the.dark.reign.of.gothic.rock.re	189.9.36.168	189.9.36.168	0	952	952
	Z-EXT-VPN-AZURE	Z-EXT-VPN-AZURE	103.74.107.141	103.74.107.141	189.9.36.168	189.9.36.168	0	902	902
	Z-EXT-VPN-AZURE	Z-EXT-VPN-AZURE	195.154.200.146	195-154-200-146.rev.poneytelecom.eu	189.9.36.168	189.9.36.168	0	902	902
	Z-EXT-VPN-AZURE	Z-EXT-VPN-AZURE	51.79.82.87	ns570119.ip-51-79-82.net	189.9.36.168	189.9.36.168	0	890	890
	Z-EXT-VPN-AZURE	Z-EXT-VPN-AZURE	14.1.112.177	14.1.112.177	189.9.36.168	189.9.36.168	0	720	720
	Z-EXT-VPN-AZURE	Z-EXT-VPN-AZURE	45.79.42.210	45-79-42-210.ip.linodeusercontent.com	189.9.36.168	189.9.36.168	0	674	674
	Z-EXT-VPN-AZURE	Z-EXT-VPN-AZURE	62.210.13.20	62-210-13-20.rev.poneytelecom.eu	189.9.36.168	189.9.36.168	0	496	496
	Z-EXT-VPN-AZURE	Z-EXT-VPN-AZURE	51.89.124.57	ip57.ip-51-89-124.eu	189.9.36.168	189.9.36.168	0	483	483
	Z-EXT-VPN-AZURE	Z-EXT-VPN-AZURE	185.94.189.182	185.94.189.182	189.9.36.168	189.9.36.168	0	470	470
	Z-EXT-VPN-AZURE	Z-EXT-VPN-AZURE	185.182.184.120	vm852866.contaboserver.net	189.9.36.168	189.9.36.168	0	463	463
	Z-EXT-VPN-AZURE	Z-EXT-VPN-AZURE	218.248.29.102	218.248.29.102	189.9.36.168	189.9.36.168	0	461	461
	Z-EXT-VPN-AZURE	Z-EXT-VPN-AZURE	104.223.56.130	unassigned.quadranet.com	189.9.36.168	189.9.36.168	0	458	458
	Z-EXT-VPN-AZURE	Z-EXT-VPN-AZURE	92.204.248.74	92.204.248.74	189.9.36.168	189.9.36.168	0	458	458
	Z-EXT-VPN-AZURE	Z-EXT-VPN-AZURE	104.223.55.62	loosened.entersource.com	189.9.36.168	189.9.36.168	0	458	458
	Z-EXT-VPN-AZURE	Z-EXT-VPN-AZURE	92.118.39.84	92.118.39.84	189.9.36.168	189.9.36.168	0	456	456
	Z-EXT-VPN-AZURE	Z-EXT-VPN-AZURE	141.95.145.196	ns31492572.ip-141-95-145.eu	189.9.36.168	189.9.36.168	0	451	451
Mon, Apr 25, 2022	Z-INT_INTERNA	Z-EXT-VPN-AZURE	10.102.9.180	10.102.9.180	172.16.168.6	172.16.168.6	29.88 M	2.86 G	2.89 G
	Z-INT_INFOVIA-BLOCO_A	Z-EXT-VPN-AZURE	10.223.10.119	10.223.10.119	172.16.170.254	172.16.170.254	1.19 M	1.29 M	2.49 M
	Z-INT_INTERNA	Z-EXT-VPN-AZURE	10.102.11.124	10.102.11.124	172.16.168.6	172.16.168.6	443.30 k	411.69 k	854.99 k
	Z-EXT-VPN-AZURE	Z-EXT-VPN-AZURE	144.217.252.186	ns543332.ip-144-217-252.net	189.9.36.168	189.9.36.168	0	12.92 k	12.92 k
	Z-EXT-VPN-AZURE	Z-EXT-VPN-AZURE	146.88.240.4	www.arbor-observatory.com	189.9.36.168	189.9.36.168	0	3.76 k	3.76 k
	Z-EXT-VPN-AZURE	Z-EXT-VPN-AZURE	104.223.56.130	unassigned.quadranet.com	189.9.36.168	189.9.36.168	0	2.73 k	2.73 k
	Z-INT_INTERNA	Z-EXT-VPN-AZURE	10.102.9.105	10.102.9.105	189.9.36.163	189.9.36.163	666	1.42 k	2.08 k
	Z-EXT-VPN-AZURE	Z-EXT-VPN-AZURE	151.80.213.41	ip41.ip-151-80-213.eu	189.9.36.168	189.9.36.168	0	1.32 k	1.32 k
	Z-EXT-VPN-AZURE	Z-EXT-VPN-AZURE	14.1.112.177	14.1.112.177	189.9.36.168	189.9.36.168	0	1.28 k	1.28 k
	Z-EXT-VPN-AZURE	Z-EXT-VPN-AZURE	74.82.47.36	scan-11h.shadowserver.org	189.9.36.168	189.9.36.168	0	1.27 k	1.27 k
	Z-EXT-VPN-AZURE	Z-EXT-VPN-AZURE	209.141.33.68	the.dark.reign.of.gothic.rock.re	189.9.36.168	189.9.36.168	0	1.19 k	1.19 k
	Z-EXT-VPN-AZURE	Z-EXT-VPN-AZURE	62.210.13.20	62-210-13-20.rev.poneytelecom.eu	189.9.36.168	189.9.36.168	0	1.02 k	1.02 k
	Z-EXT-VPN-AZURE	Z-EXT-VPN-AZURE	148.153.135.178	148.153.135.178	189.9.36.168	189.9.36.168	510	510	1.02 k
	Z-EXT-VPN-AZURE	Z-EXT-VPN-AZURE	155.146.96.69	155.146.96.69	189.9.36.168	189.9.36.168	510	510	1.02 k
	Z-EXT-VPN-AZURE	Z-EXT-VPN-AZURE	134.119.184.118	134.119.184.118	189.9.36.168	189.9.36.168	0	917	917
	Z-EXT-VPN-AZURE	Z-EXT-VPN-AZURE	80.94.93.125	80.94.93.125	189.9.36.168	189.9.36.168	0	899	899
	Z-EXT-VPN-AZURE	Z-EXT-VPN-AZURE	92.118.39.12	92.118.39.12	189.9.36.168	189.9.36.168	0	896	896
	Z-EXT-VPN-AZURE	Z-EXT-VPN-AZURE	193.46.255.47	193.46.255.47	189.9.36.168	189.9.36.168	0	879	879
	Z-EXT-VPN-AZURE	Z-EXT-VPN-AZURE	103.74.107.141	103.74.107.141	189.9.36.168	189.9.36.168	0	643	643
	Z-EXT-VPN-AZURE	Z-EXT-VPN-AZURE	66.170.99.2	66.170.99.2	189.9.36.168	189.9.36.168	230	320	550
	Z-EXT-VPN-AZURE	Z-EXT-VPN-AZURE	51.89.124.57	51.89.124.57	189.9.36.168	189.9.36.168	0	483	483
	Z-EXT-VPN-AZURE	Z-EXT-VPN-AZURE	92.204.248.74	92.204.248.74	189.9.36.168	189.9.36.168	0	459	459
	Z-EXT-VPN-AZURE	Z-EXT-VPN-AZURE	92.118.39.130	92.118.39.130	189.9.36.168	189.9.36.168	0	459	459
	Z-EXT-VPN-AZURE	Z-EXT-VPN-AZURE	104.223.55.62	104.223.55.62	189.9.36.168	189.9.36.168	0	458	458
	Z-EXT-VPN-AZURE	Z-EXT-VPN-AZURE	135.181.80.156	135.181.80.156	189.9.36.168	189.9.36.168	0	457	457
Fri, May 6, 2022	Z-INT_INTERNA	Z-EXT-VPN-AZURE	10.102.9.180	10.102.9.180	172.16.168.6	172.16.168.6	121.13 M	2.49 G	2.61 G
	Z-INT_INFOVIA-BLOCO_A	Z-EXT-VPN-AZURE	10.223.10.119	10.223.10.119	172.16.170.254	172.16.170.254	9.32 M	10.52 M	19.85 M
	Z-INT_INTERNA	Z-EXT-VPN-AZURE	10.102.9.105	10.102.9.105	172.16.168.6	172.16.168.6	8.54 M	6.66 M	15.21 M
	Z-INT_INTERNA	Z-EXT-VPN-AZURE	10.102.11.124	10.102.11.124	172.16.168.6	172.16.168.6	686.19 k	644.16 k	1.33 M
	Z-EXT-VPN-AZURE	Z-EXT-VPN-AZURE	2.57.122.233	2.57.122.233	189.9.36.168	189.9.36.168	0	4.77 k	4.77 k
	Z-EXT-VPN-AZURE	Z-EXT-VPN-AZURE	185.151.107.102	185.151.107.102	189.9.36.168	189.9.36.168	0	4.48 k	4.48 k
	Z-EXT-VPN-AZURE	Z-EXT-VPN-AZURE	146.88.240.4	146.88.240.4	189.9.36.168	189.9.36.168	0	4.09 k	4.09 k
	Z-EXT-VPN-AZURE	Z-EXT-VPN-AZURE	2.57.122.19	2.57.122.19	189.9.36.168	189.9.36.168	0	3.43 k	3.43 k
	Z-EXT-VPN-AZURE	Z-EXT-VPN-AZURE	185.151.107.101	185.151.107.101	189.9.36.168	189.9.36.168	0	2.30 k	2.30 k
	Z-EXT-VPN-AZURE	Z-EXT-VPN-AZURE	71.6.199.23	71.6.199.23	189.9.36.168	189.9.36.168	0	1.27 k	1.27 k
	Z-EXT-VPN-AZURE	Z-EXT-VPN-AZURE	65.49.20.88	65.49.20.88	189.9.36.168	189.9.36.168	0	1.27 k	1.27 k
	Z-EXT-VPN-AZURE	Z-EXT-VPN-AZURE	209.141.32.204	209.141.32.204	189.9.36.168	189.9.36.168	0	1.19 k	1.19 k
	Z-EXT-VPN-AZURE	Z-EXT-VPN-AZURE	130.76.184.142	130.76.184.142	189.9.36.168	189.9.36.168	0	1.15 k	1.15 k
	Z-EXT-VPN-AZURE	Z-EXT-VPN-AZURE	148.153.135.178	148.153.135.178	189.9.36.168	189.9.36.168	510	510	1.02 k
	Z-EXT-VPN-AZURE	Z-EXT-VPN-AZURE	195.154.200.146	195.154.200.146	189.9.36.168	189.9.36.168	0	926	926
	Z-EXT-VPN-AZURE	Z-EXT-VPN-AZURE	163.172.49.67	163.172.49.67	189.9.36.168	189.9.36.168	0	919	919
	Z-EXT-VPN-AZURE	Z-EXT-VPN-AZURE	92.118.39.130	92.118.39.130	189.9.36.168	189.9.36.168	0	915	915

	Z-EXT-VPN-AZURE	Z-EXT-VPN-AZURE	103.74.107.141	103.74.107.141	189.9.36.168	189.9.36.168	0	902	902
	Z-EXT-VPN-AZURE	Z-EXT-VPN-AZURE	92.118.39.95	92.118.39.95	189.9.36.168	189.9.36.168	0	901	901
	Z-EXT-VPN-AZURE	Z-EXT-VPN-AZURE	80.94.93.125	80.94.93.125	189.9.36.168	189.9.36.168	0	896	896
	Z-EXT-VPN-AZURE	Z-EXT-VPN-AZURE	14.1.112.177	14.1.112.177	189.9.36.168	189.9.36.168	0	854	854
	Z-EXT-VPN-AZURE	Z-EXT-VPN-AZURE	155.146.96.69	155.146.96.69	189.9.36.168	189.9.36.168	306	306	612
	Z-EXT-VPN-AZURE	Z-EXT-VPN-AZURE	62.210.13.20	62.210.13.20	189.9.36.168	189.9.36.168	0	501	501
	Z-EXT-VPN-AZURE	Z-EXT-VPN-AZURE	198.211.116.238	198.211.116.238	189.9.36.168	189.9.36.168	0	461	461
	Z-EXT-VPN-AZURE	Z-EXT-VPN-AZURE	92.204.248.74	92.204.248.74	189.9.36.168	189.9.36.168	0	459	459
Sat, Apr 30, 2022	Z-INT_INTERNA	Z-EXT-VPN-AZURE	10.102.9.105	10.102.9.105	172.16.168.6	172.16.168.6	297.82 M	5.44 M	303.27 M
	Z-INT_INTERNA	Z-EXT-VPN-AZURE	10.102.9.180	10.102.9.180	172.16.168.6	172.16.168.6	20.21 M	2 M	22.21 M
	Z-INT_INFOVIA-BLOCO_A	Z-EXT-VPN-AZURE	10.223.10.119	10.223.10.119	172.16.170.254	172.19.170.254	5.98 M	3.91 M	9.90 M
	Z-INT_INTERNA	Z-EXT-VPN-AZURE	10.102.11.124	10.102.11.124	172.16.168.6	172.16.168.6	694.29 k	682.32 k	1.34 M
	Z-EXT-VPN-AZURE	Z-EXT-VPN-AZURE	146.88.240.4	146.88.240.4	189.9.36.168	189.9.36.168	0	3.92 k	3.92 k
	Z-EXT-VPN-AZURE	Z-EXT-VPN-AZURE	185.151.107.102	185.151.107.102	189.9.36.168	189.9.36.168	0	2.68 k	2.68 k
	Z-EXT-VPN-AZURE	Z-EXT-VPN-AZURE	65.108.46.62	65.108.46.62	189.9.36.168	189.9.36.168	0	1.36 k	1.36 k
	Z-EXT-VPN-AZURE	Z-EXT-VPN-AZURE	151.80.213.41	151.80.213.41	189.9.36.168	189.9.36.168	0	1.31 k	1.31 k
	Z-EXT-VPN-AZURE	Z-EXT-VPN-AZURE	66.94.109.198	66.94.109.198	189.9.36.168	189.9.36.168	0	1.27 k	1.27 k
	Z-EXT-VPN-AZURE	Z-EXT-VPN-AZURE	184.105.139.87	184.105.139.87	189.9.36.168	189.9.36.168	0	1.27 k	1.27 k
	Z-EXT-VPN-AZURE	Z-EXT-VPN-AZURE	14.1.112.177	14.1.112.177	189.9.36.168	189.9.36.168	0	1.15 k	1.15 k
	Z-EXT-VPN-AZURE	Z-EXT-VPN-AZURE	148.153.135.178	148.153.135.178	189.9.36.168	189.9.36.168	510	510	1.02 k
	Z-EXT-VPN-AZURE	Z-EXT-VPN-AZURE	155.146.96.69	155.146.96.69	189.9.36.168	189.9.36.168	510	510	1.02 k
	Z-EXT-VPN-AZURE	Z-EXT-VPN-AZURE	62.210.13.20	62.210.13.20	189.9.36.168	189.9.36.168	0	992	992
	Z-EXT-VPN-AZURE	Z-EXT-VPN-AZURE	195.154.200.146	195.154.200.146	189.9.36.168	189.9.36.168	0	902	902
	Z-EXT-VPN-AZURE	Z-EXT-VPN-AZURE	194.233.90.223	194.233.90.223	189.9.36.168	189.9.36.168	0	864	864
	Z-EXT-VPN-AZURE	Z-EXT-VPN-AZURE	103.74.107.141	103.74.107.141	189.9.36.168	189.9.36.168	0	753	753
	Z-EXT-VPN-AZURE	Z-EXT-VPN-AZURE	209.141.33.68	209.141.33.68	189.9.36.168	189.9.36.168	0	714	714
	Z-EXT-VPN-AZURE	Z-EXT-VPN-AZURE	185.151.107.101	185.151.107.101	189.9.36.168	189.9.36.168	0	640	640
	Z-EXT-VPN-AZURE	Z-EXT-VPN-AZURE	52.175.130.141	52.175.130.141	189.9.36.168	189.9.36.168	0	640	640
	Z-EXT-VPN-AZURE	Z-EXT-VPN-AZURE	51.89.124.57	51.89.124.57	189.9.36.168	189.9.36.168	0	483	483
	Z-EXT-VPN-AZURE	Z-EXT-VPN-AZURE	66.185.26.135	66.185.26.135	189.9.36.168	189.9.36.168	0	460	460
	Z-EXT-VPN-AZURE	Z-EXT-VPN-AZURE	45.86.146.105	45.86.146.105	189.9.36.168	189.9.36.168	0	459	459
	Z-EXT-VPN-AZURE	Z-EXT-VPN-AZURE	92.204.248.74	92.204.248.74	189.9.36.168	189.9.36.168	0	459	459
	Z-EXT-VPN-AZURE	Z-EXT-VPN-AZURE	185.31.158.83	185.31.158.83	189.9.36.168	189.9.36.168	0	459	459
Mon, May 2, 2022	Z-INT_INTERNA	Z-EXT-VPN-AZURE	10.102.9.180	10.102.9.180	172.16.168.6	172.16.168.6	250.04 M	4.49 M	254.54 M
	Z-INT_INTERNA	Z-EXT-VPN-AZURE	10.102.11.124	10.102.11.124	172.16.168.6	172.16.168.6	694.62 k	652.64 k	1.34 M
	Z-EXT-VPN-AZURE	Z-EXT-VPN-AZURE	185.151.107.102	185.151.107.102	189.9.36.168	189.9.36.168	0	4.60 k	4.60 k
	Z-EXT-VPN-AZURE	Z-EXT-VPN-AZURE	146.88.240.4	146.88.240.4	189.9.36.168	189.9.36.168	0	4.09 k	4.09 k
	Z-EXT-VPN-AZURE	Z-EXT-VPN-AZURE	185.151.107.101	185.151.107.101	189.9.36.168	189.9.36.168	0	3.45 k	3.45 k
	Z-INT_INTERNA	Z-EXT-VPN-AZURE	10.102.9.105	10.102.9.105	189.9.36.163	189.9.36.163	814	1.73 k	2.55 k
	Z-EXT-VPN-AZURE	Z-EXT-VPN-AZURE	165.227.235.122	165.227.235.122	189.9.36.168	189.9.36.168	0	1.51 k	1.51 k
	Z-EXT-VPN-AZURE	Z-EXT-VPN-AZURE	65.108.46.62	65.108.46.62	189.9.36.168	189.9.36.168	0	1.43 k	1.43 k
	Z-EXT-VPN-AZURE	Z-EXT-VPN-AZURE	65.49.20.93	65.49.20.93	189.9.36.168	189.9.36.168	0	1.40 k	1.40 k
	Z-EXT-VPN-AZURE	Z-EXT-VPN-AZURE	205.205.150.59	205.205.150.59	189.9.36.168	189.9.36.168	0	1.26 k	1.26 k
	Z-EXT-VPN-AZURE	Z-EXT-VPN-AZURE	148.153.135.178	148.153.135.178	189.9.36.168	189.9.36.168	510	510	1.02 k
	Z-EXT-VPN-AZURE	Z-EXT-VPN-AZURE	155.146.96.69	155.146.96.69	189.9.36.168	189.9.36.168	510	510	1.02 k
	Z-EXT-VPN-AZURE	Z-EXT-VPN-AZURE	185.31.158.83	185.31.158.83	189.9.36.168	189.9.36.168	0	918	918
	Z-EXT-VPN-AZURE	Z-EXT-VPN-AZURE	92.204.248.74	92.204.248.74	189.9.36.168	189.9.36.168	0	914	914
	Z-EXT-VPN-AZURE	Z-EXT-VPN-AZURE	92.118.39.130	92.118.39.130	189.9.36.168	189.9.36.168	0	913	913
	Z-EXT-VPN-AZURE	Z-EXT-VPN-AZURE	195.154.200.146	195.154.200.146	189.9.36.168	189.9.36.168	0	903	903
	Z-EXT-VPN-AZURE	Z-EXT-VPN-AZURE	80.94.93.125	80.94.93.125	189.9.36.168	189.9.36.168	0	896	896
	Z-EXT-VPN-AZURE	Z-EXT-VPN-AZURE	194.233.90.223	194.233.90.223	189.9.36.168	189.9.36.168	0	864	864
	Z-EXT-VPN-AZURE	Z-EXT-VPN-AZURE	154.31.0.27	154.31.0.27	189.9.36.168	189.9.36.168	0	695	695
	Z-EXT-VPN-AZURE	Z-EXT-VPN-AZURE	103.74.107.141	103.74.107.141	189.9.36.168	189.9.36.168	0	579	579
	Z-EXT-VPN-AZURE	Z-EXT-VPN-AZURE	62.210.13.20	62.210.13.20	189.9.36.168	189.9.36.168	0	529	529
	Z-EXT-VPN-AZURE	Z-EXT-VPN-AZURE	86.21.181.102	86.21.181.102	189.9.36.168	189.9.36.168	0	512	512
	Z-EXT-VPN-AZURE	Z-EXT-VPN-AZURE	45.134.173.25	45.134.173.25	189.9.36.168	189.9.36.168	0	476	476
	Z-EXT-VPN-AZURE	Z-EXT-VPN-AZURE	192.111.155.102	192.111.155.102	189.9.36.168	189.9.36.168	0	470	470
	Z-EXT-VPN-AZURE	Z-EXT-VPN-AZURE	151.106.15.82	151.106.15.82	189.9.36.168	189.9.36.168	0	458	458
Tue, Apr 19, 2022	Z-INT_INTERNA	Z-EXT-VPN-AZURE	10.102.9.180	10.102.9.180	172.16.168.6	172.16.168.6	11.33 M	69.62 M	80.96 M
	Z-EXT-VPN-AZURE	Z-EXT-VPN-AZURE	146.88.240.4	146.88.240.4	189.9.36.168	189.9.36.168	0	3.85 k	3.85 k
	Z-INT_INTERNA	Z-EXT-VPN-AZURE	10.102.9.105	10.102.9.105	189.9.36.163	189.9.36.163	740	1.58 k	2.32 k
	Z-EXT-VPN-AZURE	Z-EXT-VPN-AZURE	91.202.247.178	91.202.247.178	189.9.36.168	189.9.36.168	0	1.57 k	1.57 k

	Z-EXT-VPN-AZURE	Z-EXT-VPN-AZURE	64.62.197.133	64.62.197.133	189.9.36.168	189.9.36.168	0	1.27 k	1.27 k
	Z-EXT-VPN-AZURE	Z-EXT-VPN-AZURE	155.146.96.69	155.146.96.69	189.9.36.168	189.9.36.168	510	510	1.02 k
	Z-EXT-VPN-AZURE	Z-EXT-VPN-AZURE	62.210.13.20	62.210.13.20	189.9.36.168	189.9.36.168	0	994	994
	Z-EXT-VPN-AZURE	Z-EXT-VPN-AZURE	139.64.165.114	139.64.165.114	189.9.36.168	189.9.36.168	0	922	922
	Z-EXT-VPN-AZURE	Z-EXT-VPN-AZURE	92.204.248.74	92.204.248.74	189.9.36.168	189.9.36.168	0	915	915
	Z-EXT-VPN-AZURE	Z-EXT-VPN-AZURE	104.223.55.62	104.223.55.62	189.9.36.168	189.9.36.168	0	915	915
	Z-EXT-VPN-AZURE	Z-EXT-VPN-AZURE	195.154.200.146	195.154.200.146	189.9.36.168	189.9.36.168	0	902	902
	Z-EXT-VPN-AZURE	Z-EXT-VPN-AZURE	71.6.135.131	71.6.135.131	189.9.36.168	189.9.36.168	0	878	878
	Z-EXT-VPN-AZURE	Z-EXT-VPN-AZURE	148.153.135.178	148.153.135.178	189.9.36.168	189.9.36.168	408	408	816
	Z-EXT-VPN-AZURE	Z-EXT-VPN-AZURE	172.105.208.25	172.105.208.25	189.9.36.168	189.9.36.168	0	674	674
	Z-EXT-VPN-AZURE	Z-EXT-VPN-AZURE	103.74.107.141	103.74.107.141	189.9.36.168	189.9.36.168	0	561	561
	Z-EXT-VPN-AZURE	Z-EXT-VPN-AZURE	82.209.132.132	82.209.132.132	189.9.36.168	189.9.36.168	0	558	558
	Z-EXT-VPN-AZURE	Z-EXT-VPN-AZURE	195.154.172.105	195.154.172.105	189.9.36.168	189.9.36.168	0	519	519
	Z-EXT-VPN-AZURE	Z-EXT-VPN-AZURE	195.154.167.81	195.154.167.81	189.9.36.168	189.9.36.168	0	517	517
	Z-EXT-VPN-AZURE	Z-EXT-VPN-AZURE	62.210.201.179	62.210.201.179	189.9.36.168	189.9.36.168	0	516	516
	Z-EXT-VPN-AZURE	Z-EXT-VPN-AZURE	20.229.24.176	20.229.24.176	189.9.36.168	189.9.36.168	0	516	516
	Z-EXT-VPN-AZURE	Z-EXT-VPN-AZURE	51.89.124.57	51.89.124.57	189.9.36.168	189.9.36.168	0	483	483
	Z-EXT-VPN-AZURE	Z-EXT-VPN-AZURE	144.172.118.37	144.172.118.37	189.9.36.168	189.9.36.168	0	481	481
	Z-EXT-VPN-AZURE	Z-EXT-VPN-AZURE	209.141.33.68	209.141.33.68	189.9.36.168	189.9.36.168	0	476	476
	Z-EXT-VPN-AZURE	Z-EXT-VPN-AZURE	149.255.35.13	149.255.35.13	189.9.36.168	189.9.36.168	0	461	461
	Z-EXT-VPN-AZURE	Z-EXT-VPN-AZURE	134.119.184.118	134.119.184.118	189.9.36.168	189.9.36.168	0	460	460
Wed, May 4, 2022	Z-INT_INTERNA	Z-EXT-VPN-AZURE	10.102.9.180	10.102.9.180	172.16.168.6	172.16.168.6	38.24 M	9.86 M	48.10 M
	Z-INT_INTERNA	Z-EXT-VPN-AZURE	10.102.9.105	10.102.9.105	172.16.168.6	172.16.168.6	5.75 M	1.80 M	7.56 M
	Z-INT_INFOVIA-BLOCO_A	Z-EXT-VPN-AZURE	10.223.10.119	10.223.10.119	172.16.170.254	172.16.170.254	1.63 M	2.82 M	4.45 M
	Z-INT_INTERNA	Z-EXT-VPN-AZURE	10.102.11.124	10.102.11.124	172.16.168.6	172.16.168.6	694.25 k	652.92 k	1.34 M
	Z-INT_INTERNA	Z-EXT-VPN-AZURE	10.102.9.105	10.102.9.105	189.9.36.163	189.9.36.163	5.47 k	11.69 k	17.16 k
	Z-EXT-VPN-AZURE	Z-EXT-VPN-AZURE	146.88.240.4	146.88.240.4	189.9.36.168	189.9.36.168	0	4.09 k	4.09 k
	Z-EXT-VPN-AZURE	Z-EXT-VPN-AZURE	185.151.107.102	185.151.107.102	189.9.36.168	189.9.36.168	0	3.07 k	3.07 k
	Z-EXT-VPN-AZURE	Z-EXT-VPN-AZURE	205.185.127.13	205.185.127.13	189.9.36.168	189.9.36.168	0	1.48 k	1.48 k
	Z-EXT-VPN-AZURE	Z-EXT-VPN-AZURE	65.49.20.120	65.49.20.120	189.9.36.168	189.9.36.168	0	1.34 k	1.34 k
	Z-EXT-VPN-AZURE	Z-EXT-VPN-AZURE	185.151.107.101	185.151.107.101	189.9.36.168	189.9.36.168	0	1.28 k	1.28 k
	Z-EXT-VPN-AZURE	Z-EXT-VPN-AZURE	148.153.135.178	148.153.135.178	189.9.36.168	189.9.36.168	510	510	1.02 k
	Z-EXT-VPN-AZURE	Z-EXT-VPN-AZURE	155.146.96.69	155.146.96.69	189.9.36.168	189.9.36.168	510	510	1.02 k
	Z-EXT-VPN-AZURE	Z-EXT-VPN-AZURE	62.210.13.20	62.210.13.20	189.9.36.168	189.9.36.168	0	967	967
	Z-EXT-VPN-AZURE	Z-EXT-VPN-AZURE	209.141.32.204	209.141.32.204	189.9.36.168	189.9.36.168	0	952	952
	Z-EXT-VPN-AZURE	Z-EXT-VPN-AZURE	92.204.248.74	92.204.248.74	189.9.36.168	189.9.36.168	0	917	917
	Z-EXT-VPN-AZURE	Z-EXT-VPN-AZURE	89.248.169.6	89.248.169.6	189.9.36.168	189.9.36.168	0	913	913
	Z-EXT-VPN-AZURE	Z-EXT-VPN-AZURE	195.154.200.146	195.154.200.146	189.9.36.168	189.9.36.168	0	903	903
	Z-EXT-VPN-AZURE	Z-EXT-VPN-AZURE	80.94.93.125	80.94.93.125	189.9.36.168	189.9.36.168	0	899	899
	Z-EXT-VPN-AZURE	Z-EXT-VPN-AZURE	71.6.135.131	71.6.135.131	189.9.36.168	189.9.36.168	0	878	878
	Z-EXT-VPN-AZURE	Z-EXT-VPN-AZURE	51.77.12.250	51.77.12.250	189.9.36.168	189.9.36.168	0	656	656
	Z-EXT-VPN-AZURE	Z-EXT-VPN-AZURE	103.74.107.141	103.74.107.141	189.9.36.168	189.9.36.168	0	643	643
	Z-EXT-VPN-AZURE	Z-EXT-VPN-AZURE	147.203.255.20	147.203.255.20	189.9.36.168	189.9.36.168	0	613	613
	Z-EXT-VPN-AZURE	Z-EXT-VPN-AZURE	31.14.41.35	31.14.41.35	189.9.36.168	189.9.36.168	0	476	476
	Z-EXT-VPN-AZURE	Z-EXT-VPN-AZURE	177.67.80.188	177.67.80.188	189.9.36.168	189.9.36.168	234	234	468
	Z-EXT-VPN-AZURE	Z-EXT-VPN-AZURE	185.31.158.83	185.31.158.83	189.9.36.168	189.9.36.168	0	458	458
Thu, May 5, 2022	Z-INT_INTERNA	Z-EXT-VPN-AZURE	10.102.9.180	10.102.9.180	172.16.168.6	172.16.168.6	25.22 M	2.92 M	28.14 M
	Z-INT_INTERNA	Z-EXT-VPN-AZURE	10.102.9.105	10.102.9.105	172.16.168.6	172.16.168.6	11.30 M	4.48 M	15.79 M
	Z-INT_INFOVIA-BLOCO_A	Z-EXT-VPN-AZURE	10.223.10.119	10.223.10.119	172.16.170.254	172.16.170.254	2.16 M	2.50 M	4.66 M
	Z-INT_INTERNA	Z-EXT-VPN-AZURE	10.102.11.124	10.102.11.124	172.16.168.6	172.16.168.6	694.12 k	652.57 k	1.34 M
	Z-EXT-VPN-AZURE	Z-EXT-VPN-AZURE	185.151.107.102	185.151.107.102	189.9.36.168	189.9.36.168	0	4.92 k	4.92 k
	Z-EXT-VPN-AZURE	Z-EXT-VPN-AZURE	146.88.240.4	146.88.240.4	189.9.36.168	189.9.36.168	0	3.92 k	3.92 k
	Z-EXT-VPN-AZURE	Z-EXT-VPN-AZURE	185.151.107.101	185.151.107.101	189.9.36.168	189.9.36.168	0	2.81 k	2.81 k
	Z-EXT-VPN-AZURE	Z-EXT-VPN-AZURE	2.57.121.234	2.57.121.234	189.9.36.168	189.9.36.168	0	1.37 k	1.37 k
	Z-EXT-VPN-AZURE	Z-EXT-VPN-AZURE	64.62.197.182	64.62.197.182	189.9.36.168	189.9.36.168	0	1.27 k	1.27 k
	Z-EXT-VPN-AZURE	Z-EXT-VPN-AZURE	14.1.112.177	14.1.112.177	189.9.36.168	189.9.36.168	0	1.15 k	1.15 k
	Z-EXT-VPN-AZURE	Z-EXT-VPN-AZURE	155.146.96.69	155.146.96.69	189.9.36.168	189.9.36.168	510	510	1.02 k
	Z-EXT-VPN-AZURE	Z-EXT-VPN-AZURE	148.153.135.178	148.153.135.178	189.9.36.168	189.9.36.168	510	510	1.02 k
	Z-EXT-VPN-AZURE	Z-EXT-VPN-AZURE	205.185.127.13	205.185.127.13	189.9.36.168	189.9.36.168	0	990	990
	Z-EXT-VPN-AZURE	Z-EXT-VPN-AZURE	89.187.179.113	89.187.179.113	189.9.36.168	189.9.36.168	0	923	923
	Z-EXT-VPN-AZURE	Z-EXT-VPN-AZURE	92.204.248.74	92.204.248.74	189.9.36.168	189.9.36.168	0	916	916
	Z-EXT-VPN-AZURE	Z-EXT-VPN-AZURE	104.223.54.254	104.223.54.254	189.9.36.168	189.9.36.168	0	914	914

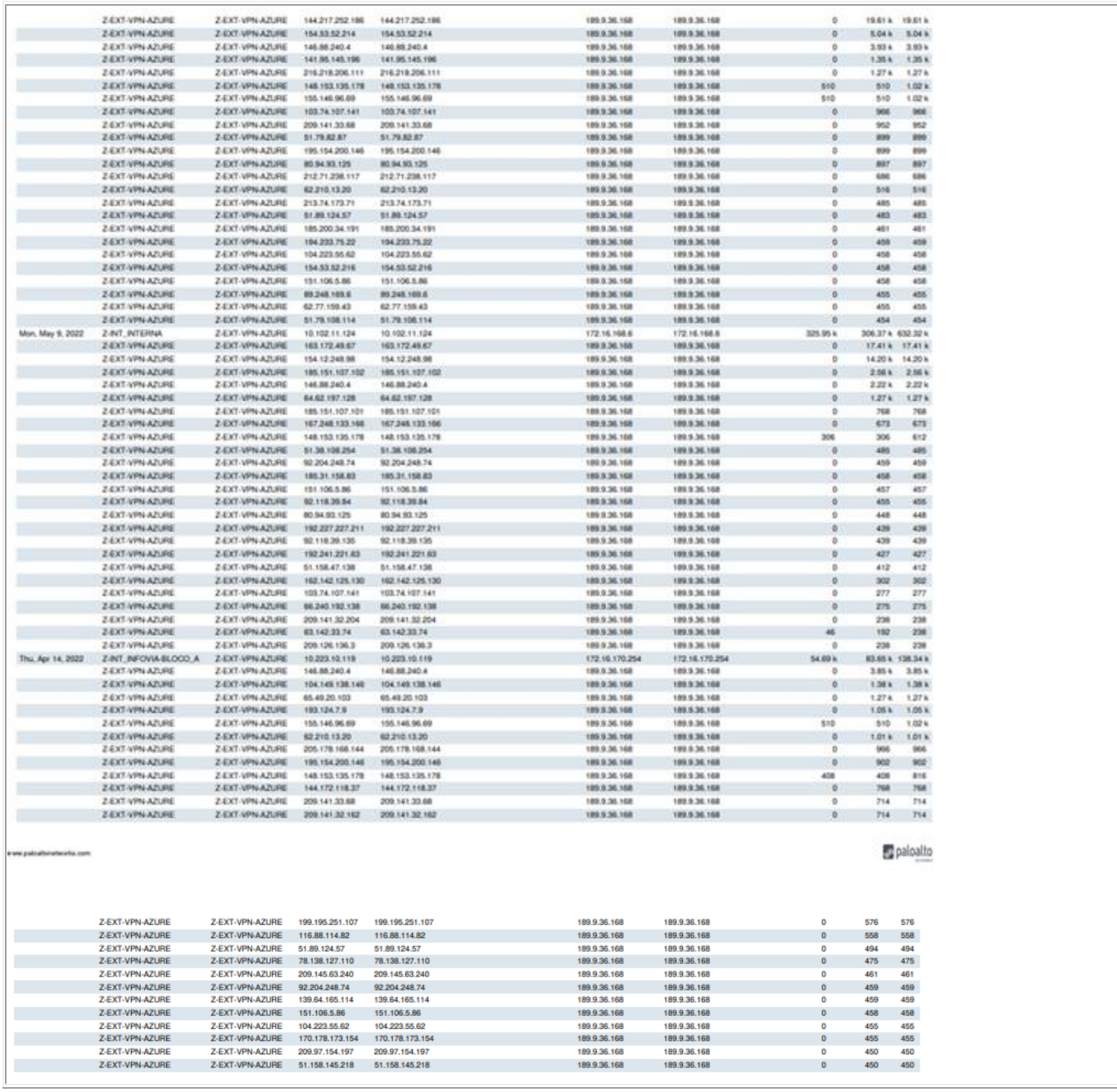
	Z-EXT-VPN-AZURE	Z-EXT-VPN-AZURE	92.118.39.130	92.118.39.130	189.9.36.168	189.9.36.168	0	914	914
	Z-EXT-VPN-AZURE	Z-EXT-VPN-AZURE	185.31.158.83	185.31.158.83	189.9.36.168	189.9.36.168	0	914	914
	Z-EXT-VPN-AZURE	Z-EXT-VPN-AZURE	104.244.76.185	104.244.76.185	189.9.36.168	189.9.36.168	0	726	726
	Z-EXT-VPN-AZURE	Z-EXT-VPN-AZURE	51.77.12.250	51.77.12.250	189.9.36.168	189.9.36.168	0	656	656
	Z-EXT-VPN-AZURE	Z-EXT-VPN-AZURE	103.74.107.141	103.74.107.141	189.9.36.168	189.9.36.168	0	579	579
	Z-EXT-VPN-AZURE	Z-EXT-VPN-AZURE	62.210.13.20	62.210.13.20	189.9.36.168	189.9.36.168	0	518	518
	Z-EXT-VPN-AZURE	Z-EXT-VPN-AZURE	51.75.241.220	51.75.241.220	189.9.36.168	189.9.36.168	0	507	507
	Z-EXT-VPN-AZURE	Z-EXT-VPN-AZURE	195.154.200.146	195.154.200.146	189.9.36.168	189.9.36.168	0	463	463
	Z-EXT-VPN-AZURE	Z-EXT-VPN-AZURE	212.129.23.120	212.129.23.120	189.9.36.168	189.9.36.168	0	462	462
Sat, May 7, 2022	Z-INT_INTERNA	Z-EXT-VPN-AZURE	10.102.9.180	10.102.9.180	172.16.168.6	172.16.168.6	33.66 M	2.48 M	36.15 M
	Z-INT_INTERNA	Z-EXT-VPN-AZURE	10.102.9.105	10.102.9.105	172.16.168.6	172.16.168.6	8.37 M	2.99 M	11.37 M
	Z-INT_INTERNA	Z-EXT-VPN-AZURE	10.102.11.124	10.102.11.124	172.16.168.6	172.16.168.6	694.68 k	652.32 k	1.34 M
	Z-EXT-VPN-AZURE	Z-EXT-VPN-AZURE	185.151.107.102	185.151.107.102	189.9.36.168	189.9.36.168	0	5.69 k	5.69 k
	Z-EXT-VPN-AZURE	Z-EXT-VPN-AZURE	146.88.240.4	146.88.240.4	189.9.36.168	189.9.36.168	0	4.01 k	4.01 k
	Z-EXT-VPN-AZURE	Z-EXT-VPN-AZURE	216.218.206.108	216.218.206.108	189.9.36.168	189.9.36.168	0	1.27 k	1.27 k
	Z-EXT-VPN-AZURE	Z-EXT-VPN-AZURE	185.151.107.101	185.151.107.101	189.9.36.168	189.9.36.168	0	1.15 k	1.15 k
	Z-EXT-VPN-AZURE	Z-EXT-VPN-AZURE	148.153.135.178	148.153.135.178	189.9.36.168	189.9.36.168	510	510	1.02 k
	Z-EXT-VPN-AZURE	Z-EXT-VPN-AZURE	80.94.93.125	80.94.93.125	189.9.36.168	189.9.36.168	0	895	895
	Z-EXT-VPN-AZURE	Z-EXT-VPN-AZURE	209.141.32.204	209.141.32.204	189.9.36.168	189.9.36.168	0	714	714
	Z-EXT-VPN-AZURE	Z-EXT-VPN-AZURE	103.74.107.141	103.74.107.141	189.9.36.168	189.9.36.168	0	643	643
	Z-EXT-VPN-AZURE	Z-EXT-VPN-AZURE	62.210.13.20	62.210.13.20	189.9.36.168	189.9.36.168	0	507	507
	Z-EXT-VPN-AZURE	Z-EXT-VPN-AZURE	51.38.108.254	51.38.108.254	189.9.36.168	189.9.36.168	0	485	485
	Z-EXT-VPN-AZURE	Z-EXT-VPN-AZURE	163.172.49.67	163.172.49.67	189.9.36.168	189.9.36.168	0	460	460
	Z-EXT-VPN-AZURE	Z-EXT-VPN-AZURE	92.118.39.130	92.118.39.130	189.9.36.168	189.9.36.168	0	459	459
	Z-EXT-VPN-AZURE	Z-EXT-VPN-AZURE	85.95.241.192	85.95.241.192	189.9.36.168	189.9.36.168	0	458	458
	Z-EXT-VPN-AZURE	Z-EXT-VPN-AZURE	104.223.54.254	104.223.54.254	189.9.36.168	189.9.36.168	0	458	458
	Z-EXT-VPN-AZURE	Z-EXT-VPN-AZURE	185.31.158.83	185.31.158.83	189.9.36.168	189.9.36.168	0	457	457
	Z-EXT-VPN-AZURE	Z-EXT-VPN-AZURE	92.204.248.74	92.204.248.74	189.9.36.168	189.9.36.168	0	457	457
	Z-EXT-VPN-AZURE	Z-EXT-VPN-AZURE	51.159.30.137	51.159.30.137	189.9.36.168	189.9.36.168	0	456	456
	Z-EXT-VPN-AZURE	Z-EXT-VPN-AZURE	92.118.39.84	92.118.39.84	189.9.36.168	189.9.36.168	0	455	455
	Z-EXT-VPN-AZURE	Z-EXT-VPN-AZURE	192.241.252.87	192.241.252.87	189.9.36.168	189.9.36.168	0	450	450
	Z-EXT-VPN-AZURE	Z-EXT-VPN-AZURE	51.159.16.82	51.159.16.82	189.9.36.168	189.9.36.168	0	450	450
	Z-EXT-VPN-AZURE	Z-EXT-VPN-AZURE	154.53.51.8	154.53.51.8	189.9.36.168	189.9.36.168	0	444	444
	Z-EXT-VPN-AZURE	Z-EXT-VPN-AZURE	212.83.135.137	212.83.135.137	189.9.36.168	189.9.36.168	0	440	440
Tue, Apr 12, 2022	Z-INT_INTERNA	Z-EXT-VPN-AZURE	10.102.9.180	10.102.9.180	172.16.168.6	172.16.168.6	43.04 M	2.13 M	45.19 M
	Z-INT_INTERNA	Z-EXT-VPN-AZURE	10.102.9.180	10.102.9.180	172.16.170.254	172.16.170.254	647.14 k	1.42 M	2.06 M
	Z-INT_INTERNA	Z-EXT-VPN-AZURE	10.102.9.105	10.102.9.105	172.16.170.254	172.16.170.254	191.14 k	195.41 k	386.56 k
	Z-INT_INFOVIA-BLOCO_A	Z-EXT-VPN-AZURE	10.223.10.119	10.223.10.119	172.16.170.254	172.16.170.254	49.24 k	89.40 k	138.64 k
	Z-INT_INTERNA	Z-EXT-VPN-AZURE	10.102.9.105	10.102.9.105	189.9.36.163	189.9.36.163	1.85 k	4.25 k	6.10 k
	Z-EXT-VPN-AZURE	Z-EXT-VPN-AZURE	193.46.255.6	193.46.255.6	189.9.36.168	189.9.36.168	0	5.71 k	5.71 k
	Z-EXT-VPN-AZURE	Z-EXT-VPN-AZURE	146.88.240.4	146.88.240.4	189.9.36.168	189.9.36.168	0	3.85 k	3.85 k
	Z-EXT-VPN-AZURE	Z-EXT-VPN-AZURE	104.149.138.146	104.149.138.146	189.9.36.168	189.9.36.168	0	1.38 k	1.38 k
	Z-EXT-VPN-AZURE	Z-EXT-VPN-AZURE	184.105.139.91	184.105.139.91	189.9.36.168	189.9.36.168	0	1.27 k	1.27 k
	Z-EXT-VPN-AZURE	Z-EXT-VPN-AZURE	148.153.135.178	148.153.135.178	189.9.36.168	189.9.36.168	510	510	1.02 k
	Z-EXT-VPN-AZURE	Z-EXT-VPN-AZURE	155.146.96.69	155.146.96.69	189.9.36.168	189.9.36.168	510	510	1.02 k
	Z-EXT-VPN-AZURE	Z-EXT-VPN-AZURE	209.141.33.68	209.141.33.68	189.9.36.168	189.9.36.168	0	952	952
	Z-EXT-VPN-AZURE	Z-EXT-VPN-AZURE	209.141.32.162	209.141.32.162	189.9.36.168	189.9.36.168	0	952	952
	Z-EXT-VPN-AZURE	Z-EXT-VPN-AZURE	139.64.165.114	139.64.165.114	189.9.36.168	189.9.36.168	0	921	921
	Z-EXT-VPN-AZURE	Z-EXT-VPN-AZURE	193.46.255.169	193.46.255.169	189.9.36.168	189.9.36.168	0	919	919
	Z-EXT-VPN-AZURE	Z-EXT-VPN-AZURE	92.204.248.74	92.204.248.74	189.9.36.168	189.9.36.168	0	913	913
	Z-EXT-VPN-AZURE	Z-EXT-VPN-AZURE	138.197.101.95	138.197.101.95	189.9.36.168	189.9.36.168	470	442	912
	Z-EXT-VPN-AZURE	Z-EXT-VPN-AZURE	89.248.169.6	89.248.169.6	189.9.36.168	189.9.36.168	0	911	911
	Z-EXT-VPN-AZURE	Z-EXT-VPN-AZURE	80.94.93.125	80.94.93.125	189.9.36.168	189.9.36.168	0	899	899
	Z-EXT-VPN-AZURE	Z-EXT-VPN-AZURE	154.53.51.8	154.53.51.8	189.9.36.168	189.9.36.168	0	882	882
	Z-EXT-VPN-AZURE	Z-EXT-VPN-AZURE	139.177.185.114	139.177.185.114	189.9.36.168	189.9.36.168	0	674	674
	Z-EXT-VPN-AZURE	Z-EXT-VPN-AZURE	8.34.174.225	8.34.174.225	189.9.36.168	189.9.36.168	0	541	541
	Z-EXT-VPN-AZURE	Z-EXT-VPN-AZURE	20.229.24.176	20.229.24.176	189.9.36.168	189.9.36.168	0	516	516
	Z-EXT-VPN-AZURE	Z-EXT-VPN-AZURE	51.89.124.57	51.89.124.57	189.9.36.168	189.9.36.168	0	494	494
	Z-EXT-VPN-AZURE	Z-EXT-VPN-AZURE	62.210.13.20	62.210.13.20	189.9.36.168	189.9.36.168	0	494	494
Thu, Apr 28, 2022	Z-INT_INTERNA	Z-EXT-VPN-AZURE	10.102.9.180	10.102.9.180	172.16.168.6	172.16.168.6	37.34 M	2.92 M	40.27 M
	Z-INT_INFOVIA-BLOCO_A	Z-EXT-VPN-AZURE	10.223.10.119	10.223.10.119	172.16.170.254	172.16.170.254	1.37 M	2.08 M	3.45 M
	Z-INT_INTERNA	Z-EXT-VPN-AZURE	10.102.11.124	10.102.11.124	172.16.168.6	172.16.168.6	437.87 k	411.38 k	849.26 k

	Z-INT_INTERNA	Z-EXT-VPN-AZURE	10.102.9.105	10.102.9.105	189.9.36.163	189.9.36.163	1.40 k	3 k	4.40 k
	Z-EXT-VPN-AZURE	Z-EXT-VPN-AZURE	146.88.240.4	146.88.240.4	189.9.36.168	189.9.36.168	0	3.85 k	3.85 k
	Z-EXT-VPN-AZURE	Z-EXT-VPN-AZURE	139.162.209.65	139.162.209.65	189.9.36.168	189.9.36.168	0	1.51 k	1.51 k
	Z-EXT-VPN-AZURE	Z-EXT-VPN-AZURE	194.233.90.223	194.233.90.223	189.9.36.168	189.9.36.168	0	1.38 k	1.38 k
	Z-EXT-VPN-AZURE	Z-EXT-VPN-AZURE	92.118.39.95	92.118.39.95	189.9.36.168	189.9.36.168	0	1.35 k	1.35 k
	Z-EXT-VPN-AZURE	Z-EXT-VPN-AZURE	64.62.197.141	64.62.197.141	189.9.36.168	189.9.36.168	0	1.27 k	1.27 k
	Z-EXT-VPN-AZURE	Z-EXT-VPN-AZURE	148.153.135.178	148.153.135.178	189.9.36.168	189.9.36.168	510	510	1.02 k
	Z-EXT-VPN-AZURE	Z-EXT-VPN-AZURE	209.141.33.68	209.141.33.68	189.9.36.168	189.9.36.168	0	952	952
	Z-EXT-VPN-AZURE	Z-EXT-VPN-AZURE	195.154.200.146	195.154.200.146	189.9.36.168	189.9.36.168	0	901	901
	Z-EXT-VPN-AZURE	Z-EXT-VPN-AZURE	51.79.82.87	51.79.82.87	189.9.36.168	189.9.36.168	0	897	897
	Z-EXT-VPN-AZURE	Z-EXT-VPN-AZURE	66.94.109.198	66.94.109.198	189.9.36.168	189.9.36.168	0	873	873
	Z-EXT-VPN-AZURE	Z-EXT-VPN-AZURE	103.74.107.141	103.74.107.141	189.9.36.168	189.9.36.168	0	838	838
	Z-EXT-VPN-AZURE	Z-EXT-VPN-AZURE	155.146.96.69	155.146.96.69	189.9.36.168	189.9.36.168	408	408	816
	Z-EXT-VPN-AZURE	Z-EXT-VPN-AZURE	187.138.78.72	187.138.78.72	189.9.36.168	189.9.36.168	0	558	558
	Z-EXT-VPN-AZURE	Z-EXT-VPN-AZURE	62.210.13.20	62.210.13.20	189.9.36.168	189.9.36.168	0	505	505
	Z-EXT-VPN-AZURE	Z-EXT-VPN-AZURE	163.172.108.90	163.172.108.90	189.9.36.168	189.9.36.168	0	465	465
	Z-EXT-VPN-AZURE	Z-EXT-VPN-AZURE	198.211.116.238	198.211.116.238	189.9.36.168	189.9.36.168	0	461	461
	Z-EXT-VPN-AZURE	Z-EXT-VPN-AZURE	151.106.15.82	151.106.15.82	189.9.36.168	189.9.36.168	0	460	460
	Z-EXT-VPN-AZURE	Z-EXT-VPN-AZURE	194.31.98.142	194.31.98.142	189.9.36.168	189.9.36.168	0	458	458
	Z-EXT-VPN-AZURE	Z-EXT-VPN-AZURE	92.118.39.84	92.118.39.84	189.9.36.168	189.9.36.168	0	457	457
	Z-EXT-VPN-AZURE	Z-EXT-VPN-AZURE	108.21.252.202	108.21.252.202	189.9.36.168	189.9.36.168	0	457	457
	Z-EXT-VPN-AZURE	Z-EXT-VPN-AZURE	92.204.248.74	92.204.248.74	189.9.36.168	189.9.36.168	0	456	456
Mon, Apr 18, 2022	Z-INT_INTERNA	Z-EXT-VPN-AZURE	10.102.9.180	10.102.9.180	172.16.168.6	172.16.168.6	14.73 M	4.42 M	19.16 M
	Z-EXT-VPN-AZURE	Z-EXT-VPN-AZURE	146.88.240.4	146.88.240.4	189.9.36.168	189.9.36.168	0	3.85 k	3.85 k
	Z-EXT-VPN-AZURE	Z-EXT-VPN-AZURE	45.58.140.218	45.58.140.218	189.9.36.168	189.9.36.168	0	1.37 k	1.37 k
	Z-EXT-VPN-AZURE	Z-EXT-VPN-AZURE	216.218.206.87	216.218.206.87	189.9.36.168	189.9.36.168	0	1.27 k	1.27 k
	Z-EXT-VPN-AZURE	Z-EXT-VPN-AZURE	20.229.24.176	20.229.24.176	189.9.36.168	189.9.36.168	0	1.03 k	1.03 k
	Z-EXT-VPN-AZURE	Z-EXT-VPN-AZURE	148.153.135.178	148.153.135.178	189.9.36.168	189.9.36.168	510	510	1.02 k
	Z-EXT-VPN-AZURE	Z-EXT-VPN-AZURE	209.141.33.68	209.141.33.68	189.9.36.168	189.9.36.168	0	952	952
	Z-EXT-VPN-AZURE	Z-EXT-VPN-AZURE	89.248.169.6	89.248.169.6	189.9.36.168	189.9.36.168	0	913	913
	Z-EXT-VPN-AZURE	Z-EXT-VPN-AZURE	51.79.82.87	51.79.82.87	189.9.36.168	189.9.36.168	0	898	898
	Z-EXT-VPN-AZURE	Z-EXT-VPN-AZURE	71.6.146.186	71.6.146.186	189.9.36.168	189.9.36.168	0	870	870
	Z-EXT-VPN-AZURE	Z-EXT-VPN-AZURE	155.146.96.69	155.146.96.69	189.9.36.168	189.9.36.168	408	408	816
	Z-EXT-VPN-AZURE	Z-EXT-VPN-AZURE	202.150.191.14	202.150.191.14	189.9.36.168	189.9.36.168	0	768	768
	Z-EXT-VPN-AZURE	Z-EXT-VPN-AZURE	62.210.13.20	62.210.13.20	189.9.36.168	189.9.36.168	0	520	520
	Z-EXT-VPN-AZURE	Z-EXT-VPN-AZURE	51.89.124.57	51.89.124.57	189.9.36.168	189.9.36.168	0	483	483
	Z-INT_INTERNA	Z-EXT-VPN-AZURE	10.102.9.105	10.102.9.105	189.9.36.163	189.9.36.163	148	316	464
	Z-EXT-VPN-AZURE	Z-EXT-VPN-AZURE	92.118.39.12	92.118.39.12	189.9.36.168	189.9.36.168	0	456	456
	Z-EXT-VPN-AZURE	Z-EXT-VPN-AZURE	51.79.108.114	51.79.108.114	189.9.36.168	189.9.36.168	0	454	454
	Z-EXT-VPN-AZURE	Z-EXT-VPN-AZURE	195.154.200.146	195.154.200.146	189.9.36.168	189.9.36.168	0	452	452
	Z-EXT-VPN-AZURE	Z-EXT-VPN-AZURE	51.158.145.218	51.158.145.218	189.9.36.168	189.9.36.168	0	452	452
	Z-EXT-VPN-AZURE	Z-EXT-VPN-AZURE	209.97.154.197	209.97.154.197	189.9.36.168	189.9.36.168	0	451	451
	Z-EXT-VPN-AZURE	Z-EXT-VPN-AZURE	193.46.255.47	193.46.255.47	189.9.36.168	189.9.36.168	0	440	440
	Z-EXT-VPN-AZURE	Z-EXT-VPN-AZURE	192.241.217.121	192.241.217.121	189.9.36.168	189.9.36.168	0	431	431
	Z-EXT-VPN-AZURE	Z-EXT-VPN-AZURE	51.158.47.138	51.158.47.138	189.9.36.168	189.9.36.168	0	412	412
	Z-EXT-VPN-AZURE	Z-EXT-VPN-AZURE	104.206.128.6	104.206.128.6	189.9.36.168	189.9.36.168	0	412	412
	Z-EXT-VPN-AZURE	Z-EXT-VPN-AZURE	192.241.218.47	192.241.218.47	189.9.36.168	189.9.36.168	0	406	406
Tue, May 3, 2022	Z-INT_INTERNA	Z-EXT-VPN-AZURE	10.102.9.180	10.102.9.180	172.16.168.6	172.16.168.6	9.43 M	5.42 M	14.85 M
	Z-INT_INTERNA	Z-EXT-VPN-AZURE	10.102.11.124	10.102.11.124	172.16.168.6	172.16.168.6	694.93 k	652.87 k	1.34 M
	Z-EXT-VPN-AZURE	Z-EXT-VPN-AZURE	185.151.107.102	185.151.107.102	189.9.36.168	189.9.36.168	0	6.01 k	6.01 k
	Z-EXT-VPN-AZURE	Z-EXT-VPN-AZURE	146.88.240.4	146.88.240.4	189.9.36.168	189.9.36.168	0	3.92 k	3.92 k
	Z-EXT-VPN-AZURE	Z-EXT-VPN-AZURE	185.151.107.101	185.151.107.101	189.9.36.168	189.9.36.168	0	1.66 k	1.66 k
	Z-EXT-VPN-AZURE	Z-EXT-VPN-AZURE	165.227.235.122	165.227.235.122	189.9.36.168	189.9.36.168	0	1.51 k	1.51 k
	Z-EXT-VPN-AZURE	Z-EXT-VPN-AZURE	65.49.20.106	65.49.20.106	189.9.36.168	189.9.36.168	0	1.27 k	1.27 k
	Z-EXT-VPN-AZURE	Z-EXT-VPN-AZURE	205.205.150.19	205.205.150.19	189.9.36.168	189.9.36.168	0	1.26 k	1.26 k
	Z-EXT-VPN-AZURE	Z-EXT-VPN-AZURE	92.118.39.130	92.118.39.130	189.9.36.168	189.9.36.168	0	918	918
	Z-EXT-VPN-AZURE	Z-EXT-VPN-AZURE	195.154.200.146	195.154.200.146	189.9.36.168	189.9.36.168	0	903	903
	Z-EXT-VPN-AZURE	Z-EXT-VPN-AZURE	80.94.93.125	80.94.93.125	189.9.36.168	189.9.36.168	0	893	893
	Z-EXT-VPN-AZURE	Z-EXT-VPN-AZURE	194.233.90.223	194.233.90.223	189.9.36.168	189.9.36.168	0	875	875
	Z-EXT-VPN-AZURE	Z-EXT-VPN-AZURE	103.74.107.141	103.74.107.141	189.9.36.168	189.9.36.168	0	838	838
	Z-EXT-VPN-AZURE	Z-EXT-VPN-AZURE	148.153.135.178	148.153.135.178	189.9.36.168	189.9.36.168	408	408	816
	Z-EXT-VPN-AZURE	Z-EXT-VPN-AZURE	155.146.96.69	155.146.96.69	189.9.36.168	189.9.36.168	408	408	816

	Z-EXT-VPN-AZURE	Z-EXT-VPN-AZURE	94.102.61.31	94.102.61.31	189.9.36.168	189.9.36.168	0	768	768
	Z-EXT-VPN-AZURE	Z-EXT-VPN-AZURE	51.158.24.19	51.158.24.19	189.9.36.168	189.9.36.168	0	696	696
	Z-EXT-VPN-AZURE	Z-EXT-VPN-AZURE	62.210.13.20	62.210.13.20	189.9.36.168	189.9.36.168	0	496	496
	Z-EXT-VPN-AZURE	Z-EXT-VPN-AZURE	194.31.98.142	194.31.98.142	189.9.36.168	189.9.36.168	0	485	485
	Z-EXT-VPN-AZURE	Z-EXT-VPN-AZURE	92.204.248.74	92.204.248.74	189.9.36.168	189.9.36.168	0	458	458
	Z-EXT-VPN-AZURE	Z-EXT-VPN-AZURE	185.185.83.60	185.185.83.60	189.9.36.168	189.9.36.168	0	458	458
	Z-EXT-VPN-AZURE	Z-EXT-VPN-AZURE	92.118.39.84	92.118.39.84	189.9.36.168	189.9.36.168	0	457	457
	Z-EXT-VPN-AZURE	Z-EXT-VPN-AZURE	2.57.121.234	2.57.121.234	189.9.36.168	189.9.36.168	0	456	456
	Z-EXT-VPN-AZURE	Z-EXT-VPN-AZURE	92.118.39.95	92.118.39.95	189.9.36.168	189.9.36.168	0	451	451
	Z-EXT-VPN-AZURE	Z-EXT-VPN-AZURE	20.127.23.249	20.127.23.249	189.9.36.168	189.9.36.168	0	449	449
Mon, Apr 11, 2022	Z-INT_INTERNA	Z-EXT-VPN-AZURE	10.102.9.180	10.102.9.180	172.16.168.6	172.16.168.6	3.60 M	6.31 M	9.91 M
	Z-INT_INFOVIA-BLOCO_A	Z-EXT-VPN-AZURE	10.223.10.119	10.223.10.119	172.16.170.254	172.16.170.254	227.20 k	376.48 k	603.68 k
	Z-INT_INTERNA	Z-EXT-VPN-AZURE	10.102.11.124	10.102.11.124	172.16.168.6	172.16.168.6	11.80 k	11.72 k	23.53 k
	Z-EXT-VPN-AZURE	Z-EXT-VPN-AZURE	146.88.240.4	146.88.240.4	189.9.36.168	189.9.36.168	0	3.85 k	3.85 k
	Z-EXT-VPN-AZURE	Z-EXT-VPN-AZURE	209.182.193.173	209.182.193.173	189.9.36.168	189.9.36.168	0	1.38 k	1.38 k
	Z-EXT-VPN-AZURE	Z-EXT-VPN-AZURE	80.94.93.125	80.94.93.125	189.9.36.168	189.9.36.168	0	1.34 k	1.34 k
	Z-EXT-VPN-AZURE	Z-EXT-VPN-AZURE	64.62.197.204	64.62.197.204	189.9.36.168	189.9.36.168	0	1.27 k	1.27 k
	Z-EXT-VPN-AZURE	Z-EXT-VPN-AZURE	155.146.96.69	155.146.96.69	189.9.36.168	189.9.36.168	510	510	1.02 k
	Z-EXT-VPN-AZURE	Z-EXT-VPN-AZURE	148.153.135.178	148.153.135.178	189.9.36.168	189.9.36.168	510	510	1.02 k
	Z-INT_INTERNA	Z-EXT-VPN-AZURE	10.102.9.105	10.102.9.105	189.9.36.163	189.9.36.163	296	632	926
	Z-EXT-VPN-AZURE	Z-EXT-VPN-AZURE	104.223.55.62	104.223.55.62	189.9.36.168	189.9.36.168	0	914	914
	Z-EXT-VPN-AZURE	Z-EXT-VPN-AZURE	195.154.200.146	195.154.200.146	189.9.36.168	189.9.36.168	0	903	903
	Z-EXT-VPN-AZURE	Z-EXT-VPN-AZURE	14.1.112.177	14.1.112.177	189.9.36.168	189.9.36.168	0	854	854
	Z-EXT-VPN-AZURE	Z-EXT-VPN-AZURE	209.141.32.162	209.141.32.162	189.9.36.168	189.9.36.168	0	714	714
	Z-EXT-VPN-AZURE	Z-EXT-VPN-AZURE	209.141.33.68	209.141.33.68	189.9.36.168	189.9.36.168	0	714	714
	Z-EXT-VPN-AZURE	Z-EXT-VPN-AZURE	143.244.48.158	143.244.48.158	189.9.36.168	189.9.36.168	0	541	541
	Z-EXT-VPN-AZURE	Z-EXT-VPN-AZURE	20.229.24.176	20.229.24.176	189.9.36.168	189.9.36.168	0	516	516
	Z-EXT-VPN-AZURE	Z-EXT-VPN-AZURE	62.210.13.20	62.210.13.20	189.9.36.168	189.9.36.168	0	504	504
	Z-EXT-VPN-AZURE	Z-EXT-VPN-AZURE	51.89.124.57	51.89.124.57	189.9.36.168	189.9.36.168	0	494	494
	Z-EXT-VPN-AZURE	Z-EXT-VPN-AZURE	193.46.255.169	193.46.255.169	189.9.36.168	189.9.36.168	0	460	460
	Z-EXT-VPN-AZURE	Z-EXT-VPN-AZURE	193.46.255.74	193.46.255.74	189.9.36.168	189.9.36.168	0	459	459
	Z-EXT-VPN-AZURE	Z-EXT-VPN-AZURE	92.204.248.74	92.204.248.74	189.9.36.168	189.9.36.168	0	458	458
	Z-EXT-VPN-AZURE	Z-EXT-VPN-AZURE	89.248.169.6	89.248.169.6	189.9.36.168	189.9.36.168	0	457	457
	Z-EXT-VPN-AZURE	Z-EXT-VPN-AZURE	51.158.145.218	51.158.145.218	189.9.36.168	189.9.36.168	0	451	451
	Z-EXT-VPN-AZURE	Z-EXT-VPN-AZURE	146.59.236.28	146.59.236.28	189.9.36.168	189.9.36.168	0	451	451
Sun, May 1, 2022	Z-INT_INFOVIA-BLOCO_A	Z-EXT-VPN-AZURE	10.223.10.119	10.223.10.119	172.16.170.254	172.16.170.254	1.19 M	1.69 M	2.88 M
	Z-INT_INTERNA	Z-EXT-VPN-AZURE	10.102.11.124	10.102.11.124	172.16.168.6	172.16.168.6	694.39 k	652.32 k	1.34 M
	Z-INT_INTERNA	Z-EXT-VPN-AZURE	10.102.9.180	10.102.9.180	172.16.168.6	172.16.168.6	425.24 k	354.95 k	780.19 k
	Z-EXT-VPN-AZURE	Z-EXT-VPN-AZURE	185.180.143.145	185.180.143.145	189.9.36.168	189.9.36.168	0	5.77 k	5.77 k
	Z-EXT-VPN-AZURE	Z-EXT-VPN-AZURE	185.151.107.102	185.151.107.102	189.9.36.168	189.9.36.168	0	5.50 k	5.50 k
	Z-EXT-VPN-AZURE	Z-EXT-VPN-AZURE	146.88.240.4	146.88.240.4	189.9.36.168	189.9.36.168	0	4.01 k	4.01 k
	Z-EXT-VPN-AZURE	Z-EXT-VPN-AZURE	148.153.135.178	148.153.135.178	189.9.36.168	189.9.36.168	1.47 k	1.85 k	3.33 k
	Z-EXT-VPN-AZURE	Z-EXT-VPN-AZURE	185.151.107.101	185.151.107.101	189.9.36.168	189.9.36.168	0	2.17 k	2.17 k
	Z-EXT-VPN-AZURE	Z-EXT-VPN-AZURE	139.59.13.18	139.59.13.18	189.9.36.168	189.9.36.168	0	1.51 k	1.51 k
	Z-EXT-VPN-AZURE	Z-EXT-VPN-AZURE	194.233.90.223	194.233.90.223	189.9.36.168	189.9.36.168	0	1.29 k	1.29 k
	Z-EXT-VPN-AZURE	Z-EXT-VPN-AZURE	74.82.47.55	74.82.47.55	189.9.36.168	189.9.36.168	0	1.27 k	1.27 k
	Z-EXT-VPN-AZURE	Z-EXT-VPN-AZURE	155.146.96.69	155.146.96.69	189.9.36.168	189.9.36.168	510	510	1.02 k
	Z-EXT-VPN-AZURE	Z-EXT-VPN-AZURE	65.108.46.62	65.108.46.62	189.9.36.168	189.9.36.168	0	921	921
	Z-EXT-VPN-AZURE	Z-EXT-VPN-AZURE	92.118.39.130	92.118.39.130	189.9.36.168	189.9.36.168	0	918	918
	Z-EXT-VPN-AZURE	Z-EXT-VPN-AZURE	45.58.140.218	45.58.140.218	189.9.36.168	189.9.36.168	0	915	915
	Z-EXT-VPN-AZURE	Z-EXT-VPN-AZURE	195.154.200.146	195.154.200.146	189.9.36.168	189.9.36.168	0	899	899
	Z-EXT-VPN-AZURE	Z-EXT-VPN-AZURE	80.94.93.125	80.94.93.125	189.9.36.168	189.9.36.168	0	894	894
	Z-EXT-VPN-AZURE	Z-EXT-VPN-AZURE	14.1.112.177	14.1.112.177	189.9.36.168	189.9.36.168	0	854	854
	Z-EXT-VPN-AZURE	Z-EXT-VPN-AZURE	103.74.107.141	103.74.107.141	189.9.36.168	189.9.36.168	0	728	728
	Z-EXT-VPN-AZURE	Z-EXT-VPN-AZURE	51.89.124.57	51.89.124.57	189.9.36.168	189.9.36.168	0	483	483
	Z-EXT-VPN-AZURE	Z-EXT-VPN-AZURE	15.204.2.169	15.204.2.169	189.9.36.168	189.9.36.168	0	476	476
	Z-EXT-VPN-AZURE	Z-EXT-VPN-AZURE	209.141.33.68	209.141.33.68	189.9.36.168	189.9.36.168	0	476	476
	Z-EXT-VPN-AZURE	Z-EXT-VPN-AZURE	92.118.39.84	92.118.39.84	189.9.36.168	189.9.36.168	0	458	458
	Z-EXT-VPN-AZURE	Z-EXT-VPN-AZURE	151.106.15.82	151.106.15.82	189.9.36.168	189.9.36.168	0	458	458
	Z-EXT-VPN-AZURE	Z-EXT-VPN-AZURE	185.31.158.83	185.31.158.83	189.9.36.168	189.9.36.168	0	458	458
Wed, Apr 13, 2022	Z-INT_INTERNA	Z-EXT-VPN-AZURE	10.102.9.180	10.102.9.180	172.16.168.6	172.16.168.6	493.81 k	1.66 M	2.16 M
	Z-INT_INTERNA	Z-EXT-VPN-AZURE	10.102.9.105	10.102.9.105	172.16.170.254	172.16.170.254	158.88 k	164.81 k	323.70 k

	Z-EXT-VPN-AZURE	Z-EXT-VPN-AZURE	146.88.240.4	146.88.240.4	189.9.36.168	189.9.36.168	0	3.85 k	3.85 k
	Z-EXT-VPN-AZURE	Z-EXT-VPN-AZURE	184.105.139.79	184.105.139.79	189.9.36.168	189.9.36.168	0	1.27 k	1.27 k
	Z-EXT-VPN-AZURE	Z-EXT-VPN-AZURE	148.153.135.178	148.153.135.178	189.9.36.168	189.9.36.168	510	510	1.02 k
	Z-EXT-VPN-AZURE	Z-EXT-VPN-AZURE	139.64.165.114	139.64.165.114	189.9.36.168	189.9.36.168	0	921	921
	Z-EXT-VPN-AZURE	Z-EXT-VPN-AZURE	92.204.248.74	92.204.248.74	189.9.36.168	189.9.36.168	0	914	914
	Z-EXT-VPN-AZURE	Z-EXT-VPN-AZURE	195.154.200.146	195.154.200.146	189.9.36.168	189.9.36.168	0	899	899
	Z-EXT-VPN-AZURE	Z-EXT-VPN-AZURE	51.79.82.87	51.79.82.87	189.9.36.168	189.9.36.168	0	897	897
	Z-EXT-VPN-AZURE	Z-EXT-VPN-AZURE	155.146.96.69	155.146.96.69	189.9.36.168	189.9.36.168	408	408	816
	Z-EXT-VPN-AZURE	Z-EXT-VPN-AZURE	209.141.33.68	209.141.33.68	189.9.36.168	189.9.36.168	0	714	714
	Z-INT_INTERNA	Z-EXT-VPN-AZURE	10.102.9.105	10.102.9.105	189.9.36.163	189.9.36.163	222	474	696
	Z-EXT-VPN-AZURE	Z-EXT-VPN-AZURE	147.203.255.20	147.203.255.20	189.9.36.168	189.9.36.168	0	613	613
	Z-EXT-VPN-AZURE	Z-EXT-VPN-AZURE	103.74.107.141	103.74.107.141	189.9.36.168	189.9.36.168	0	515	515
	Z-EXT-VPN-AZURE	Z-EXT-VPN-AZURE	209.141.51.43	209.141.51.43	189.9.36.168	189.9.36.168	0	512	512
	Z-EXT-VPN-AZURE	Z-EXT-VPN-AZURE	62.210.13.20	62.210.13.20	189.9.36.168	189.9.36.168	0	506	506
	Z-EXT-VPN-AZURE	Z-EXT-VPN-AZURE	51.89.124.57	51.89.124.57	189.9.36.168	189.9.36.168	0	494	494
	Z-EXT-VPN-AZURE	Z-EXT-VPN-AZURE	209.141.32.162	209.141.32.162	189.9.36.168	189.9.36.168	0	476	476
	Z-EXT-VPN-AZURE	Z-EXT-VPN-AZURE	139.28.218.34	139.28.218.34	189.9.36.168	189.9.36.168	0	470	470
	Z-EXT-VPN-AZURE	Z-EXT-VPN-AZURE	193.46.255.169	193.46.255.169	189.9.36.168	189.9.36.168	0	461	461
	Z-EXT-VPN-AZURE	Z-EXT-VPN-AZURE	89.248.169.6	89.248.169.6	189.9.36.168	189.9.36.168	0	457	457
	Z-EXT-VPN-AZURE	Z-EXT-VPN-AZURE	51.158.145.218	51.158.145.218	189.9.36.168	189.9.36.168	0	450	450
	Z-EXT-VPN-AZURE	Z-EXT-VPN-AZURE	20.110.123.63	20.110.123.63	189.9.36.168	189.9.36.168	0	449	449
	Z-EXT-VPN-AZURE	Z-EXT-VPN-AZURE	199.195.251.107	199.195.251.107	189.9.36.168	189.9.36.168	0	448	448
	Z-EXT-VPN-AZURE	Z-EXT-VPN-AZURE	80.94.93.125	80.94.93.125	189.9.36.168	189.9.36.168	0	445	445
Sun, Apr 24, 2022	Z-INT_INTERNA	Z-EXT-VPN-AZURE	10.102.11.124	10.102.11.124	172.16.168.6	172.16.168.6	692.63 k	652.39 k	1.34 M
	Z-EXT-VPN-AZURE	Z-EXT-VPN-AZURE	144.217.252.186	144.217.252.186	189.9.36.168	189.9.36.168	0	16.68 k	16.68 k
	Z-EXT-VPN-AZURE	Z-EXT-VPN-AZURE	104.152.52.167	104.152.52.167	189.9.36.168	189.9.36.168	0	6.52 k	6.52 k
	Z-EXT-VPN-AZURE	Z-EXT-VPN-AZURE	163.181.64.132	163.181.64.132	189.9.36.168	189.9.36.168	2.14 k	2.14 k	4.28 k
	Z-EXT-VPN-AZURE	Z-EXT-VPN-AZURE	146.88.240.4	146.88.240.4	189.9.36.168	189.9.36.168	0	3.93 k	3.93 k
	Z-EXT-VPN-AZURE	Z-EXT-VPN-AZURE	148.153.135.178	148.153.135.178	189.9.36.168	189.9.36.168	1.47 k	1.85 k	3.33 k
	Z-EXT-VPN-AZURE	Z-EXT-VPN-AZURE	92.118.39.180	92.118.39.180	189.9.36.168	189.9.36.168	0	1.77 k	1.77 k
	Z-EXT-VPN-AZURE	Z-EXT-VPN-AZURE	184.105.247.214	184.105.247.214	189.9.36.168	189.9.36.168	0	1.27 k	1.27 k
	Z-EXT-VPN-AZURE	Z-EXT-VPN-AZURE	155.146.96.69	155.146.96.69	189.9.36.168	189.9.36.168	510	510	1.02 k
	Z-EXT-VPN-AZURE	Z-EXT-VPN-AZURE	62.210.13.20	62.210.13.20	189.9.36.168	189.9.36.168	0	1 k	1 k
	Z-EXT-VPN-AZURE	Z-EXT-VPN-AZURE	92.204.248.74	92.204.248.74	189.9.36.168	189.9.36.168	0	914	914
	Z-EXT-VPN-AZURE	Z-EXT-VPN-AZURE	161.35.236.116	161.35.236.116	189.9.36.168	189.9.36.168	470	442	912
	Z-EXT-VPN-AZURE	Z-EXT-VPN-AZURE	103.74.107.141	103.74.107.141	189.9.36.168	189.9.36.168	0	902	902
	Z-EXT-VPN-AZURE	Z-EXT-VPN-AZURE	80.94.93.125	80.94.93.125	189.9.36.168	189.9.36.168	0	897	897
	Z-EXT-VPN-AZURE	Z-EXT-VPN-AZURE	92.118.39.12	92.118.39.12	189.9.36.168	189.9.36.168	0	896	896
	Z-EXT-VPN-AZURE	Z-EXT-VPN-AZURE	51.79.82.87	51.79.82.87	189.9.36.168	189.9.36.168	0	895	895
	Z-EXT-VPN-AZURE	Z-EXT-VPN-AZURE	185.182.184.120	185.182.184.120	189.9.36.168	189.9.36.168	0	886	886
	Z-EXT-VPN-AZURE	Z-EXT-VPN-AZURE	209.141.33.68	209.141.33.68	189.9.36.168	189.9.36.168	0	714	714
	Z-EXT-VPN-AZURE	Z-EXT-VPN-AZURE	147.203.255.20	147.203.255.20	189.9.36.168	189.9.36.168	0	613	613
	Z-EXT-VPN-AZURE	Z-EXT-VPN-AZURE	126.92.228.98	126.92.228.98	189.9.36.168	189.9.36.168	0	541	541
	Z-EXT-VPN-AZURE	Z-EXT-VPN-AZURE	20.229.24.176	20.229.24.176	189.9.36.168	189.9.36.168	0	516	516
	Z-EXT-VPN-AZURE	Z-EXT-VPN-AZURE	51.79.108.114	51.79.108.114	189.9.36.168	189.9.36.168	0	458	458
	Z-EXT-VPN-AZURE	Z-EXT-VPN-AZURE	167.160.91.18	167.160.91.18	189.9.36.168	189.9.36.168	0	455	455
	Z-EXT-VPN-AZURE	Z-EXT-VPN-AZURE	62.77.159.43	62.77.159.43	189.9.36.168	189.9.36.168	0	455	455
	Z-EXT-VPN-AZURE	Z-EXT-VPN-AZURE	104.223.56.130	104.223.56.130	189.9.36.168	189.9.36.168	0	453	453
Sun, May 8, 2022	Z-INT_INTERNA	Z-EXT-VPN-AZURE	10.102.11.124	10.102.11.124	172.16.168.6	172.16.168.6	694.56 k	652.32 k	1.34 M
	Z-EXT-VPN-AZURE	Z-EXT-VPN-AZURE	185.151.107.102	185.151.107.102	189.9.36.168	189.9.36.168	0	5.24 k	5.24 k
	Z-EXT-VPN-AZURE	Z-EXT-VPN-AZURE	146.88.240.4	146.88.240.4	189.9.36.168	189.9.36.168	0	3.94 k	3.94 k
	Z-EXT-VPN-AZURE	Z-EXT-VPN-AZURE	148.153.135.178	148.153.135.178	189.9.36.168	189.9.36.168	1.37 k	1.75 k	3.12 k
	Z-EXT-VPN-AZURE	Z-EXT-VPN-AZURE	185.151.107.101	185.151.107.101	189.9.36.168	189.9.36.168	0	2.17 k	2.17 k
	Z-EXT-VPN-AZURE	Z-EXT-VPN-AZURE	184.105.139.68	184.105.139.68	189.9.36.168	189.9.36.168	0	1.27 k	1.27 k
	Z-EXT-VPN-AZURE	Z-EXT-VPN-AZURE	62.210.13.20	62.210.13.20	189.9.36.168	189.9.36.168	0	1 k	1 k
	Z-EXT-VPN-AZURE	Z-EXT-VPN-AZURE	209.141.32.204	209.141.32.204	189.9.36.168	189.9.36.168	0	952	952
	Z-EXT-VPN-AZURE	Z-EXT-VPN-AZURE	80.94.93.125	80.94.93.125	189.9.36.168	189.9.36.168	0	898	898
	Z-EXT-VPN-AZURE	Z-EXT-VPN-AZURE	103.74.107.141	103.74.107.141	189.9.36.168	189.9.36.168	0	753	753
	Z-EXT-VPN-AZURE	Z-EXT-VPN-AZURE	167.94.138.145	167.94.138.145	189.9.36.168	189.9.36.168	0	673	673
	Z-EXT-VPN-AZURE	Z-EXT-VPN-AZURE	147.203.255.20	147.203.255.20	189.9.36.168	189.9.36.168	0	613	613
	Z-EXT-VPN-AZURE	Z-EXT-VPN-AZURE	51.38.108.254	51.38.108.254	189.9.36.168	189.9.36.168	0	485	485
	Z-EXT-VPN-AZURE	Z-EXT-VPN-AZURE	163.172.49.67	163.172.49.67	189.9.36.168	189.9.36.168	0	459	459

	Z-EXT-VPN-AZURE	Z-EXT-VPN-AZURE	104.223.54.254	104.223.54.254	189.9.36.168	189.9.36.168	0	458	458
	Z-EXT-VPN-AZURE	Z-EXT-VPN-AZURE	212.129.23.120	212.129.23.120	189.9.36.168	189.9.36.168	0	457	457
	Z-EXT-VPN-AZURE	Z-EXT-VPN-AZURE	151.106.5.86	151.106.5.86	189.9.36.168	189.9.36.168	0	457	457
	Z-EXT-VPN-AZURE	Z-EXT-VPN-AZURE	185.31.158.83	185.31.158.83	189.9.36.168	189.9.36.168	0	457	457
	Z-EXT-VPN-AZURE	Z-EXT-VPN-AZURE	92.204.248.74	92.204.248.74	189.9.36.168	189.9.36.168	0	457	457
	Z-EXT-VPN-AZURE	Z-EXT-VPN-AZURE	192.227.227.211	192.227.227.211	189.9.36.168	189.9.36.168	0	439	439
	Z-EXT-VPN-AZURE	Z-EXT-VPN-AZURE	45.154.96.251	45.154.96.251	189.9.36.168	189.9.36.168	0	432	432
	Z-EXT-VPN-AZURE	Z-EXT-VPN-AZURE	192.241.212.100	192.241.212.100	189.9.36.168	189.9.36.168	0	431	431
	Z-EXT-VPN-AZURE	Z-EXT-VPN-AZURE	192.241.220.173	192.241.220.173	189.9.36.168	189.9.36.168	0	406	406
	Z-EXT-VPN-AZURE	Z-EXT-VPN-AZURE	45.56.81.119	45.56.81.119	189.9.36.168	189.9.36.168	0	382	382
	Z-EXT-VPN-AZURE	Z-EXT-VPN-AZURE	192.241.222.21	192.241.222.21	189.9.36.168	189.9.36.168	0	382	382
Sat, Apr 23, 2022	Z-INT_INTERNA	Z-EXT-VPN-AZURE	10.102.11.124	10.102.11.124	172.16.168.6	172.16.168.6	692.38 k	652.32 k	1.34 M
	Z-EXT-VPN-AZURE	Z-EXT-VPN-AZURE	154.53.52.214	154.53.52.214	189.9.36.168	189.9.36.168	0	5.04 k	5.04 k
	Z-EXT-VPN-AZURE	Z-EXT-VPN-AZURE	146.88.240.4	146.88.240.4	189.9.36.168	189.9.36.168	0	3.76 k	3.76 k
	Z-EXT-VPN-AZURE	Z-EXT-VPN-AZURE	64.62.197.154	64.62.197.154	189.9.36.168	189.9.36.168	0	1.27 k	1.27 k
	Z-EXT-VPN-AZURE	Z-EXT-VPN-AZURE	209.141.33.68	209.141.33.68	189.9.36.168	189.9.36.168	0	952	952
	Z-EXT-VPN-AZURE	Z-EXT-VPN-AZURE	144.217.252.186	144.217.252.186	189.9.36.168	189.9.36.168	0	951	951
	Z-EXT-VPN-AZURE	Z-EXT-VPN-AZURE	104.223.55.62	104.223.55.62	189.9.36.168	189.9.36.168	0	908	908
	Z-EXT-VPN-AZURE	Z-EXT-VPN-AZURE	92.118.39.12	92.118.39.12	189.9.36.168	189.9.36.168	0	898	898
	Z-EXT-VPN-AZURE	Z-EXT-VPN-AZURE	195.154.200.146	195.154.200.146	189.9.36.168	189.9.36.168	0	896	896
	Z-EXT-VPN-AZURE	Z-EXT-VPN-AZURE	80.94.93.125	80.94.93.125	189.9.36.168	189.9.36.168	0	897	897
	Z-EXT-VPN-AZURE	Z-EXT-VPN-AZURE	51.79.82.87	51.79.82.87	189.9.36.168	189.9.36.168	0	897	897
	Z-EXT-VPN-AZURE	Z-EXT-VPN-AZURE	155.146.96.69	155.146.96.69	189.9.36.168	189.9.36.168	408	408	816
	Z-EXT-VPN-AZURE	Z-EXT-VPN-AZURE	148.153.135.178	148.153.135.178	189.9.36.168	189.9.36.168	408	408	816
	Z-EXT-VPN-AZURE	Z-EXT-VPN-AZURE	103.74.107.141	103.74.107.141	189.9.36.168	189.9.36.168	0	579	579
	Z-EXT-VPN-AZURE	Z-EXT-VPN-AZURE	62.210.13.20	62.210.13.20	189.9.36.168	189.9.36.168	0	504	504
	Z-EXT-VPN-AZURE	Z-EXT-VPN-AZURE	51.89.124.57	51.89.124.57	189.9.36.168	189.9.36.168	0	483	483
	Z-EXT-VPN-AZURE	Z-EXT-VPN-AZURE	92.118.39.84	92.118.39.84	189.9.36.168	189.9.36.168	0	457	457
	Z-EXT-VPN-AZURE	Z-EXT-VPN-AZURE	104.223.56.130	104.223.56.130	189.9.36.168	189.9.36.168	0	457	457
	Z-EXT-VPN-AZURE	Z-EXT-VPN-AZURE	51.79.108.114	51.79.108.114	189.9.36.168	189.9.36.168	0	457	457
	Z-EXT-VPN-AZURE	Z-EXT-VPN-AZURE	167.160.91.18	167.160.91.18	189.9.36.168	189.9.36.168	0	456	456
	Z-EXT-VPN-AZURE	Z-EXT-VPN-AZURE	89.248.169.6	89.248.169.6	189.9.36.168	189.9.36.168	0	454	454
	Z-EXT-VPN-AZURE	Z-EXT-VPN-AZURE	51.158.145.218	51.158.145.218	189.9.36.168	189.9.36.168	0	451	451
	Z-EXT-VPN-AZURE	Z-EXT-VPN-AZURE	192.241.252.87	192.241.252.87	189.9.36.168	189.9.36.168	0	446	446
	Z-EXT-VPN-AZURE	Z-EXT-VPN-AZURE	212.83.135.137	212.83.135.137	189.9.36.168	189.9.36.168	0	445	445
	Z-EXT-VPN-AZURE	Z-EXT-VPN-AZURE	104.206.128.10	104.206.128.10	189.9.36.168	189.9.36.168	0	416	416
Fri, Apr 15, 2022	Z-INT_INFOVIA-BLOCO_A	Z-EXT-VPN-AZURE	10.223.10.119	10.223.10.119	172.16.170.254	172.16.170.254	443.61 k	439.71 k	883.32 k
	Z-EXT-VPN-AZURE	Z-EXT-VPN-AZURE	68.183.105.150	68.183.105.150	189.9.36.168	189.9.36.168	0	4.05 k	4.05 k
	Z-EXT-VPN-AZURE	Z-EXT-VPN-AZURE	138.68.165.233	138.68.165.233	189.9.36.168	189.9.36.168	0	4.05 k	4.05 k
	Z-EXT-VPN-AZURE	Z-EXT-VPN-AZURE	146.88.240.4	146.88.240.4	189.9.36.168	189.9.36.168	0	3.85 k	3.85 k
	Z-EXT-VPN-AZURE	Z-EXT-VPN-AZURE	209.97.154.197	209.97.154.197	189.9.36.168	189.9.36.168	0	2.25 k	2.25 k
	Z-EXT-VPN-AZURE	Z-EXT-VPN-AZURE	14.1.112.177	14.1.112.177	189.9.36.168	189.9.36.168	0	1.28 k	1.28 k
	Z-EXT-VPN-AZURE	Z-EXT-VPN-AZURE	184.105.247.238	184.105.247.238	189.9.36.168	189.9.36.168	0	1.27 k	1.27 k
	Z-EXT-VPN-AZURE	Z-EXT-VPN-AZURE	148.153.135.178	148.153.135.178	189.9.36.168	189.9.36.168	510	510	1.02 k
	Z-EXT-VPN-AZURE	Z-EXT-VPN-AZURE	155.146.96.69	155.146.96.69	189.9.36.168	189.9.36.168	510	510	1.02 k
	Z-EXT-VPN-AZURE	Z-EXT-VPN-AZURE	209.141.33.68	209.141.33.68	189.9.36.168	189.9.36.168	0	952	952
	Z-EXT-VPN-AZURE	Z-EXT-VPN-AZURE	209.141.32.162	209.141.32.162	189.9.36.168	189.9.36.168	0	952	952
	Z-EXT-VPN-AZURE	Z-EXT-VPN-AZURE	195.154.200.146	195.154.200.146	189.9.36.168	189.9.36.168	0	901	901
	Z-EXT-VPN-AZURE	Z-EXT-VPN-AZURE	51.79.82.87	51.79.82.87	189.9.36.168	189.9.36.168	0	894	894
	Z-EXT-VPN-AZURE	Z-EXT-VPN-AZURE	150.249.174.92	150.249.174.92	189.9.36.168	189.9.36.168	0	678	678
	Z-EXT-VPN-AZURE	Z-EXT-VPN-AZURE	62.210.13.20	62.210.13.20	189.9.36.168	189.9.36.168	0	500	500
	Z-EXT-VPN-AZURE	Z-EXT-VPN-AZURE	139.64.165.114	139.64.165.114	189.9.36.168	189.9.36.168	0	462	462
	Z-EXT-VPN-AZURE	Z-EXT-VPN-AZURE	92.204.248.74	92.204.248.74	189.9.36.168	189.9.36.168	0	459	459
	Z-EXT-VPN-AZURE	Z-EXT-VPN-AZURE	104.223.55.62	104.223.55.62	189.9.36.168	189.9.36.168	0	457	457
	Z-EXT-VPN-AZURE	Z-EXT-VPN-AZURE	51.158.145.218	51.158.145.218	189.9.36.168	189.9.36.168	0	451	451
	Z-EXT-VPN-AZURE	Z-EXT-VPN-AZURE	141.95.145.196	141.95.145.196	189.9.36.168	189.9.36.168	0	450	450
	Z-EXT-VPN-AZURE	Z-EXT-VPN-AZURE	193.46.255.6	193.46.255.6	189.9.36.168	189.9.36.168	0	449	449
	Z-EXT-VPN-AZURE	Z-EXT-VPN-AZURE	20.205.15.107	20.205.15.107	189.9.36.168	189.9.36.168	0	445	445
	Z-EXT-VPN-AZURE	Z-EXT-VPN-AZURE	192.241.213.178	192.241.213.178	189.9.36.168	189.9.36.168	0	431	431
	Z-EXT-VPN-AZURE	Z-EXT-VPN-AZURE	167.94.138.100	167.94.138.100	189.9.36.168	189.9.36.168	0	430	430
	Z-EXT-VPN-AZURE	Z-EXT-VPN-AZURE	51.158.47.138	51.158.47.138	189.9.36.168	189.9.36.168	0	412	412
Fri, Apr 22, 2022	Z-INT_INTERNA	Z-EXT-VPN-AZURE	10.102.11.124	10.102.11.124	172.16.168.6	172.16.168.6	356.84 k	335.65 k	692.49 k



	Z-EXT-VPN-AZURE	Z-EXT-VPN-AZURE	144.217.252.186	144.217.252.186	189.9.36.168	189.9.36.168	0	19.61 k	19.61 k
	Z-EXT-VPN-AZURE	Z-EXT-VPN-AZURE	154.53.52.214	154.53.52.214	189.9.36.168	189.9.36.168	0	5.04 k	5.04 k
	Z-EXT-VPN-AZURE	Z-EXT-VPN-AZURE	146.88.240.4	146.88.240.4	189.9.36.168	189.9.36.168	0	3.93 k	3.93 k
	Z-EXT-VPN-AZURE	Z-EXT-VPN-AZURE	141.95.145.196	141.95.145.196	189.9.36.168	189.9.36.168	0	1.35 k	1.35 k
	Z-EXT-VPN-AZURE	Z-EXT-VPN-AZURE	216.218.206.111	216.218.206.111	189.9.36.168	189.9.36.168	0	1.27 k	1.27 k
	Z-EXT-VPN-AZURE	Z-EXT-VPN-AZURE	148.153.135.178	148.153.135.178	189.9.36.168	189.9.36.168	510	510	1.02 k
	Z-EXT-VPN-AZURE	Z-EXT-VPN-AZURE	155.146.96.69	155.146.96.69	189.9.36.168	189.9.36.168	510	510	1.02 k
	Z-EXT-VPN-AZURE	Z-EXT-VPN-AZURE	103.74.107.141	103.74.107.141	189.9.36.168	189.9.36.168	0	966	966
	Z-EXT-VPN-AZURE	Z-EXT-VPN-AZURE	209.141.33.68	209.141.33.68	189.9.36.168	189.9.36.168	0	952	952
	Z-EXT-VPN-AZURE	Z-EXT-VPN-AZURE	51.79.82.87	51.79.82.87	189.9.36.168	189.9.36.168	0	899	899
	Z-EXT-VPN-AZURE	Z-EXT-VPN-AZURE	195.154.200.146	195.154.200.146	189.9.36.168	189.9.36.168	0	899	899
	Z-EXT-VPN-AZURE	Z-EXT-VPN-AZURE	80.94.93.125	80.94.93.125	189.9.36.168	189.9.36.168	0	897	897
	Z-EXT-VPN-AZURE	Z-EXT-VPN-AZURE	212.71.238.117	212.71.238.117	189.9.36.168	189.9.36.168	0	686	686
	Z-EXT-VPN-AZURE	Z-EXT-VPN-AZURE	62.210.13.20	62.210.13.20	189.9.36.168	189.9.36.168	0	516	516
	Z-EXT-VPN-AZURE	Z-EXT-VPN-AZURE	213.74.173.71	213.74.173.71	189.9.36.168	189.9.36.168	0	485	485
	Z-EXT-VPN-AZURE	Z-EXT-VPN-AZURE	51.89.124.57	51.89.124.57	189.9.36.168	189.9.36.168	0	483	483
	Z-EXT-VPN-AZURE	Z-EXT-VPN-AZURE	185.200.34.191	185.200.34.191	189.9.36.168	189.9.36.168	0	461	461
	Z-EXT-VPN-AZURE	Z-EXT-VPN-AZURE	194.233.75.22	194.233.75.22	189.9.36.168	189.9.36.168	0	459	459
	Z-EXT-VPN-AZURE	Z-EXT-VPN-AZURE	104.223.55.62	104.223.55.62	189.9.36.168	189.9.36.168	0	458	458
	Z-EXT-VPN-AZURE	Z-EXT-VPN-AZURE	154.53.52.216	154.53.52.216	189.9.36.168	189.9.36.168	0	458	458
	Z-EXT-VPN-AZURE	Z-EXT-VPN-AZURE	151.106.5.86	151.106.5.86	189.9.36.168	189.9.36.168	0	458	458
	Z-EXT-VPN-AZURE	Z-EXT-VPN-AZURE	89.248.169.6	89.248.169.6	189.9.36.168	189.9.36.168	0	455	455
	Z-EXT-VPN-AZURE	Z-EXT-VPN-AZURE	62.77.159.43	62.77.159.43	189.9.36.168	189.9.36.168	0	455	455
	Z-EXT-VPN-AZURE	Z-EXT-VPN-AZURE	51.79.108.114	51.79.108.114	189.9.36.168	189.9.36.168	0	454	454
Mon, May 9, 2022	Z-INT_INTERNA	Z-EXT-VPN-AZURE	10.102.11.124	10.102.11.124	172.16.168.6	172.16.168.6	325.95 k	306.37 k	632.32 k
	Z-EXT-VPN-AZURE	Z-EXT-VPN-AZURE	163.172.49.67	163.172.49.67	189.9.36.168	189.9.36.168	0	17.41 k	17.41 k
	Z-EXT-VPN-AZURE	Z-EXT-VPN-AZURE	154.12.248.98	154.12.248.98	189.9.36.168	189.9.36.168	0	14.20 k	14.20 k
	Z-EXT-VPN-AZURE	Z-EXT-VPN-AZURE	185.151.107.102	185.151.107.102	189.9.36.168	189.9.36.168	0	2.56 k	2.56 k
	Z-EXT-VPN-AZURE	Z-EXT-VPN-AZURE	146.88.240.4	146.88.240.4	189.9.36.168	189.9.36.168	0	2.22 k	2.22 k
	Z-EXT-VPN-AZURE	Z-EXT-VPN-AZURE	64.62.197.128	64.62.197.128	189.9.36.168	189.9.36.168	0	1.27 k	1.27 k
	Z-EXT-VPN-AZURE	Z-EXT-VPN-AZURE	185.151.107.101	185.151.107.101	189.9.36.168	189.9.36.168	0	768	768
	Z-EXT-VPN-AZURE	Z-EXT-VPN-AZURE	167.248.133.166	167.248.133.166	189.9.36.168	189.9.36.168	0	673	673
	Z-EXT-VPN-AZURE	Z-EXT-VPN-AZURE	148.153.135.178	148.153.135.178	189.9.36.168	189.9.36.168	306	306	612
	Z-EXT-VPN-AZURE	Z-EXT-VPN-AZURE	51.38.108.254	51.38.108.254	189.9.36.168	189.9.36.168	0	485	485
	Z-EXT-VPN-AZURE	Z-EXT-VPN-AZURE	92.204.248.74	92.204.248.74	189.9.36.168	189.9.36.168	0	459	459
	Z-EXT-VPN-AZURE	Z-EXT-VPN-AZURE	185.31.158.83	185.31.158.83	189.9.36.168	189.9.36.168	0	458	458
	Z-EXT-VPN-AZURE	Z-EXT-VPN-AZURE	151.106.5.86	151.106.5.86	189.9.36.168	189.9.36.168	0	457	457
	Z-EXT-VPN-AZURE	Z-EXT-VPN-AZURE	92.118.39.84	92.118.39.84	189.9.36.168	189.9.36.168	0	455	455
	Z-EXT-VPN-AZURE	Z-EXT-VPN-AZURE	80.94.93.125	80.94.93.125	189.9.36.168	189.9.36.168	0	448	448
	Z-EXT-VPN-AZURE	Z-EXT-VPN-AZURE	192.227.227.211	192.227.227.211	189.9.36.168	189.9.36.168	0	439	439
	Z-EXT-VPN-AZURE	Z-EXT-VPN-AZURE	92.118.39.135	92.118.39.135	189.9.36.168	189.9.36.168	0	439	439
	Z-EXT-VPN-AZURE	Z-EXT-VPN-AZURE	192.241.221.63	192.241.221.63	189.9.36.168	189.9.36.168	0	427	427
	Z-EXT-VPN-AZURE	Z-EXT-VPN-AZURE	51.158.47.138	51.158.47.138	189.9.36.168	189.9.36.168	0	412	412
	Z-EXT-VPN-AZURE	Z-EXT-VPN-AZURE	162.142.125.130	162.142.125.130	189.9.36.168	189.9.36.168	0	302	302
	Z-EXT-VPN-AZURE	Z-EXT-VPN-AZURE	103.74.107.141	103.74.107.141	189.9.36.168	189.9.36.168	0	277	277
	Z-EXT-VPN-AZURE	Z-EXT-VPN-AZURE	66.240.192.138	66.240.192.138	189.9.36.168	189.9.36.168	0	275	275
	Z-EXT-VPN-AZURE	Z-EXT-VPN-AZURE	209.141.32.204	209.141.32.204	189.9.36.168	189.9.36.168	0	238	238
	Z-EXT-VPN-AZURE	Z-EXT-VPN-AZURE	63.142.33.74	63.142.33.74	189.9.36.168	189.9.36.168	46	192	238
	Z-EXT-VPN-AZURE	Z-EXT-VPN-AZURE	209.126.136.3	209.126.136.3	189.9.36.168	189.9.36.168	0	238	238
Thu, Apr 14, 2022	Z-INT_INFOVIA-BLOCO_A	Z-EXT-VPN-AZURE	10.223.10.119	10.223.10.119	172.16.170.254	172.16.170.254	54.69 k	83.65 k	138.34 k
	Z-EXT-VPN-AZURE	Z-EXT-VPN-AZURE	146.88.240.4	146.88.240.4	189.9.36.168	189.9.36.168	0	3.85 k	3.85 k
	Z-EXT-VPN-AZURE	Z-EXT-VPN-AZURE	104.149.138.146	104.149.138.146	189.9.36.168	189.9.36.168	0	1.38 k	1.38 k
	Z-EXT-VPN-AZURE	Z-EXT-VPN-AZURE	65.49.20.103	65.49.20.103	189.9.36.168	189.9.36.168	0	1.27 k	1.27 k
	Z-EXT-VPN-AZURE	Z-EXT-VPN-AZURE	193.124.7.9	193.124.7.9	189.9.36.168	189.9.36.168	0	1.05 k	1.05 k
	Z-EXT-VPN-AZURE	Z-EXT-VPN-AZURE	155.146.96.69	155.146.96.69	189.9.36.168	189.9.36.168	510	510	1.02 k
	Z-EXT-VPN-AZURE	Z-EXT-VPN-AZURE	62.210.13.20	62.210.13.20	189.9.36.168	189.9.36.168	0	1.01 k	1.01 k
	Z-EXT-VPN-AZURE	Z-EXT-VPN-AZURE	205.178.168.144	205.178.168.144	189.9.36.168	189.9.36.168	0	966	966
	Z-EXT-VPN-AZURE	Z-EXT-VPN-AZURE	195.154.200.146	195.154.200.146	189.9.36.168	189.9.36.168	0	902	902
	Z-EXT-VPN-AZURE	Z-EXT-VPN-AZURE	148.153.135.178	148.153.135.178	189.9.36.168	189.9.36.168	408	408	816
	Z-EXT-VPN-AZURE	Z-EXT-VPN-AZURE	144.172.118.37	144.172.118.37	189.9.36.168	189.9.36.168	0	768	768
	Z-EXT-VPN-AZURE	Z-EXT-VPN-AZURE	209.141.33.68	209.141.33.68	189.9.36.168	189.9.36.168	0	714	714
	Z-EXT-VPN-AZURE	Z-EXT-VPN-AZURE	209.141.32.162	209.141.32.162	189.9.36.168	189.9.36.168	0	714	714

www.paloaltonetworks.com

paloalto

	Z-EXT-VPN-AZURE	Z-EXT-VPN-AZURE	199.195.251.107	199.195.251.107	189.9.36.168	189.9.36.168	0	576	576
	Z-EXT-VPN-AZURE	Z-EXT-VPN-AZURE	116.88.114.82	116.88.114.82	189.9.36.168	189.9.36.168	0	558	558
	Z-EXT-VPN-AZURE	Z-EXT-VPN-AZURE	51.89.124.57	51.89.124.57	189.9.36.168	189.9.36.168	0	494	494
	Z-EXT-VPN-AZURE	Z-EXT-VPN-AZURE	78.138.127.110	78.138.127.110	189.9.36.168	189.9.36.168	0	475	475
	Z-EXT-VPN-AZURE	Z-EXT-VPN-AZURE	209.145.63.240	209.145.63.240	189.9.36.168	189.9.36.168	0	461	461
	Z-EXT-VPN-AZURE	Z-EXT-VPN-AZURE	92.204.248.74	92.204.248.74	189.9.36.168	189.9.36.168	0	459	459
	Z-EXT-VPN-AZURE	Z-EXT-VPN-AZURE	139.64.165.114	139.64.165.114	189.9.36.168	189.9.36.168	0	459	459
	Z-EXT-VPN-AZURE	Z-EXT-VPN-AZURE	151.106.5.86	151.106.5.86	189.9.36.168	189.9.36.168	0	458	458
	Z-EXT-VPN-AZURE	Z-EXT-VPN-AZURE	104.223.55.62	104.223.55.62	189.9.36.168	189.9.36.168	0	455	455
	Z-EXT-VPN-AZURE	Z-EXT-VPN-AZURE	170.178.173.154	170.178.173.154	189.9.36.168	189.9.36.168	0	455	455
	Z-EXT-VPN-AZURE	Z-EXT-VPN-AZURE	209.97.154.197	209.97.154.197	189.9.36.168	189.9.36.168	0	450	450
	Z-EXT-VPN-AZURE	Z-EXT-VPN-AZURE	51.158.145.218	51.158.145.218	189.9.36.168	189.9.36.168	0	450	450

Expansão do licenciamento da Solução de Tratamento e Entrega de Dados

Os VIRTUAL APPLIANCES deverão ser compatíveis com a plataforma operacional que será disponibilizada pelo MMFDH de acordo com o subitem enumerado a seguir:

Sistema de Virtualização Microsoft Hyper-V Server 2016 ou versões superiores, a critério do MMFDH;

O MMFDH disponibilizará os equipamentos que atuarão como servidores físicos hospedeiros para os VIRTUAL APPLIANCES;

Cada VIRTUAL APPLIANCE deverá ser capaz de balancear o tráfego de entrada e saída para a Internet de 1 Gbps (um gigabits por segundo) ou superior, de tráfego IP oriundo de clientes externos e internos em enlaces de comunicação de redes distintas, de diferentes operadoras de telecomunicações, sem a necessidade da utilização do protocolo BGP ou qualquer outro protocolo de roteamento;

Os VIRTUAL APPLIANCES deverão operar de forma redundante em topologia de alta disponibilidade, ou seja, na eventualidade da falha de um dos VIRTUAL APPLIANCES, outro APPLIANCE deverá automaticamente assumir, de forma transparente, todas as funções executadas pelo APPLIANCE defeituoso, com sincronismo de configurações e sem perda das sessões que estiverem em curso;

Todos os VIRTUAL APPLIANCES fornecidos deverão estar em linha na data de sua entrega, não sendo aceitos VIRTUAL APPLIANCES que tenham sido descontinuados ou com data de descontinuidade anunciada;

Todos os softwares integrantes das soluções ofertadas, inclusive firmware e sistema operacional dos VIRTUAL APPLIANCES, deverão ser fornecidos na versão mais nova comercializada na data da abertura das Propostas;

Deverão ser fornecidos em conjunto com as soluções ofertadas, todos os acessórios, softwares e opcionais necessários para o correto funcionamento do VIRTUAL APPLIANCES;

Suportar e garantir a instalação em ambiente de alta disponibilidade;

Assegurar que a solução deverá ser capaz de trabalhar no modo Ativo/Standby, com virtual appliance da mesma marca e modelo;

Fornecer uma solução que opere no modo Ativo/Ativo, mantendo o status das conexões. Aceita-se como Ativo/Ativo a utilização de dois endereços Virtuais, onde cada endereço fica ativo em um elemento e standby no outro;

Assegurar que a operação da solução de 2 ou mais appliances virtuais, quando implementada em ambiente redundante suporte sincronismo de sessão entre os dois membros. A falha do virtual appliance principal não deverá causar a interrupção das sessões balanceadas;

A solução deve possuir escalabilidade, podendo crescer na forma de cluster adicionando novos appliances virtuais ou físicos inclusive de modelos diferentes;

Possuir suporte a IPv6;

A solução deve suportar múltiplas tabelas de rotas independentes;

Possuir capacidade para gerenciar os recursos disponíveis de acordo com as funções habilitadas nos equipamentos SLB, GSLB, Aceleração Web, etc.

A solução deve possuir múltiplos domínios de roteamento em IPv4 e IPv6;

Possuir ferramenta online web gratuita na qual seja possível carregar as configurações e receber diagnóstico da solução com informações sobre atualizações, melhores práticas, estado da solução e informações preventivas.

Possuir suporte à funcionalidade de VXLAN, essencial para integração com o ambiente de virtualização (Software Defined Network).

Gerenciamento

Implementar uma configuração de endereçamento IP estático ou dinâmico (DHCP/BOOTP) para o gerenciamento;

Implementar o SNTP (Simple Network Time Protocol) ou NTP (Network Time Protocol);

Permitir acesso in-band via SSH;

Manter internamente múltiplos arquivos de configurações do sistema;

Utilizar SCP ou HTTPS como mecanismo de transferência de arquivos de configuração e Sistema Operacional;

Possuir auto-complementação de comandos na CLI;

Possuir ajuda contextual;

Interface por linha de comando (CLI – Command Line Interface) que possibilite a configuração dos equipamentos;

Possuir, no mínimo, Três níveis de usuários na GUI – Super-Usuário, Usuário com permissões reduzidas, e usuário Somente Leitura;

Os usuários de gerência deverão poder ser autenticados em bases remotas. No mínimo RADIUS, LDAP e TACACS+ deverão ser suportados;

Deverá ser possível receber da base RADIUS, LDAP e TACACS+ o nível de acesso (Grupo ou Permissões);

Possuir Interface Gráfica via Web;

A interface Gráfica deverá permitir a atualização do sistema operacional e/ou a instalação de patches ou Hotfixes sem o uso da linha de comando;

A interface gráfica deverá permitir a configuração de qual partição o equipamento deverá dar o boot;

Possuir um comando, via CLI, que mostre o tráfego de utilização das interfaces (bps e pps);

Suportar a rollback de configuração e imagem;

Possuir e fornecer MIBs compiláveis na plataforma HP Open View Network Node Manager;

Possuir e fornecer geração de mensagens de syslog para eventos relevantes ao sistema;

Possuir configuração de múltiplos syslog servers para os quais o equipamento irá enviar as mensagens de syslog;

Possuir armazenamento de mensagens de syslog em dispositivo interno ao equipamento;

A interface Gráfica deverá permitir a reinicialização do equipamento;

Reinicialização do equipamento por comando na CLI;

Possuir recurso de gerência via SNMP e implementar SNMPv1, SNMPv2c e SNMPV3;

Possuir traps SNMP;

Possui suporte a monitoração utilizando RMON através de pelo menos 4 grupos:

statistics, history, alarms e events

Os logs de sistema devem ter a opção de ser armazenados internamente ao sistema ou em servidor externo;

Implementar Debugging: CLI via console e SSH;

Deve possuir suporte a Link Layer Discovery Protocol (LLDP);

Deve ser possível enviar, pelo menos, as seguintes informações via LLDP: Port ID, TTL, Port Description, System Name, System Description, Management Address, Port VLAN ID, Port and Protocol VLAN ID, VLAN Name, Protocol Identity, Link Aggregation, Maximum Frame Size;

A Solução deve ter a capacidade de permitir a criação de MIBs customizadas;

A Solução deve ter suporte a sFlow;

Distribuição de carga e otimização das aplicações

Suportar todas as aplicações comuns de um Switch Layer 7, como:

Server Load-Balancing;

Firewall Load-Balancing;

Proxy Load-Balancing;

Suportar Balanceamento apenas em direção ao servidor, onde a resposta do servidor real é enviada diretamente ao cliente;

A solução deve permitir o encapsulamento, em camada 3, do tráfego entre o balanceador e o servidor para tráfego IPv4 e IPv6, quando o balanceamento é realizado apenas em direção ao servidor, onde a resposta do servidor real é enviada diretamente ao cliente;

Permitir a clonagem de pools, de forma que a solução envie uma cópia do tráfego para um pool adicional, como por exemplo um pool de IDSs ou Sniffers, para fins de análise de tráfego de rede ou mesmo para identificação de padrões de acesso não permitidos ou indicações de atividade maliciosas ou ataques de rede;

Possuir recursos para balancear servidores com qualquer hardware, sistema operacional e tipo de aplicação;

A solução deve possuir recurso de ativação de grupo prioritário, no qual o administrador pode especificar a quantidade mínima de servidores que devem estar disponíveis em cada grupo e a prioridade dos grupos.

Caso o número de servidores disponíveis fique menor do que o estipulado pelo administrador, a solução deve automaticamente distribuir o tráfego para o próximo grupo com maior prioridade não afetando o serviço.

Caso o número de servidores disponíveis volte ao valor mínimo estipulado pelo administrador, a solução deve automaticamente retirar o grupo com menor prioridade de balanceamento, voltando ao estado original.

Possuir capacidade de abrir um número reduzido de conexões TCP com o servidor e inserir os HTTP requests gerado pelos clientes nestas conexões, reduzindo a necessidade de estabelecimento de conexões nos servidores e aumentando a performance do serviço;

Suportar os seguintes métodos de balanceamento:

Round Robin;

Least Connections;

Weighted Percentage (por peso);

Servidor ou equipamento com resposta mais rápida baseado no tráfego real;

Weighted Percentage dinâmico (baseado no número de conexões);

Dinâmico, baseado em parâmetros de um determinado servidor ou equipamento, coletados via SNMP ou WMI;

A solução deve permitir aplicar criptografia de cookies para a proteção dos cookies utilizados pela aplicação web;

Possuir recursos para balancear as sessões novas, mas preservar sessões existentes no mesmo servidor, implementando persistência de sessão dos seguintes tipos:

Por cookie: inserção de um novo cookie na sessão;

Por cookie: utilização do valor do cookie da aplicação, sem adição de cookie;

Por endereço IP destino;

Por endereço IP origem;

Por sessão SSL;

Através da análise da URL acessada.;

Através da análise de qualquer parâmetro no header HTTP;

Através da análise do MS Terminal Services Session (MSRDP);

Através da análise do SIP Call ID ou Source IP;

Através da análise de qualquer informação da porção de dados (camada 7);

A solução deve utilizar Cache Array Routing Protocol (CARP) no algoritmo de HASH;

O equipamento oferecido deverá suportar os seguintes métodos de monitoramento dos servidores reais:

Layer 3 – ICMP;

Conexões TCP e UDP pela respectiva porta no servidor;

Devem existir monitores predefinidos para, no mínimo, os seguintes protocolos: ICMP, HTTP, HTTPS, Diameter, FTP, SASP, SMB, RADIUS, MSSQL, NNTP, ORACLE, RPC, LDAP, IMAP, SMTP, POP3, SIP, Real Server, SOAP, SNMP e WMI;

Possuir recursos para balanceamento de carga de servidores SIP para VoIP (equipamento SIP PROXY);

Possuir recursos para limitar o número de sessões estabelecidas com cada servidor real;

Possuir recursos para limitar o número de sessões estabelecidas com cada servidor virtual;

Possuir recursos para limitar o número de sessões estabelecidas com cada grupo de servidores;

Possuir recursos para limitar o número de sessões estabelecidas com cada servidor físico;

Realizar Network Address Translation (NAT);

Realizar Proteção contra Denial of Service (DoS);

Realizar Proteção contra Syn flood;

Realizar Limpeza de cabeçalho HTTP;

A solução deve permitir o controle da resposta ICMP por servidor virtual;

Possuir recursos para que a configuração seja baseada em perfis, permitindo uma fácil administração;

Possuir capacidade de geração e gestão de perfis hierarquizados, permitindo maior facilidade na administração de políticas similares;

Permitir a criação de Virtual Servers com endereço IPv4 e os servidores reais com endereços IPv6;

Possuir recursos para executar compressão de conteúdo HTTP, para reduzir a quantidade de informações enviadas ao cliente;

Deve permitir compressão tipo GZIP e Deflate;

Definir qual tipo de compressão será habilitada (gzip1 a gzip9, deflate);

Possuir capacidade para definir compressão especificamente para certos tipos de objetos;

Possuir recursos para fazer aceleração de SSL, onde os certificados digitais são instalados no equipamento e as requisições HTTP são enviadas aos servidores sem criptografia;

Garantir que na aceleração de SSL, tanto a troca de chaves quanto a criptografia dos dados seja realizada com aceleração em hardware, para não onerar o sistema, este item somente é válido para solução em appliance;

Deve possuir capacidade de importação dos certificados e chaves criptográficas, para transações seguras entre cliente/servidor, podendo assim operar em modo “man in the middle”, ou seja, descriptografar, otimizar e re-criptografar o tráfego SSL sem comprometer a segurança da conexão SSL estabelecida previamente entre cliente/servidor. Caso haja falha na leitura da conexão SSL, esta deverá, se assim definido, prosseguir em regime de passthrough.

A solução deve possuir a funcionalidade de espelhamento de conexões SSL.

A solução deve possuir a capacidade de redirecionar o SSL Offload (troca de chaves) de determinado serviço para outro appliance físico que tenha mais capacidade para tratamento SSL. Dessa forma deve ser possível otimizar recursos executando tarefas que exigem muito desempenho para serem tratadas em hardware especializado.

Possuir recursos para configurar o equipamento para recriptografar em SSL a requisição ao enviar para o servidor, permitindo as demais otimizações em ambiente 100% criptografado;

Todas as funcionalidades de inspeção, proteção e aceleração de tráfego criptografado através de SSL/TLS especificadas neste edital devem estar disponíveis quando a conexão segura for estabelecida usando:

Autenticação do servidor por parte do cliente, através da verificação da validade do certificado digital fornecido pelo lado servidor durante o processo de estabelecimento do túnel SSL/TLS;

Autenticação do cliente por parte do servidor, através da solicitação e verificação da validade do certificado digital fornecido pelo cliente durante o processo de estabelecimento do túnel SSL/TLS;

Ambas as autenticações acima mencionadas ocorrendo de forma simultânea;

Ao realizar inspeção, proteção, OffLoad e aceleração de tráfego criptografado através de SSL/TLS, a solução deverá ser capaz de:

Encaminhar ao servidor real via cabeçalho HTTP ou de forma transparente, todo o certificado digital utilizado pelo lado cliente para se autenticar perante o servidor durante o processo de estabelecimento do túnel SSL/TLS;

Encaminhar ao servidor real via cabeçalho HTTP campos específicos do certificado digital utilizado pelo cliente para se autenticar perante o servidor durante o processo de estabelecimento do túnel SSL/TLS;

A solução deve permitir aplicar criptografia de cookies para a proteção dos cookies utilizados pela aplicação web;

Possuir recursos para fazer aceleração de SSL, onde os certificados digitais são instalados no equipamento e as requisições POP3S, IMAPSe SMTPS são enviadas aos servidores sem criptografia;

A solução deve possuir diversos recursos relacionados ao uso de criptografia com o objetivo de otimizar e minimizar o impacto na performance das aplicações. Dentre eles deve ser possível configurar parâmetros como:

SSL session cache Timeout;

Session Ticket;

OCSP (Online Certificate Status Protocol) Stapling;

Dynamic Record Sizing;

ALPN (Application Layer Protocol Negotiation);

Perfect Forward Secrecy;

Suportar a utilização de memória RAM como cache de objetos HTTP, para responder às requisições dos usuários sem utilizar recursos dos servidores;

Possuir capacidade, no uso do recurso de cache, em definir quais tipos de objeto serão armazenados em cache e quais nunca devem ser cacheados;

Garantir que o recurso de cache possa ajustar quanta memória será utilizada para armazenar objetos;

Suporte a otimização do protocolo TCP para ajustes a parâmetros das conexões clientes e servidor;

A solução deve suportar Internet Content Adaptation Protocol (ICAP);

Deve ser capaz de realizar DHCP relay;

Deve possuir relatórios das aplicações, com pelos menos os seguintes gráficos:

Tempo de resposta da aplicação;

Latência;

Conexões para conjunto de servidores, servidores individuais;

Por URL;

A ferramenta de relatórios deve possuir pelo menos os seguintes filtros para a geração dos gráficos:

Servidores virtuais;

Servidores balanceados;

URLs;

Países de origem, baseados em geolocalização (GEOIP);

Dispositivos de origem do cliente (user agent);

Deve possuir framework unificado para configuração da aplicação;

Deve possuir criptografia IPSEC para comunicação entre os balanceadores;

Quando licenciada, a solução deve ter a capacidade de realizar cache transparente das respostas DNS;

A Solução deve ter a capacidade de permitir a criação de MIBs customizadas;

A Solução deve ter suporte a sFlow;

A solução deve possuir múltiplos domínios de roteamento em IPv4 e IPv6;

A solução deve permitir que cada domínio de roteamento utilize BGP, OSPF e RIP em IPv4 e IPv6;

A solução deve suportar Equal Cost Multipath (ECMP);

A solução deve realizar Bidirectional Forward Detection (BFD);

A solução deve ter suporte a Stream Control Transmission Protocol (SCTP);

Deve ter suporte a Transport Layer Security (TLS) Server Name Indication (SNI);

A solução deve possuir monitor HTTP/HTTPS com autenticação NTLM embutida, que permita verificar se o HTTP/HTTPS está operando assim como a plataforma de autenticação;

A solução deve ter suporte a TLS 1.2, SHA 2 Cipher e SHA256 hash;

A solução deve ter suporte a criptografia Perfect Forward Secrecy não apenas para troca de chaves RSA.

A solução deve ser capaz de colocar em fila as requisições TCP que excedam a capacidade de conexões do grupo de servidores ou de um servidor. O balanceador não deverá descartar as conexões que excedam o número de conexões do servidor ou do grupo de servidores:

Deve ser possível configurar o tamanho máximo da fila;

Deve ser possível configurar o tempo máximo de permanência na fila;

A solução deve realizar Controle de Banda Estático para grupos de aplicações e rede;

A solução deve realizar Controle de Banda Dinâmico por aplicação e usuário;

A solução deve realizar Controle de Banda baseado em domínio de roteamento;

Permitir tráfego por parâmetros de QoS (Quality of Service) ou rate-shaping, com pelo menos 2 (duas) filas para priorização de tráfego baseada na camada de aplicação; Através dessa priorização de tráfego e restrição de largura de banda deverá ser possível permitir um melhor nível de serviço para clientes preferenciais em detrimento dos demais clientes. A solução deve permitir a priorização de tráfego de entrada para determinadas aplicações.

A solução deve permitir a criação de túneis IP por domínio de roteamento utilizando GRE, IPIP, EtherIP, PPP;

A solução deve permitir a criação de túneis IP transparente utilizando GRE e IPIP;

Fornecer recursos para o uso de servidores (reals) no mesmo Virtual Server;

Possuir suporte ao protocolo SPDY e HTTP 2.0;

O equipamento deve possuir suporte ao espelhamento de conexões FTP, Telnet, HTTP, UDP, SSL.

O equipamento deverá permitir a sincronização das configurações:

De forma automática;

Manualmente, forçando a sincronização apenas no momento desejado;

Permitir a configuração das interfaces de alta disponibilidade do cluster (heartbeat), com opções para:

Compartilhar a rede de heartbeat com a rede de dados; e

Utilizar uma rede exclusiva para o heartbeat.

Permitir que regras customizadas em linguagem aberta possam ser utilizadas para customizar a distribuição dinâmica de tráfego e aumentar a proteção contra ataques;

A solução deve possuir linguagem de programação open-source que permita a manipulação do tráfego de entrada e saída, viabilizando assim a alteração de parâmetros no cabeçalho e no corpo das mensagens.

Essa linguagem de programação deve permitir a importação de pacotes, garantindo assim que a agilidade e flexibilidade no compartilhamento dos scripts.

Permitir a criação de políticas através de interface gráfica web para manipulação de tráfego através de lógica para pelo menos os seguintes operadores:

GEOIP, http-basic-auth, http-cookie, http-header, http-host, http-method, http-referer, http-set-cookie, http-status, http-uri e http-version.

Deve ser possível tomar as seguintes ações através dessas políticas:

Bloqueio de tráfego;

Reescrita e manipulação de URL;

Registro de tráfego (log);

Adição de informação no cabeçalho HTTP;

Redirecionamento do tráfego para um membro específico;

Selecionar uma política específica para Aplicação Web;

A solução deverá ser capaz de fazer log de todas as sessões, onde os registros deverão conter:

Endereço IP de origem;

Porta TCP ou UDP de origem;

Endereço IP de destino;

Porta TCP ou UDP de destino;

Protocolo de camada 4 (TCP ou UDP);

Data e hora da mensagem;

URL acessada;

A solução deve possuir políticas de uso de senhas administrativas tais como: nível de complexidade, período de validade e travamento de conta devido a erros múltiplos de login de forma nativa ou no mínimo integrado a uma base Active Directory.

A solução deve suportar controle de versão da política de configuração de forma a permitir fazer roll back de políticas aplicadas.

A solução deve ser capaz de analisar a performance de aplicações web.

A solução deve possuir relatórios das aplicações.

Deve prover métricas de aplicações como:

Transações por Segundo;

Tempo de latência do cliente e servidor;

Throughput de requisição e resposta;

Sessões;

A solução deverá gerar informações para permitir análises históricas e auxiliar nos processos de manutenções preventivas, de troubleshooting, de planejamento de capacidade e de análise da experiência dos usuários finais no acesso das aplicações.

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.

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.

A geração de informações históricas deverá permitir:

O detalhamento do tempo de resposta total de carregamento de uma URL e ou Página;

Permitir a correlação de métricas de uso de rede com o comportamento das aplicações.

Proteção contra ataques de aplicação:

A solução deve operar nos modos ativo-ativo e ativo-standby;

O equipamento oferecido deverá proteger a infraestrutura web de ataques contra a camada de aplicação (Camada 7);

Deve possuir tecnologia para mitigação de DDoS em camada 7 baseado em analise comportamental, usando o aprendizado.

Não deve haver a necessidade de intervenção de usuário para configurar thresholds DoS pois esses valores devem ser auto-ajustáveis e adpatativos de acordo com mudanças.

A solução deve possuir a capacidade de automaticamente capturar tráfego no formato TCP Dump relativos a ataques DoS L7, Web Scraping e força bruta permitindo uma análise mais aprofundada por parte do administrador.

A solução deve suportar o uso de firewall camada 3-4 junto com firewall camada 7 no mesmo equipamento/appliance para evitar problemas com o aumento da latência.

O equipamento oferecido deverá possuir a certificação ICSA para Firewall de Aplicação (Web Application Firewall);

Permitir a utilização de um modelo positivo de segurança para proteger contra ataques conhecidos aos protocolos HTTP e HTTPS e às aplicações web acessíveis através destes.

Possuir política de segurança de aplicações web pré-configurada na solução.

Permite a criação de políticas diferenciadas por aplicação e por URL, onde cada aplicação e URL poderão ter políticas totalmente diferentes;

Permitir a criação de políticas diferenciadas por aplicação.

Permite 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;

A solução deverá se integrar a soluções de análise (Scanner) de vulnerabilidade do site. O resultado desta análise deve ser utilizado para configurar as políticas do equipamento;

A solução deve permitir a integração com soluções de análise de vulnerabilidades (Scanner) de terceiros como por exemplo: Trustwave App Scanner (Cenzic), White Hat Sentinel, IBM AppScan, Qualys, Quotium Seeker, HP Webinspect.

A solução deve permitir a inspeção de upload de arquivos para os servidores de aplicação;

Essa inspeção pode ser feito via integração ICAP. Deve ser possível integrar com diferentes softwares de Antivírus;

Deve se integrar com o software de Antivírus existente no ambiente da Contratante.

Permitir que regras customizadas em linguagem aberta possam ser utilizadas para customizar e aumentar a proteção contra ataques recentes;

Permitir a integração com Firewall de Database de outros fabricantes.

A solução deve se integrar com outras soluções de segurança e análise de logs de outros fabricantes.

O fabricante da solução deve disponiibilizar também a comercialização como serviço na nuvem (WAFaaS), incluindo o serviço de migrar as regras/políticas existentes do Datacenter para a nuvem.

Deve possuir tecnologia de detecção de anomalias baseado nos IDs dos dispositivos, permitindo a detecção de DoS, ataques de força bruta e ataques de sequestro de sessão. Deve ser possível filtar relatórios por IDs de dispositivos.

A solução deve permitir incluir em blacklist os endereços IPs que repetidamente falharem a desafios no browser. Portanto o sistema não precisa usar recursos para mitigar trafego enviado por esses endereços Ips. Ao entrar em Blacklist o sistema automaticamente bloqueia os pacotes enviados por esse endereço por um período de tempo.

A solução deve suportar e fazer a proteção do tráfego em cima de protocolo WebSocket.

A solução deve possibilitar o uso de multiplas formas de logging remoto ao mesmo tempo para a mesma aplicação. Portanto dever ser possível por exemplo logar os requests válidos num servidor de SIEM e os requests inválidos em outro servidor de SIEM de outra marca e modelo.

A solução deverá possuir funcionalidade de proteção positiva e segura contra ataques, como:

Acesso por Força Bruta;

Ameaças Web AJAX/JSON;

DoS e DDoS camada 7;

Buffer Overflow;

Cross Site Request Forgery (CSRF);

Cross-Site Scripting (XSS);

SQL Injection;

Parameter tampering

Cookie poisoning;

HTTP Request Smuggling;

Manipulação de campos escondidos;

Manipulação de cookies;

Roubo de sessão através de manipulação de cookies;

Sequestro de sessão;

Força bruta no browser;

XML bombs/DoS;

Checagem de consistência de formulários;

Checagem do cabeçalho do “user-agent” para identificar clientes inválidos.

A solução deve suportar o uso de páginas de login AJAX/JSON tanto com configuração manual como descoberta automatica;

Deverá ser capaz de identificar e bloquear ataques através de:

Regras de verificação personalizadas – política de segurança configurada.

Assinaturas, com atualização periódica da base pelo fabricante;

As assinaturas devem ser atualizadas durante o período do contrato sem que seja necessário nenhum custo a mais por parte da CONTRATANTE na aquisição de novas licenças ou subscrições. Deve fazer parte da solução de WAF ofertada.

Prevenir contra vazamento de dados sensíveis (mensagens de erro HTTP, códigos das aplicações, entre outros) dos servidores de aplicação, retirando os dados ou mascarando a informação nas páginas enviadas aos usuários.

Permitir a customização da resposta de bloqueio.

Permitir a liberação temporária ou definitiva (white-list) de endereços IP bloqueados por terem originados ataques detectados pela solução.

Deve permitir limitar o número de conexões e requisições por IP de origem para cada endereço IP Virtual.

Deve permitir adicionar, automaticamente e manualmente, em uma lista de bloqueio, os endereços IP de origem que ultrapassarem o limite estabelecido, por um período de tempo determinado através de configuração.

Deve permitir criar lista de exceção (white list) por endereço IP específico ou faixa de sub-rede.

A solução deve suportar o modelo de segurança positiva definido pelo OWASP, pelo menos o que consta no TOP 10.

Permitir o uso do parâmetro HTTP X-Forwarded-For como parte da política de controle.

Deverá implantar, no mínimo, as seguintes funcionalidades:

Proteção contra Buffer Overflow;

Checagem de URL;

Checagem de métodos HTTP utilizados (GET, POST, HEAD, OPTIONS, PUT, TRACE, DELETE, CONNECT);

Proteção contra envios de comandos SQL escondidos nas requisições enviadas a bases de dados (SQL Injection);

Proteção contra Cross-site Scripting;

Funcionalidade de Cookie Encryption;

Checagem de consistência de formulários;

Checagem do cabeçalho “user-agent” para identificar clientes inválidos.

Implementar as seguintes funcionalidades:

Cloaking – Proteção contra exposição de informações do ambiente e servidores internos como:

Sistema operacional e servidor web com impressão digital;

Esconder qualquer mensagem de erro HTTP dos usuários;

Remover as mensagens de erro às páginas que serão enviadas aos usuários;

Permitir a utilização de uma página HTML informativa e personalizável como HTTP Response aos bloqueios.

Deve ser possível verificar o endereço de origem do pacote IP no cabeçalho IP e no parâmetro X-forwarded-for (XFF).

Deve suportar a criação de políticas por geo-localização, permitindo que o tráfego de determinado(s) País/Países seja(m) bloqueado(s).

Possuir mecanismo de aprendizado automático capaz de identificar todos os conteúdos das aplicações, incluindo URLs, parâmetros URLs, campos de formulários, o que se espera de cada campo (tipo de dado, tamanho de caracteres), cookies, arquivos XML e elementos XML.

O equipamento oferecido deverá possuir uma funcionalidade de criação automática de políticas, onde a política de segurança é criada e atualizada automaticamente baseando-se no tráfego real observado à aplicação;

O perfil aprendido de forma automatizada pode ser ajustado, editado ou bloqueado;

O equipamento oferecido deverá possuir proteção baseada em assinaturas para prover proteção contra ataques conhecidos. Deverá ser possível desabilitar algumas assinaturas específicas em determinados parâmetros, como uma exceção a regra geral;

A atualizações de assinaturas deverão passar por um período configurável de testes, ondes nenhuma requisição que viole a assinatura será bloqueada, apenas informada no relatório. Este processo deve ser automatizado, não sendo necessário criar regras específicas a cada atualização de assinatura;

O equipamento oferecido deverá permitir o bloqueio de ataques DoS na camada 7, possuindo também a opção de apenas registrar o ataque, sem tomar nenhuma ação de bloqueio;

O equipamento oferecido deverá possuir as seguintes formas de detecção de ataques DoS na camada de aplicação:

Número de requisições por segundo enviados a uma URL específica;

Número de requisições por segundo enviados de um IP específico;

Detecção através de código executado no cliente com o objetivo de detectar interação humana ou comportamento de robôs (bots);

Número máximo de transações por segundo (TPS) de um determinado IP;

Aumento de um determinado percentual do número de transações por segundo (TPS);

Aumento do stress do servidor de aplicação;

O equipamento oferecido deverá permitir o bloqueio de ataques de força bruta de usuário/senha em páginas de acesso (login) que protegem áreas restritas. Este bloqueio deve limitar o número máximo de tentativas e o tempo do bloqueio deverá ser configurável;

O equipamento oferecido deverá permitir o bloqueio de determinados endereços IPs que ultrapassarem um número máximo de violações por minuto. O período de bloqueio deverá ser configurável e durante este período todas as requisições do cliente serão bloqueadas automaticamente;

O equipamento oferecido deverá permitir o bloqueio de robôs (bots) que acessam a aplicação através de detecção automática, não dependendo de cadastros manuais. Robôs conhecidos do mercado, como Google, Yahoo e Microsoft Bing deverão ser liberados por padrão;

O equipamento oferecido deverá permitir o cadastro de robôs que podem acessar a aplicação;

Possuir política de segurança de aplicações pré-configuradas no equipamento para pelo menos as seguintes aplicações:

IBM Lotus Domino;

Microsoft ActiveSync v1.0, v2.0;

Microsoft OWA in Exchange 2003, 2007, 2010;

Microsoft SharePoint 2003, 2007, 2010;

Oracle 10g Portal;

Oracle Application 11i;

Oracle PeopleSoft Portal;

SAP NetWeaver;

O equipamento oferecido deverá implementar proteção ao JSON (JavaScript Object Notation);

Possuir firewall XML integrado – suporte a filtro e validação de funções XML específicas da aplicação;

Implementar a segurança de web services, através dos seguintes métodos:

Criptografar/Decriptografar partes das mensagens SOAP;

Assinar digitalmente partes das mensagens SOAP;

Verificação de partes das mensagens SOAP;

Prevenir o vazamento de informações, permitindo o bloqueio ou a remoção dos dados confidenciais;

Prevenir que erros de aplicação ou infraestrutura sejam mostrados ao usuário;

Deverá ter integração, via ICAP, com servidor de antivírus para verificação dos arquivos a serem carregados nos servidores;

Permitir o uso do parâmetro HTTP X-Forwarded-For como parte da política de controle;

Deverá proteger o protocolo FTP com pelo menos os seguintes métodos:

Determinar os comandos FTP permitidos;

Requests FTP anônimos;

Checar compliance com o protocolo FTP;

Proteger contra ataques de força bruta nos logins;

Deverá proteger o protocolo SMTP com pelo menos os seguintes métodos:

A comunicação deve ser aderente a RFC 2821;

Limitar o número de mensagens;

Validar registro SPF do DNS;

Determinar quais métodos SMTP podem ser utilizados;

Deverá armazenar os log localmente ou exportar para Syslog server;

Deverá proteger contra atraques CSRF (Cross-Site Request Forgery), podendo ser possível especificar quais URLs serão examinadas;

Deverá possuir controle de fluxo por aplicação permitindo definir o fluxo de acesso de uma URL para outra da mesma aplicação. Dessa forma qualquer tentativa de acesso a um determido site que não siga o fluxo passando pelas URLs pré-definidas deverá ser bloqueado como uma tentativa de acesso ilegal.

A solução deve fornecer relatórios consolidados de ataques com pelo menos os seguintes dados: Resumo geral com as políticas ativas, anomalias e estatísticas de tráfego, Ataques DoS, Ataques de Força Bruta, Ataques de Robôs, Violações, URL, Endereços IP, Países, Severidade e PCI Compliance.

Deverá permitir o agendamento de relatórios a serem entregues por email;

Fornecer os seguintes Gráficos de alertas por:

Política de segurança;

Tipos de ataques;

Violações;

URL;

Endereços IP;

Países;

Severidade;

Código de resposta;

Métodos;

Protocolos;

Vírus;

Usuário;

Sessão;

Deverá exportar as requisições que contém os ataques, pelo menos nos formatos PDF e binário;

Deve possuir relatório em tempo real sobre ataques DoS L7, atualizado automaticamente;

A solução deve mostrar o impacto de ataques DoS L7 na performance e memória do servidor;

Os logs devem indicar o momento de início e final de um ataque DoS L7;

Possuir método de mitigação de DoS L7 baseado em: CAPTCHA ; Descarte de todas as requisições de um determinado IP e/ou país suspeito; Geolocalização, incluindo a prevenção com CAPTCHA para países suspeitos que ultrapassarem os thresholds; Defesa proativa contra Bot, através da injeção de um desafio JavaScript para detectar se é um usuário legítimo ou robô;

A solução deve permitir que ao detectar um falso positivo, o administrador aceite a requisição e atualize a política automaticamente.

A solução ao se integrar com um Scanner de vulnerabilidade deve mostrar quais a vulnerabilidades podem ser resolvidas automaticamente (pela própria solução de WAF) e quais podem ser resolvidas manualmente, pelo próprio administrador. No caso de resolução manual, deve ainda mostrar um guia com os passos necessários para resolver aquela vulnerabilidade, inclusive com a avisos de possíveis consequências na aplicação Web.

A solução deve classificar o nível de violação de uma requisição, possuindo pelo menos 5 níveis, onde o nível 5 é referente a violação mais grave e portanto deve ter prioridade.

A solução deve possuir proteção de DDoS L7 baseado em análise comportamental, sem precisar de nenhuma configuração manual.

Suportar os protocolos HTTP/1.0, HTTP/1.1 e HTTP/2.0.

Suportar codificação HTML "application/x-www-form-urlencoded".

Suportar Cookies v0 e v1.

Suportar codificação fragmentada (chunked encoding) em requisições e respostas.

Suportar compressão de requisições e respostas.

Suportar validação de protocolo, como:

Possibilidade de restringir uso de métodos;

Possibilidade de restringir protocolos e versões de protocolos;

Strict (per-RFC) Request Validation;

Validar caracteres URL-encoded; e

Validação de codificação fora de padrão %uXXYY.

Suportar restrições de HTML, como:

Tamanho do nome de parâmetros;

Tamanho dos valores de parâmetros; e

Combinação de tamanho de parâmetros (nome e valores).

Suportar POST no upload de arquivo.

Permitir configurar ou oferecer restrições para tamanho individual de arquivo.

Permitir customizar a lógica na inspeção de upload de arquivos.

Suporte para os métodos Basic, Digest e NTLM para autenticação.

Suporte para autenticação por back end tipo LDAP e Microsoft Active Directory.

Capacidade de filtrar cabeçalhos, corpo e status de respostas.

Suportar as seguintes técnicas de detecção:

URL-decoding;

Terminação Null Byte String;

Paths auto-referenciados;

Case de caracteres misturados;

Uso excessivo de espaços em branco;

Remoção de comentários;

Decodificação de entidades HTML; e

Caracteres de escape.

Possuir registro de logs com as seguintes características:

Em cada registro de log de acesso deve ser inserido um identificador de transação HTTP que deve ser único, envolvendo o par requisição/resposta;

Os registros de log de acesso e eventos devem ser armazenados em arquivo ou em banco de dados que permita a exportação ou em outro formato aberto como 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;

Permitir configurar a retenção dos logs por tempo e volume; e

Ter capacidade para detecção, remoção ou codificação de dados sensíveis do log.

A solução deverá gerar relatórios com as seguintes características:

Permitir a filtragem por data ou hora, endereço IP e tipo de incidente;

Permitir a geração de relatórios sob demanda ou pré-programados periodicamente (diário e semanal); e

Permitir a geração de relatórios em formatos PDF/A (versão aberta) e HTML.

Possuir as seguintes características de gerenciamento:

Facilidade para liberação de regras aprendidas automaticamente que estejam gerando grande quantidade de falso positivo;

Facilidade para transformar um ataque detectado e considerado falso positivo como regra do firewall;

Facilidade para aplicar diferentes regras para diversas aplicações;

Capacidade para customizar regras de negação de serviço;

Capacidade para combinar detecção e prevenção na construção das regras; e

Capacidade para desfazer a aplicação de uma regra.

Possuir mecanismos que garantam a capacidade de gerenciamento do equipamento sob condições de alto tráfego.

A solução deve apresentar perfil de aprendizagem automática com:

Capacidade de aprendizagem automática sem intervenção humana; e

Capacidade de inspeção das regras criadas automaticamente.

Permitir o gerenciamento da configuração com as seguintes características:

Gerenciamento por autenticação dos usuários e as autorizações baseadas em perfis (roles); e

Capacidade de gerenciamento remoto dos equipamentos.

Apresentar logs e relatórios administrativos com as seguintes características:

Capacidade para identificar e notificar falhas do sistema ou perda de performance;

Capacidade de agregação de informações para simplificar a revisão das atividades do dispositivo; e

Capacidade para gerar estatísticas de serviço e sistema.

Possuir suporte a XML:

Para proteção de WebServices;

Em conformidade com a especificação WS-I básico; e

Com capacidade de restringir métodos do WebService via definição em WSDL.

Suportar funções de camuflagem (cloaking), como:

Esconder qualquer mensagem de erro http dos usuários; e

Remover as mensagens de erro das paginas que serão enviadas aos usuários.

Proteger a aplicação Web contra robôs sofisticados através da combinação de desafios enviados ao browser do usuário e tecnicas avançadas de analise comportamental.

A solução deve ecnriptar dados e credenciais na camada de aplicação, sem ter a necessidade de atualizar a aplicação.

Essas informações devem ser encriptadas para proteger o login e as credenciais dos usuários e com isso os dados da aplicação.

Deve aprender automaticamente o comportamento da aplicação e combinar o comportamento heurístico do trafego com o stress do servidor de aplicação para determinar uma condição de DDoS.

Ao detectar uma condição de DDoS, assinaturas dinâmicas devem ser automaticamente criadas e implementadas em tempo real para proteção da aplicação.

Deve possuir uma proteção proativa contra ataques automatizados por robôs e outras ferramentas de ataque.

Deve proteger informações sensíveis e confidenciais da interceptação por terceiros, através da criptografia de dados quando ainda no browser do usuário.

Deve proteger esses dados criptografados de malwares e keyloggers.

Deve possuir proteção contra ataques DDoS, através da análise de comportamento de trafego usando técnicas de analise de dados e Machine Learning.

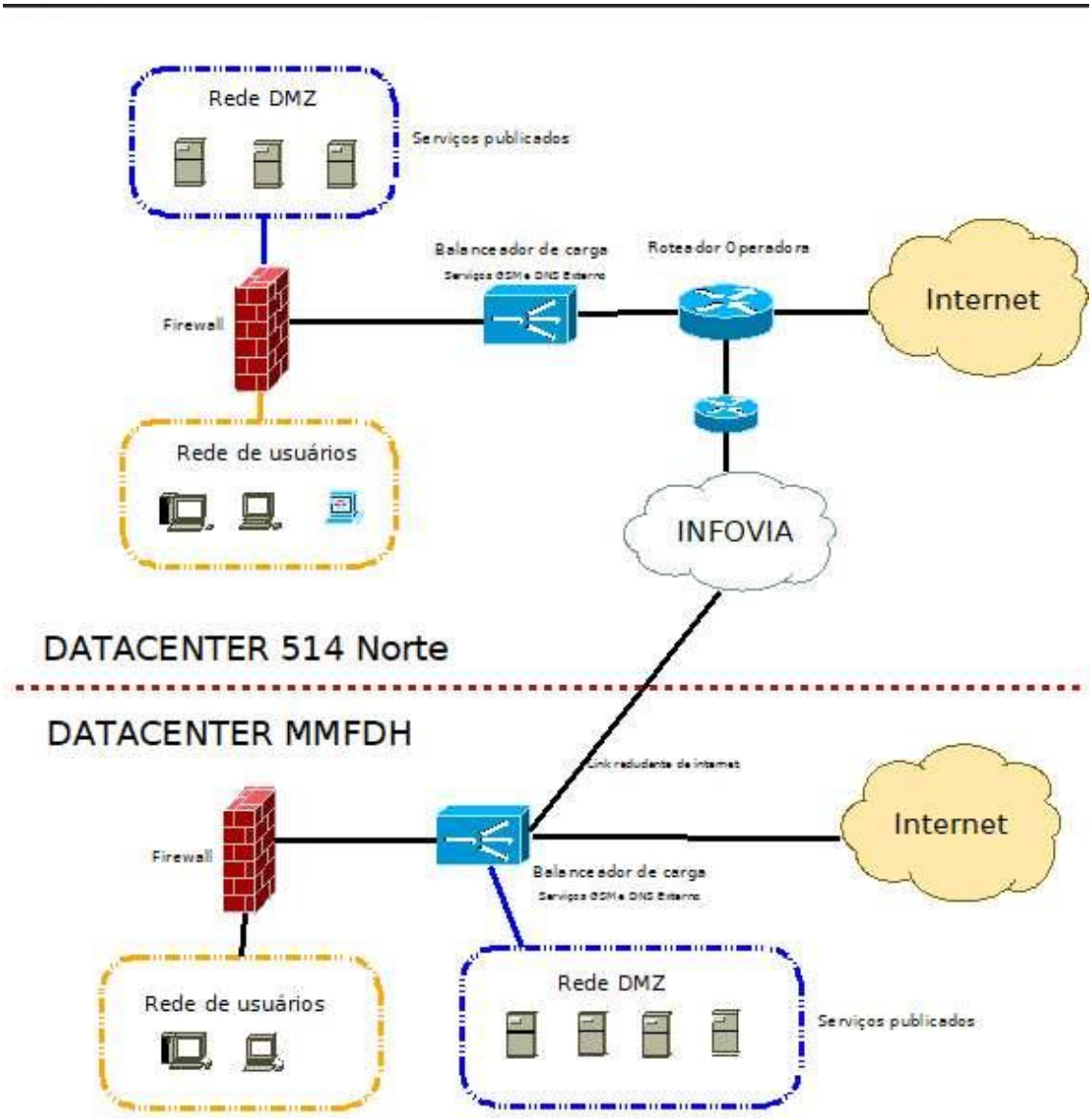
Através da analise continua de carga e monitoração de saúde de servidores, deve ser possível identificar anomalias e mitiga-las.

Deve ajudar a previnir contra ataques de Credential Stuffing, onde bases de credenciais expostas na Internet são usados para tentativa de acesso de outras aplicações Web.

Ainda relação a Expansão do licenciamento da Solução de Tratamento e Entrega de Dados este licenciamento permite uma instalação em outro site, permitindo uma efetiva disponibilidade.

Os relatórios elencados no item “b” evidencias a quantidade de tráfego de serviços em nuvem, os quais demanda a adoção de medidas no sentido de aprimorar a sua segurança de acesso e também a disponibilidade. Considerando-se que as funcionalidades da solução adquirida no Contrato n° 35/2018 não contemplam serviços em nuvem, propõe-se a expansão do licenciamento, de modo a incluir os serviços do Office 365 e da VPN Azure. Para tanto, será necessária a contratação de um cluster do appliance virtual, o qual é capaz de atender de forma satisfatória à demanda posta e à demanda futura de segurança e disponibilidade dos serviços em nuvem.

Em relação à Expansão do licenciamento da Solução de Tratamento e Entrega de Dados, importa destacar que o licenciamento permite uma instalação em outro site (datacenter) fisicamente distante, permitindo uma efetiva disponibilidade. A figura a seguir demonstra a proposta de topologia de instalação da ferramenta:

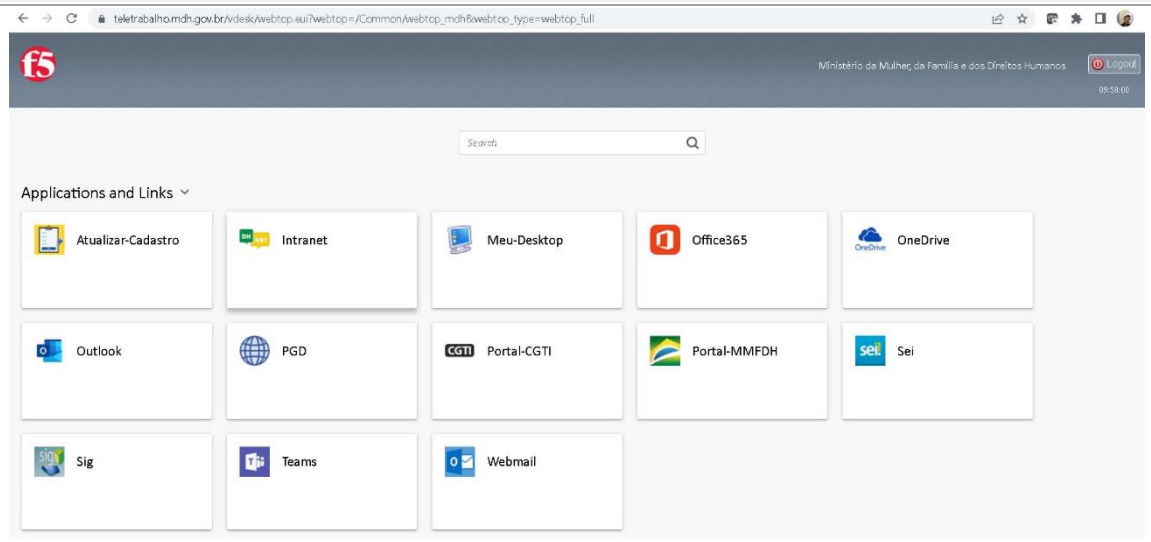


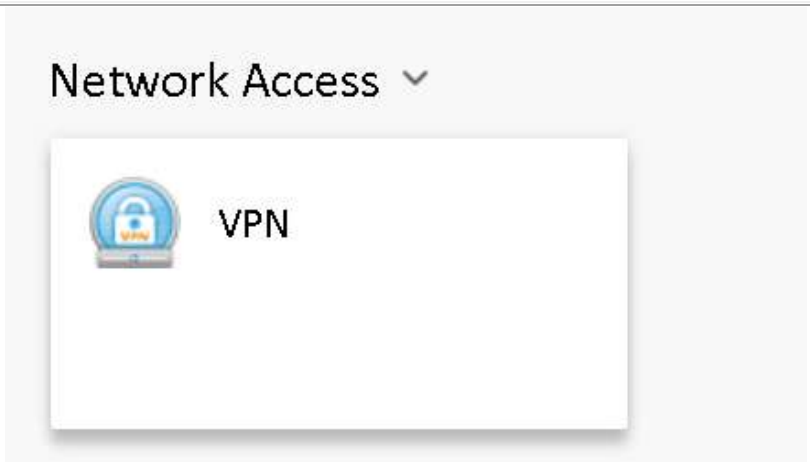
É importante também destacar o papel fundamental que a Solução de Balanceamento F5 teve por ocasião da pandemia da Covid-19. Graças à ferramenta, foi criado o portal teletrabalho.mdh.gov.br. Considerando a determinação para afastamento de todos os

servidores e colaborados do Ministério que estavam em trabalho presencial, coube à CGTI disponibilizar os meios para que esses profissionais pudessem continuar executando suas tarefas, de forma a evitar a interrupção dos serviços da Pasta à sociedade.

Sendo, assim, em tempo recorde, foi criado e disponibilizado o portal Teletrabalho, o qual, além da imensurável valia apresentada naquela ocasião, é a ferramenta oficial utilizada pelo Ministério para acesso à sua rede de dados pelos servidores participantes do Programa de Gestão e quaisquer outros que necessitam de acesso externo à rede.

Diante o exposto, o mecanismo utilizado para garantir o acesso seguro aos recursos digitais do teletrabalho deste Ministério e realizado através do **F5** Networks conforme imagem abaixo:





Um dos principais produtos **F5** Networks é o **Big-IP** que trata-se de um equipamento de Gerenciamento de Tráfego de Aplicativos (Application Traffic Management).

O sistema **BIG-IP** (este nome único era/é usado para se referir ao controlador da rede de aplicações web, no geral, sendo um termo abrangente para hardware e software) configura-se entre os melhores no mercado, pois seu hardware possui uma alta capacidade de processamento, o que permite a hospedagem de inúmeras conexões simultâneas, isso porque ele realiza a distribuição da demanda entre os vários servidores disponíveis.

Diante do exposto e contemplando a solução de tratamento e entrega de dados do MMFDH, pelo acesso ao Teletrabalho, o equipamento tem por finalidade:

Prover acesso seguro aos sistemas administrativos e corporativos utilizados pelo MMFDH (SEI, correio eletrônico, Internet, dentre outros) para o desempenho de suas funções.

Prover acesso de boa qualidade aos recursos providos externamente a rede do MMFDH através do tratamento e melhor utilização da capacidade oferecida pelos links de internet.

Prover acesso de boa qualidade priorizando o tráfego das aplicações classificadas como essenciais para alcançar os objetivos primários do Órgão.

Os serviços de manutenção corretiva, assistência e suporte técnico para os equipamentos citados deverão contemplar a substituição de equipamentos e/ou módulos e/ou componentes (fontes, “fans” e sfp) que apresentem defeito durante a vigência do contrato.