MINISTÉRIO DA JUSTIÇA E SEGURANÇA PÚBLICA

EDITAL DE LICITAÇÃO

PREGÃO ELETRÔNICO Nº 14/2021

08006.001082/2020-13

Torna-se público, para conhecimento dos interessados, que a União, por intermédio do Ministério da Justiça e Segurança Pública, por meio da Pregoeira designada pela Portaria CGL nº 173, de 06 de agosto de 2021, da Coordenação-Geral de Licitações e Contratos da Subsecretaria de Administração, publicada no D.O.U. de 13 de agosto de 2021, realizará licitação para registro de preços, na modalidade PREGÃO, na forma ELETRÔNICA, **com critério de julgamento menor preço** por grupo, sob a forma de execução indireta, no regime de empreitada por preço unitário, nos termos da Lei nº 10.520, de 17 de julho de 2002, do Decreto nº 10.024, de 20 de setembro de 2019, do Decreto 9.507, de 21 de setembro de 2018, do Decreto nº 7.746, de 05 de junho de 2012, do Decreto nº 7.892, de 23 de janeiro de 2013, da Instrução Normativa SGD/ME nº 1, de 4 de abril de 2019, das Instruções Normativas SEGES/MP nº 05, de 26 de maio de 2017 e nº 03, de 26 de abril de 2018 e da Instrução Normativa SLTI/MP nº 01, de 19 de janeiro de 2010, da Lei Complementar nº 123, de 14 de dezembro de 2006, da Lei nº 11.488, de 15 de junho de 2007, do Decreto nº 8.538, de 06 de outubro de 2015, , da Portaria MJSP nº 513, de 15 de setembro de 2020, aplicando-se, subsidiariamente, a Lei nº 8.666, de 21 de junho de 1993 e as exigências estabelecidas neste Edital.

Data da sessão: 29/09/2021

Horário: 9h

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

1. DO OBJETO

1.1. O objeto da presente licitação é a escolha da proposta mais vantajosa para a contratação de serviços de tecnologia da informação e comunicação de empresa especializada, mediante Sistema de Registro de Preços, para prestação de serviços de implementação de solução para avaliação de vulnerabilidades em ativos de tecnologia da informação e aplicações web ao Ministério da Justiça e Segura Pública, compreendendo: a subscrição de licenças de software, abarcando a atualização, o treinamento e o suporte técnico (24x7); e o serviço técnico especializado, conforme condições, quantidades e exigências estabelecidas neste Edital e seus anexos.

1.2. A licitação será dividida em grupos, formados por um ou mais itens, conforme tabela constante do Termo de Referência, facultando-se ao licitante a participação em quantos grupos forem

de seu interesse, devendo oferecer proposta para todos os itens que os compõem.

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

1.4. Cada serviço ou produto do lote deverá estar discriminado em itens separados nas propostas de preços, de modo a permitir a identificação do seu preço individual na composição do preço global, e a eventual incidência sobre cada item das margens de preferência para produtos e serviços que atendam às Normas Técnicas Brasileiras - NTB.

2. DOS RECURSOS ORÇAMENTÁRIOS

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

2.1.1. Programa de Trabalho: 04122003220000001

2.1.2. Natureza da Despesa: 339040.06 (Itens 1 e 3 - Subscrição de software) e 339035.04 (Itens 2 e 4 - Consultoria em TIC)

2.1.3. Plano Interno (PI): GL67OTCGLTI

2.1.4. Plano de Trabalho Resumido (PTRES): 172184

2.1.5. Fonte: 0100

2.1.6. Ação: 2000

2.1.7. Plano Orçamentário (PO): 000C

3. DO REGISTRO DE PREÇOS

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

4. DO CREDENCIAMENTO

4.1. 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.

4.2. 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.

4.3. 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.

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

4.5. 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.

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

5. DA PARTICIPAÇÃO NO PREGÃO

5.1. 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.

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

5.2. Não poderão participar desta licitação os interessados:

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

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

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

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

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

5.2.6. entidades empresariais que estejam reunidas em consórcio;

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

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

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

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

5.3. 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.

5.3.1. 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);

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

5.5. É vedada a contratação de uma mesma empresa para dois ou mais serviços licitados, quando, por sua natureza, esses serviços exigirem a segregação de funções, tais como serviços de execução e de assistência à fiscalização, assegurando a possibilidade de participação de todos licitantes em ambos os itens.

5.6. Como condição para participação no Pregão, o licitante assinalará “sim” ou “não” em

campo próprio do sistema eletrônico, relativo às seguintes declarações:

5.6.1. 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.

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

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

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

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

5.6.5. 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;

5.6.6. que a proposta foi elaborada de forma independente, nos termos da Instrução Normativa SLTI/MP nº 2, de 16 de setembro de 2009.

5.6.7. 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;

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

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

5.6.9.1. 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.

5.7. Deverá, ainda, apresentar declaração que tem ciência de que, caso vencedor, deverá implementar Programa de Integridade, nos termos do item 5.2.32 do Termo de Referência.

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

6. DA APRESENTAÇÃO DA PROPOSTA E DOS DOCUMENTOS DE HABILITAÇÃO

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

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

6.3. 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.

6.4. 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.

6.5. 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.

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

6.7. 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.

6.8. 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.

7. DO PREENCHIMENTO DA PROPOSTA

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

7.1.1. valor unitário e total do item;

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

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

7.3. Nos valores propostos estarão inclusos todos os custos operacionais, encargos previdenciários, trabalhistas, tributários, comerciais e quaisquer outros que incidam direta ou indiretamente na prestação dos serviços.

7.3.1. 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.

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

7.4. 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:

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

7.4.2. 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.

7.5. 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.

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

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

7.8. 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.

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

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

7.10.1. 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.

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

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

8.2. 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.

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

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

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

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

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

8.5. 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.

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

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

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

8.8. O intervalo mínimo de diferença de valores ou percentuais entre os lances, que incidirá tanto em relação aos lances intermediários quanto em relação à proposta que cobrir a melhor oferta deverá ser de 1% (um por cento).

8.9. 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.

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

8.11. 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.

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

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

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

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

8.16. 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.

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

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

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

8.20. 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 artigos 44 e 45 da LC nº 123, de 2006, regulamentada pelo Decreto nº 8.538, de 2015.

8.21. 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.

8.22. 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.

8.23. 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.

8.24. 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.

8.25. 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.

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

8.26.1. prestados por empresas brasileiras;

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

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

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

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

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

8.28.2. 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.

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

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

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

9. DA ACEITABILIDADE DA PROPOSTA VENCEDORA.

9.1. Encerrada a etapa de negociação, o pregoeiro examinará a proposta classificada em primeiro lugar quanto à adequação ao objeto e à compatibilidade do preço em relação ao máximo estipulado para contratação neste Edital e em seus anexos, observado o disposto no parágrafo único do art. 7º e no § 9º do art. 26 do Decreto n.º 10.024/2019.

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

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

9.2.2. contenha vício insanável ou ilegalidade;

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

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

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

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

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

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

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

9.5. 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.

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

9.6. 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.

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

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

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

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

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

9.10. 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.

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

10. DA HABILITAÇÃO

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

a) SICAF;

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

c) Cadastro Nacional de Condenações Cíveis por Atos de Improbidade Administrativa, mantido pelo Conselho Nacional de Justiça (www.cnj.jus.br/improbidade_adm/consultar_requerido.php).

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

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

10.1.2. 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.

10.1.2.1. 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.

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

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

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

10.1.4. 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.

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

10.2.1. 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;

10.2.2. 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.

10.2.3. 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.

10.3. 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.

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

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

10.6. 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.

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

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

10.8. **Habilitação jurídica:**

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

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

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

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

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

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

10.9. **Regularidade fiscal e trabalhista:**

10.9.1. prova de inscrição no Cadastro Nacional de Pessoas Jurídicas;

10.9.2. 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.

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

10.9.4. 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;

10.9.5. 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;

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

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

10.10. **Qualificação Econômico-Financeira:**

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

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

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

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

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

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

10.10.4. As empresas, cadastradas ou não no SICAF, que apresentarem resultado inferior ou igual a 1(um) em qualquer dos índices de Liquidez Geral (LG), Solvência Geral (SG) e Liquidez Corrente (LC), deverão comprovar patrimônio líquido de 10 % (dez por cento) do valor estimado da contratação ou do item pertinente.

10.11. **Qualificação Técnica:**

10.11.1. 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.

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

10.11.1.1.1. Grupo 1 - item 1: No mínimo, 1 (um) Atestado de Capacidade Técnica, fornecido por pessoa jurídica de direito público ou privado, comprovando que a empresa já executou ou esteja executando, em empresa ou órgão da Administração Pública, de forma satisfatória, o fornecimento de,

licenciamento referente à plataforma de avaliação de vulnerabilidades e auditoria de configurações de ativos de rede, no mínimo, de 450 (quatrocentos e cinquenta) IP´s.

10.11.1.1.2. Grupo 2 - item 3: No mínimo, 1 (um) Atestado de Capacidade Técnica, fornecido por pessoa jurídica de direito público ou privado, comprovando que a empresa já executou ou esteja executando, em empresa ou órgão da Administração Pública, de forma satisfatória, o fornecimento de licenciamento para solução de análise em aplicações Web ou o fornecimento, instalação, configuração e suporte continuado, por no mínimo 12 meses de solução de segurança para aplicações web.

10.11.1.1.3. Quando couber, a documentação relativa à qualificação técnica do licitante deverá constar em dispositivo editalício específico, quando a situação demandada a exigir.

10.11.1.1.4. Todos os documentos apresentados poderão ser alvo de diligência por parte da CONTRATANTE, sendo desclassificado o licitante que apresentar documentação falsa ou incompleta, estando sujeito, ainda, às penalidades previstas em lei;

10.11.1.1.5. No caso de atestados emitidos por empresa da iniciativa privada, não serão considerados aqueles emitidos por empresas pertencentes ao mesmo grupo empresarial da empresa proponente. Serão considerados como pertencentes ao mesmo grupo empresarial da empresa proponente, empresas controladas ou controladoras da empresa proponente, ou que tenha pelo menos uma mesma pessoa física ou jurídica que seja sócio da empresa emitente e da empresa proponente.

10.11.1.1.6. As competências exigidas correspondem às quantidades relevantes dos itens mais críticos para assegurar que a LICITANTE tenha efetiva capacidade de prestar os serviços considerando a complexidade da infraestrutura de TI da CONTRATANTE.

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

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

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

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

10.11.6. As empresas, cadastradas ou não no SICAF, deverão apresentar atestado de vistoria assinado pelo servidor responsável, nos termos do item 12.3.7 do Termo de Referência.

10.11.6.1. O atestado de vistoria poderá ser substituído por declaração emitida pelo licitante em que conste, alternativamente, ou que conhece as condições locais para execução do objeto; ou que tem pleno conhecimento das condições e peculiaridades inerentes à natureza do trabalho, assume total responsabilidade por este fato e não utilizará deste para quaisquer questionamentos futuros que ensejem desavenças técnicas ou financeiras com a contratante, nos termos do item 12.3.8 do Termo de Referência

10.12. 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.

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

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

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

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

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

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

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

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

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

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

11. DO ENCAMINHAMENTO DA PROPOSTA VENCEDORA

11.1. 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:

11.1.1. 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.

11.1.2. apresentar a proposta, devidamente ajustada ao lance vencedor;

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

11.2. 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.

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

11.3. 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).

11.3.1. 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.

11.4. 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.

11.5. 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.

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

12. DOS RECURSOS

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

12.2. 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.

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

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

12.2.3. 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.

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

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

13. DA REABERTURA DA SESSÃO PÚBLICA

13.1. A sessão pública poderá ser reaberta:

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

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

procedimentos imediatamente posteriores ao encerramento da etapa de lances.

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

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

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

14. DA ADJUDICAÇÃO E HOMOLOGAÇÃO

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

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

15. DA GARANTIA DE EXECUÇÃO

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

16. DA ATA DE REGISTRO DE PREÇOS

16.1. Homologado o resultado da licitação, terá o adjudicatário o prazo de 05 (cinco) dias úteis, contados a partir da data de sua convocação, para assinar a Ata de Registro de Preços, cujo prazo de validade encontra-se nela fixado, sob pena de decair do direito à contratação, sem prejuízo das sanções previstas neste Edital.

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

16.1.2. O prazo estabelecido no subitem anterior para assinatura da Ata de Registro de Preços poderá ser prorrogado uma única vez, por igual período, quando solicitado pelo(s) licitante(s) vencedor(s), durante o seu transcurso, e desde que devidamente aceito.

16.2. Serão formalizadas tantas Atas de Registro de Preços quanto necessárias para o registro de todos os itens constantes no Termo de Referência, com a indicação do licitante vencedor, a descrição do(s) item(ns), as respectivas quantidades, preços registrados e demais condições.

16.2.1. Será incluído na ata, sob a forma de anexo, o registro dos licitantes que aceitarem cotar os bens ou serviços com preços iguais aos do licitante vencedor na sequência da classificação do certame, excluído o percentual referente à margem de preferência, quando o objeto não atender aos requisitos previstos no art. 3º da Lei nº 8.666, de 1993.

17. DO TERMO DE CONTRATO

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

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

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

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

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

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

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

17.3.3. 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.

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

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

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

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

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

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

18. DO REAJUSTAMENTO EM SENTIDO GERAL

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

19. DO RECEBIMENTO DO OBJETO E DA FISCALIZAÇÃO

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

20. DAS OBRIGAÇÕES DA CONTRATANTE E DA CONTRATADA

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

21. DO PAGAMENTO

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

22. DAS SANÇÕES ADMINISTRATIVAS.

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

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

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

22.1.3. apresentar documentação falsa;

22.1.4. deixar de entregar os documentos exigidos no certame;

22.1.5. ensejar o retardamento da execução do objeto;

22.1.6. não mantiver a proposta;

22.1.7. cometer fraude fiscal;

22.1.8. comportar-se de modo inidôneo;

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

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

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

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

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

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

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

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

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

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

22.6. Se, durante o processo de aplicação de penalidade, houver indícios de prática de infração administrativa tipificada pela Lei nº 12.846, de 1º de agosto de 2013, como ato lesivo à administração pública nacional ou estrangeira, cópias do processo administrativo necessárias à apuração da responsabilidade da empresa deverão ser remetidas à autoridade competente, com

despacho fundamentado, para ciência e decisão sobre a eventual instauração de investigação preliminar ou Processo Administrativo de Responsabilização – PAR.

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

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

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

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

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

22.12. As penalidades serão obrigatoriamente registradas no SICAF.

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

23. DA FORMAÇÃO DO CADASTRO DE RESERVA

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

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

23.3. Havendo um ou mais licitantes que aceitem cotar suas propostas em valor igual ao do licitante vencedor, estes serão classificados segundo a ordem da última proposta individual apresentada durante a fase competitiva.

23.4. Esta ordem de classificação dos licitantes registrados deverá ser respeitada nas contratações e somente será utilizada acaso o melhor colocado no certame não assine a ata ou tenha seu registro cancelado nas hipóteses previstas nos artigos 20 e 21 do Decreto nº 7.892/213.

24. DA IMPUGNAÇÃO AO EDITAL E DO PEDIDO DE ESCLARECIMENTO

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

24.2. A impugnação poderá ser realizada por forma eletrônica, pelo e-mail licitacao@mj.gov.br, ou por petição dirigida ou protocolada no endereço à Coordenação de Procedimentos Licitatórios/COPLI – MJ, situada à Esplanada dos Ministérios, Bloco “T”, Anexo II, sala 621, em Brasília – DF, CEP 70064-900.

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

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

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

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

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

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

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

25. DAS DISPOSIÇÕES GERAIS

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

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

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

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

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

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

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

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

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

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

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

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

25.12.1. ANEXO I - Termo de Referência

25.12.1.1. ANEXO I - A - PROPOSTA DE PREÇOS

25.12.1.2. ANEXO I - B - MODELO DE ORDEM DE SERVIÇO – O.S.

25.12.1.3. ANEXO I - C - RELATÓRIO DE CHAMADO TÉCNICO – RCTA

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

25.12.1.5. ANEXO I - E - TERMO DE CIÊNCIA

25.12.1.6. ANEXO I - F - TERMO DE COMPROMISSO

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

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

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

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

25.12.1.11. ANEXO I - K - PLANILHA DE AVALIAÇÃO DE TREINAMENTO

25.12.1.12. ANEXO I - L - ESTUDO TÉCNICO PRELIMINAR DA CONTRATAÇÃO

25.12.1.13. ANEXO I - M - PORTARIA MJSP Nº 513, DE 15 DE SETEMBRO DE 2020

25.12.2. ANEXO II – Valores Máximos Admissíveis

25.12.3. ANEXO III - Minuta da Ata de Registro de Preços

25.12.4. ANEXO IV – Minuta de Termo de Contrato

25.12.5. ANEXO V - Declaração de ciência sobre a implantação do Programa de Integridade

ALEXANDRA LACERDA FERREIRA RIOS

PREGOEIRA

Documento assinado eletronicamente por **ALEXANDRA LACERDA FERREIRA RIOS**, **Pregoeiro(a)**, em 16/09/2021, às 13:42, com fundamento no § 3º do art. 4º do Decreto nº 10.543, de 13 de novembro de 2020.

A autenticidade do documento pode ser conferida no site http://sei.autentica.mj.gov.br informando o código verificador **15815064** e o código CRC **F3B895D3**
O trâmite deste documento pode ser acompanhado pelo site http://www.justica.gov.br/acesso-a-sistemas/protocolo e tem validade de prova de registro de protocolo no Ministério da Justiça e Segurança Pública.

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

ANEXO I DO EDITAL

TERMO DE REFERÊNCIA

INTRODUÇÃO

Este documento constitui peça integrante e inseparável do respectivo procedimento licitatório e têm por objetivo definir, de forma expressa, as especificações, os prazos de execução, as quantidades, as justificativas, os procedimentos de execução, o recebimento e o pagamento do objeto, dentre outros, de forma a subsidiar os interessados na participação do certame licitatório influenciando-os na preparação e na elaboração de suas propostas.

1. OBJETO DA CONTRATAÇÃO

1.1. Contratação de empresa especializada, mediante Sistema de Registro de Preços, para prestação de serviços de implementação de solução para avaliação de vulnerabilidades em ativos de tecnologia da informação e aplicações web ao Ministério da Justiça e Segura Pública, compreendendo: a subscrição de licenças de software, abarcando a atualização, o treinamento e o suporte técnico (24x7); e o serviço técnico especializado, conforme as especificações e demais condições de execução contidas no presente Termo de Referência e seus anexos.

2. DESCRIÇÃO DA SOLUÇÃO DE TIC

2.1. A descrição da solução de TIC encontra-se devidamente registrada no Estudo Técnico Preliminar (14442241) item 12 e o detalhamento quanto ao quantitativo de bens e serviços da solução encontram-se no dos itens 4.1 a 4.34.

2.2. As tabelas 1 e 2 apresentam de forma resumida o ambiente de Tecnologia da Informação e Comunicação (TIC) do Ministério da Justiça e Segurança Pública.

Tabela 1 - Resumo do Parque de Ativos de TI

Categoria	Total
Appliance de Segurança	14
Ativos de Rede	274
Host Físico no Datacenter	84
Sistemas Operacionais de Servidores	917
Armazenamento	21
Estação de Trabalho	4.334
Servidor de Aplicação	187
Sistemas Web	58
Serviços de rede	4
Total	**5.893**

Tabela 2 - Domínios e IP's

Nome	Domínios	Tipo de Domínio
consumidor.gov.br	consumidor.gov.br	Authoritative
defesadoconsumidor.gov.br	defesadoconsumidor.gov.br	Authoritative
infoseg.gov.br	infoseg.gov.br	Authoritative
justica.gov.br	justica.gov.br	Authoritative
justicagovbr.mail.onmicrosoft.com	justicagovbr.mail.onmicrosoft.com	Authoritative
migrantes.gov.br	migrantes.gov.br	Authoritative
mj.gov.br (default domain)	mj.gov.br	Authoritative
seguranca.gov.br	seguranca.gov.br	Authoritative
TOTAL DE DOMÍNIOS		**8**
TOTAL DE IP's		**6.702**

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

2.3.1. A tabela 03 apresenta a descrição dos itens a serem contratados (bens e serviços que compõem a solução), detalhados neste Termo de Referência:

Tabela 3 - Quantitativos a serem registrados

Grupo	Item	Código SIASG CATSER	DESCRIÇÃO	Quantidade			Unidade de Medida
				MJSP Órgão Gerenciador	CADE Órgão Partícipe	TOTAL	

1	1	27502	Licenciamento de plataforma de avaliação de vulnerabilidades e auditoria de configurações de ativos de rede, contemplando no mínimo 1.000 endereços IP, por ano de uso, com suporte técnico (24x7), treinamento e atualização upgrade/update, por 24 (vinte e quatro) meses	09	03	12	Licença
	2	27340	Serviço Técnico Especializado para avaliação de vulnerabilidades	960	960	1.920	Horas
2	3	27502	Licenciamento para solução de análise de segurança em aplicações Web, pacote para 8 (oito) domínios (FQDN), por ano de uso, com suporte técnico (24x7), treinamento e atualização upgrade/update, por 24 (vinte e quatro) meses	01	01	02	Licença
	4	27340	Serviço Técnico Especializado para avaliação de vulnerabilidades	960	960	1.920	Horas

2.4. **Da classificação dos serviços**

2.4.1. O objeto caracteriza-se como "serviço comum", atendendo aos padrões abertos da indústria, sendo compatível no mercado com qualidade e preços, uma vez que seus padrões de desempenho e qualidade ensejam definições objetivas de produtos e serviços de tecnologia da informação e comunicação, com base nas especificações usuais de mercado, e tem como objetivo ser enquadrado na modalidade licitatória denominada Pregão, conforme o art. 1º da Lei nº 10.520/2002.

2.4.2. Registre-se que existem diversos fornecedores capazes de executar o objeto proposto no Termo de Referência, motivo que assegura ao Ministério da Justiça e Segurança Pública o emprego da modalidade licitatória do pregão.

2.4.3. Assim, entende-se, que deverá ser processada a modalidade licitatória de pregão eletrônico do tipo menor preço, com vistas a obter a melhor proposta para a Administração Pública.

2.4.4. Os serviços a serem contratados enquadram-se nos pressupostos da Portaria nº 443, de 27 de dezembro de 2018 que estabelece os serviços que serão preferencialmente objeto de execução indireta, em atendimento ao disposto no art. 2º do Decreto nº 9.507, de 21 de setembro de 2018, constituindo-se em serviços de tecnologia da informação.

2.4.5. A prestação dos serviços não gera vínculo empregatício entre os empregados da Contratada e a Administração, vedando-se qualquer relação entre estes que caracterize pessoalidade e subordinação direta.

3. JUSTIFICATIVA E OBJETIVO DA CONTRATAÇÃO

3.1. **Contextualização e Justificativa para contratação**

3.1.1. O Ministério da Justiça e Segurança Pública possui um ambiente de Tecnologia da Informação e Comunicação (TIC) diversificado com vários recursos tecnológicos, sistemas legados e um grande número de usuários desses recursos.

3.1.2. Nesse cenário cresce a preocupação relacionada aos problemas com a segurança digital e o monitoramento das vulnerabilidades de segurança no ambiente computacional é absolutamente necessário para se manter a confidencialidade, a disponibilidade e a integridade das informações.

3.1.3. Desse modo, busca-se implementar uma solução de software capaz de testar os ativos de TI e as aplicações web periodicamente em busca de quaisquer vulnerabilidades, sejam elas relativas a atualização de sistemas operacionais e servidores de aplicação, configurações de serviços ou outras falhas técnicas. Além disso, é preciso que a solução forneça relatórios para que seja possível o acompanhamento do trabalho de identificação e mitigação de riscos.

3.1.4. A presente contratação visa suprir o Ministério da Justiça e Segurança Pública com o aparato tecnológico necessário para o efetivo cumprimento da sua missão de trabalhar para a consolidação do Estado Democrático de Direito e de sua visão em ser reconhecido pela sociedade como protagonista na defesa da cidadania, na proteção de direitos, na integração da política de segurança pública, na cooperação jurídica internacional e no combate à corrupção, ao crime organizado e ao crime violento.

3.1.5. Nesse sentido, o fortalecimento e ampliação da estrutura e dos serviços de tecnologia da informação e comunicação contribuem, invariavelmente, para o aumento de desempenho dos servidores que atuam diretamente nas áreas finalísticas. Desta forma, a presente contratação busca atender as necessidades de segurança da informação das áreas de negócio do Ministério da Justiça e Segurança Pública.

3.1.6. Na sociedade contemporânea, ao mesmo tempo em que as informações são consideradas os principais ativos de uma organização, as mesmas estão também sob o constante risco. Por isso, sua perda ou cópia constitui um enorme prejuízo para as organizações. Principalmente, para um órgão como o Ministério da Justiça e Segurança Pública que atua, dentre outras, em áreas que envolvem Segurança Pública, combate à corrupção e lavagem de dinheiro, proteção e defesa do consumidor, repressão ao tráfico ilícito de drogas, operações policiais e atividades de inteligência, a ocorrência de eventos de segurança de informação que atacam a confidencialidade, autenticidade e disponibilidade deve ser impedida.

3.1.7. A adoção de um processo de gestão de vulnerabilidades com o objetivo de reduzir drasticamente problemas, como malwares, contas inativas, senhas ruins ou sistemas desatualizados, bem como a mitigação de riscos e a proteção de dados, é o que se espera com a utilização de uma ferramenta como a solução a ser contratada.

3.1.8. Tem-se a clareza de que um processo de gestão de vulnerabilidades é muito maior e mais complexo que apenas a execução de uma ferramenta e que de forma básica todo processo de gestão de vulnerabilidades deve apresentar no mínimos as etapas de identificação de vulnerabilidades; verificação da vulnerabilidade; priorização das vulnerabilidades; mitigação de vulnerabilidades e remediação de vulnerabilidades. A proposta deve contemplar não apenas o serviço avaliação de vulnerabilidade, mas também uma tecnologia de priorização

das vulnerabilidades. Estes são itens chave na maioria das soluções disponíveis no mercado e que possuem alto valor agregado.

3.1.9. Ressalta-se que a contratação está alinhada com as boas práticas e aos normativos e padrões de segurança da informação, como por exemplo, a norma ABNT NBR ISO/IEC 27002 que fornece diretrizes para práticas de gestão de segurança da informação e normas de segurança da informação para as organizações, incluindo a seleção, a implementação e o gerenciamento de controles, levando em consideração os ambientes de risco da segurança da informação da organização.

3.1.10. A gestão de vulnerabilidades técnicas, a qual tem por objetivo prevenir a exploração de vulnerabilidades técnicas, é um dos controles comumente aceitos e necessário dentro do processo de implementação de um sistema de gestão da segurança da informação baseado na ABNT NBR ISO/IEC 27001, descrita no controle 12.6.1

3.1.11. A contratação está alinhada, também, a Lei Geral de Proteção de Dados Pessoais (LGPD), a qual no Capítulo VII que trata da segurança e das boas práticas, dispõe no artigo 46 que os agentes de tratamento devem adotar medidas de segurança, técnicas e administrativas aptas a proteger os dados pessoais de acessos não autorizados e de situações acidentais ou ilícitas de destruição, perda, alteração, comunicação ou qualquer forma de tratamento inadequado ou ilícito.

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

3.2.1. Destaca-se que esta contratação está prevista no Plano Diretor de Tecnologia da Informação e Comunicação – PDTIC do MJSP 2021-2023, página 59, (Doc. Sei nº 13743301)

3.3. **Estimativa da demanda**

3.3.1. Foram realizados estudos acerca da necessidade de licenciamento relativa a subscrição de ferramenta de gestão de vulnerabilidades no âmbito do Ministério da Justiça e Segurança Pública e do CADE. Os itens e os respectivos quantitativos referem-se às necessidades do MJSP e do CADE, conforme apresentado na tabela 4.

Tabela 4 - Estimativa de itens para atender às necessidades do MJSP e do CADE

Grupo	Item	Código SIASG CATSER	DESCRIÇÃO	Quantidade			Unidade de Medida	Valor Unitário Máximo aceitável (R$)
				MJSP	CADE	TOTAL		
1	1	27502	Licenciamento de plataforma de avaliação de vulnerabilidades e auditoria de configurações de ativos de rede, contemplando no mínimo 1.000 endereços IP, por ano de uso, com suporte técnico (24x7), treinamento e atualização upgrade/update, por 24 (vinte e quatro) meses	09	03	12	Licença	R$ 537.462,56
	2	27340	Serviço Técnico Especializado para avaliação de vulnerabilidades	960	960	1.920	Horas	R$ 556,80
2	3	27502	Licenciamento para solução de análise de segurança em aplicações Web, pacote para 8 (oito) domínios (FQDN), por ano de uso, com suporte técnico (24x7), treinamento e atualização upgrade/update, por 24 (vinte e quatro) meses	01	01	02	Licença	R$ 435.166,67
	4	27340	Serviço Técnico Especializado para avaliação de vulnerabilidades	960	960	1.920	Horas	R$ 482,38

3.3.2. A estimativa da demanda está detalhada no item Estimativa da Demanda - Quantidade de Bens e Serviços do Estudo Técnico Preliminar (14442241).

3.4. **Parcelamento da Solução de TIC**

3.4.1. A solução é composta por diversos itens que, por suas características técnicas, podem ser divididos em parcelas. Uma vez que as ferramentas têm escopos de atuação bem distintos. Enquanto uma atua na camada de rede, aplicando sua inteligência e algoritmo para detectar vulnerabilidades em ativos na infraestrutura, a outra ferramenta atua na camada de aplicação, buscando brechas, erros e vulnerabilidades que podem propiciar uma invasão aos sistemas web, bancos de dados e demais aplicações, inclusive propiciando vazamento de dados e informações confidenciais.

3.4.2. Vantagens obtidas com a adoção da modalidade de contratação em grupos distintos:

3.4.2.1. Ampliação da competitividade com a possibilidade de participação de fornecedores líderes de mercado em suas respectivas áreas de atuação;

3.4.2.2. Orientação à equipe de desenvolvimento para as melhores práticas de desenvolvimento seguro.

3.4.2.3. Melhoria da qualidade e segurança das aplicações no ambiente tecnológico do Ministério, reduzindo sua exposição a ataques cibernéticos internos e externos.

3.4.2.4. Conformidade com regulações relacionadas à privacidade de dados.

3.4.2.5. Possibilidade de análise minuciosa da rede corporativa do MJSP, tanto na infraestrutura quanto nos sistemas e ferramentas de apoio, em busca de potenciais vulnerabilidades nos diversos serviços e estruturas, internas ou externas e que auxilia na extinção ou minimização dos riscos de eventuais vulnerabilidades.

3.4.2.6. Visualização global dos níveis de segurança em que se encontra a rede de comunicações de dados do MJSP e a tomada de ações imediatas para adequá-la a um nível

de segurança aceitável.

3.4.3. Desta forma, os itens 1 e 2 (grupo 1) e os itens 3 e 4 (grupo 2) devem ser contratados em grupos distintos.

3.5. **Resultados e Benefícios esperados com a contratação**

3.5.1. Maior controle de segurança da informação e proteção de dados no âmbito do Ministério da Justiça e Segurança Pública: através da redução de malwares, sistemas desatualizados, dentre outros problemas;

3.5.2. Diminuição dos esforços de correção e de testes de eficácia: as análises de vulnerabilidades de rede permitem não só a identificação de problemas de rede, mas também ajuda na sua priorização e no desenvolvimento de uma estratégia para lidar com aqueles mais críticos;

3.5.3. Melhoria na gestão de mudanças e no gerenciamento de patches: faz parte da avaliação de vulnerabilidades centralizar e gerar todos os feedbacks sobre os problemas, as suas correções e as próximas ações;

3.5.4. Fortalecimento da atuação da Equipe de Tratamento de Incidentes de Segurança nas Redes de computadores: A identificação e o tratamento das vulnerabilidades auxiliarão a ETIR na execução de suas responsabilidades de análise e respostas às notificações e atividades relacionadas a incidentes de segurança em redes de computadores além da redução desses incidentes;

3.5.5. Apoio nas auditorias de Segurança da Informação e Comunicações: a obtenção de relatórios detalhados permitirá a devida diligência durante as auditorias;

3.5.6. Atualização da Política de Segurança da Informação e Comunicações: A avaliação de vulnerabilidades possibilitará aplicar melhorias na segurança da informação e na revisão da POSIC e suas normas complementares.

3.5.7. Auxílio nos requisitos regulamentares: A identificação e o tratamento das vulnerabilidades contribuirá para que o Ministério mantenha-se em conformidade com:

3.5.7.1. os normativos emanados pelo Departamento de Segurança da Informação e Comunicações do Gabinete de Segurança Institucional da Presidência da República;

3.5.7.2. os princípios e controles de segurança definidos nos padrões ABNT NBR ISO/IEC 27001, 27002, 27005, 27011, 27014 e 27701;

3.5.7.3. a Lei Nº 13.709, de 14 de agosto de 2018, Lei Geral de Proteção de Dados Pessoais (LGPD);

3.5.7.4. os frameworks de processos de governança e boas práticas como o ITIL e COBIT.

3.6. **Justificativa para agrupamento e divisibilidade do Objeto**

3.6.1. Justifica-se a necessidade de agrupar os itens 1 e 2 no Grupo 1 e itens 3 e 4 no Grupo 2 uma vez que o Serviço Técnico Especializado refere-se ao suporte para a ferramenta objeto do licenciamento. Permitir que empresas estranhas ao fornecimento do licenciamento realizassem o suporte ou Serviço Técnico Especializado na ferramenta implantada por outra empresa poderia introduzir diversos riscos tendo em vista a necessidade de mais participantes externos ao MJSP com acesso ao ambiente, introduziria atrasos na solução dos problemas, uma vez que seria possível que uma empresa atribuísse erros ao desempenho das atividades da outra, assim como elevaria complexidade na gestão do contrato por parte dos servidores do MJSP. Considerando que esse agrupamento de itens tende a solucionar os problemas relatados, bem como reduzir o valor de contratação desses itens devido estar concentrado em uma única empresa optou-se pelo agrupamento.

3.6.2. De acordo com o art. 8º da Lei 8.666/1993, as contratações devem ser programadas no todo, coerente com o conceito de solução de TI conforme exposto no guia de boas práticas em contratação de soluções TI do TCU e na IN 01 de 2019 - SGD. Entretanto, de acordo com o § 1º do art. 23 da Lei 8.666/1993, como regra, as contratações devem ser divididas em tantas parcelas quanto possível, desde que seja técnica e economicamente viável. Em suma, deve-se planejar a solução como um todo, mas deve-se dividi-la em tantos objetos quanto possível para fins de contratação, de modo a ampliar a competitividade nas contratações.

3.7. **Justificativa para não participação de consórcios e cooperativas**

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

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

3.7.3. Desta forma, resta claro que a participação de consórcios em certames licitatórios somente se torna "obrigatória" quando o objeto a ser licitado pressuponha heterogeneidade de atividades empresariais, sendo que, sua não inclusão, resultaria em restrição da competitividade. Assim, a Administração Pública ao vedar a participação de consórcio procura manter a unidade do sistema, eis que o Termo de Referência, da forma como foi concebido demonstra a existência de uma unidade conceitual que perpassa todo o projeto. Tal integração de conceitos se verifica não só entre suas etapas, como também nos serviços previstos em cada etapa. Isto porque cada serviço solicitado representa uma preparação para que o serviço subsequente possa ser compreendido e elaborado. Vale dizer que somente a empresa que estiver envolvida e for responsável pela totalidade do objeto será conhecedora, de forma suficiente, de todas as

questões pertinentes, estando apta a apresentar os serviços de forma encadeada. A opção pela participação ou não de empresas em consórcios encontra-se na esfera da discricionariedade administrativa, a qual contempla o exame da conveniência e oportunidade do ato administrativo. Se o ato é vinculado, é porque o legislador pré-estabeleceu o que não ocorreu no caso presente. No caso em questão, a lei não estabelece disposição expressa exigindo a admissão de consórcios, mas deixa ao administrador a possibilidade de verificar as hipóteses em que este seria admissível, o que se depreende do art. 33, caput, da Lei nº. 8.666/93: "Quando permitida na licitação a participação de empresas em consórcio (...)".

3.8. **Justificativa para adoção do sistema de registro de preços**

3.8.1. O artigo 3º do Decreto nº 7.892, de 23 de janeiro de 2013, que regulamenta o SRP, estabelece as hipóteses em que a Administração Pública Federal pode utilizar o SRP:

> *Art. 3º O Sistema de Registro de Preços poderá ser adotado nas seguintes hipóteses:*
>
> *I - quando, pelas características do bem ou serviço, houver necessidade de contratações frequentes;*
> *II - quando for conveniente a aquisição de bens com previsão de entregas parceladas ou contratação de serviços remunerados por unidade de medida ou em regime de tarefa;*
> *III - quando for conveniente a aquisição de bens ou a contratação de serviços para atendimento a mais de um órgão ou entidade, ou a programas de governo; ou*
> *IV - quando, pela natureza do objeto, não for possível definir previamente o quantitativo a ser demandado pela Administração.*

3.8.2. No presente caso justifica-se a realização do procedimento licitatório no sistema de registro de preço, com fundamento no inciso III do artigo 3º do Decreto nº 7.892/2013, uma vez que o CADE manifestou interesse na participação da licitação, através do Documento SEI Nº 13754821.

3.8.3. Assim é que a utilização do SRP possibilitará um ganho de eficiência, a redução do esforço administrativo e processual na realização de diversos processos licitatórios, uma vez que a execução conjunta culmina em um único certame, haja vista que o objeto deste TR é de uso comum, além do ganho de escala e as possíveis reduções consideráveis dos preços ofertados por fornecedores, uma vez que ao concentrar expressivos volumes licitados, a Administração Pública Federal amplia as possibilidades de conseguir propostas mais vantajosas.

3.8.4. Além do mais, a Lei nº 8.666, de 1993 estabelece, em seu art. 15, que as compras, sempre que possível, deverão ser processadas através de sistema de registro de preços. Nesta mesma linha, o Decreto nº 7.892, de 2013, define no art. 3º que o Sistema de Registro de Preços poderá ser adotado na hipótese de conveniência da aquisição de bens ou a contratação de serviços para atendimento a mais de um órgão ou entidade.

3.8.5. O prazo de validade da ata de registro de preços será de 12 (doze) meses.

3.9. **Justificativa para aplicação da Norma Complementar nº 14/IN01/DSIC/GSIPR**

3.9.1. A Norma Complementar nº 14/IN01/DSIC/GSIPR estabelece princípios, diretrizes e responsabilidades relacionados à Segurança da Informação (SI) para o tratamento da informação em ambiente de Computação em Nuvem, nos órgãos e entidades da Administração Pública Federal (APF), direta e indireta.

3.9.2. Desta forma, caso a solução ofertada pelo fornecedor ou parte dela seja baseada em nuvem, deve estar de acordo com a Norma Complementar nº 14/IN01/DSIC/GSIPR.

4. ESPECIFICAÇÃO DOS REQUISITOS DA CONTRATAÇÃO

4.1. **Requisitos de Negócio**

4.1.1. Aumento da segurança da informação e comunicação no âmbito do Ministério da Justiça e Segurança Pública e o sigilo das informações do cidadão;

4.1.2. Avaliação de Vulnerabilidades em Sistemas Operacionais;

4.1.3. Avaliação de Vulnerabilidades em Sistemas e páginas WEB;

4.1.4. Detecção e Correção de falhas de softwares que possam acarretar riscos na segurança, na funcionalidade e no desempenho do sistema;

4.1.5. Implantação de mecanismos para realizar o bloqueio de ataques constantes;

4.1.6. Identificação de novas soluções de segurança e realização de suas alterações;

4.1.7. Foco na melhoria constante do sistema de segurança de dados corporativos;

4.1.8. Auxílio na implementação de políticas de segurança;

4.1.9. Agilidade na identificação de falhas.

4.2. **Requisitos de Capacitação**

4.2.1. Para os itens 2 e 4 não se aplicam os requisitos de capacitação, uma vez que se referem à contratação de serviço técnico especializado.

4.2.2. Para os Itens 1 e 3, a(s) Contratada(s) deverá(ão) fornecer treinamento por profissional certificado pelo fabricante, os requisitos de capacitação que se aplicam são:

4.2.2.1. A contratada deverá ministrar treinamento, na língua portuguesa, para até 15 (quinze) servidores indicados pelo órgão, com carga horária mínima de 20 horas.

4.2.2.2. O treinamento deverá ser ministrado por profissional com certificação oficial do fabricante.

4.2.2.3. O conteúdo do treinamento a ser ministrado deverá contemplar os seguintes itens:

a) Procedimentos de instalação física e lógica;

b) Todos os procedimentos necessários à configuração técnica;

c) Todos os procedimentos necessários à completa operação do produto; e

d) Todos os procedimentos de manutenção do produto que devem ser realizados pelos técnicos do órgão.

4.2.2.4. O treinamento deverá ser realizado nas dependências do órgão ou virtualmente a critério da CONTRATANTE.

4.2.2.5. O treinamento poderá ser ministrado em até 30 dias após a entrega das licenças de software.

4.2.2.6. O treinamento poderá ser ministrado no horário de 08:00 às 12:00 ou de 14:00 as 18:00, em dias úteis, a critério da contratante;

4.2.2.7. A critério da CONTRATANTE o treinamento poderá ser dividido em duas turmas de até 8 servidores.

4.2.3. Para os itens 2 e 4 : Os profissionais da CONTRATANTE que atuam co m o serviço técnico especializado devem ser certificados pela fabricante.

4.3. **Requisitos Legais**

4.3.1. A CONTRATADA deverá observar também os seguintes ordenamentos jurídicos:

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

4.3.3. Decreto nº 9.507/2018: Dispõe sobre a execução indireta, mediante contratação, de serviços da administração pública federal direta, autárquica e fundacional e das empresas públicas e das sociedades de economia mista controladas pela União;

4.3.4. Decreto nº 10.183/2019: Altera o Decreto nº 9.507, de 21 de setembro de 2018, que dispõe sobre a execução indireta, mediante contratação, de serviços da administração pública federal direta, autárquica e fundacional e das empresas públicas e das sociedades de economia mista controladas pela União.

4.3.5. Lei nº 8.666/1993: Regulamenta o art. 37, inciso XXI, da Constituição Federal, institui normas para licitações e contratos da Administração Pública e dá outras providências.

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

4.3.7. Decreto nº 10.024/2019, de 20 de setembro de 2019: Regulamenta o pregão, na forma eletrônica, para aquisição de bens e serviços comuns, e dá outras providências.

4.3.8. Decreto nº 3.555/2000: Aprova o Regulamento para a modalidade de licitação denominada pregão, para aquisição de bens e serviços comuns.

4.3.9. 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.

4.3.10. Decreto nº 7.892/2013: Referente ao Sistema de Registro de Preços.

4.3.11. Decreto nº 9.488/2018: Altera o Decreto nº 7.892/2013.

4.3.12. Portaria nº 443/2018: Estabelece os serviços que serão preferencialmente objeto de execução indireta, em atendimento ao disposto no art. 2º do Decreto nº 9.507, de 21 de setembro de 2018.

4.3.13. Portaria nº 513/2020 MJSP: Dispõe sobre a implantação de Programa de Integridade em empresas contratadas pelo Ministério da Justiça e Segurança Pública.

4.3.14. Instrução Normativa nº 5/2017- MP: Dispõe sobre as regras e diretrizes do procedimento de contratação de serviços sob o regime de execução indireta no âmbito da Administração Pública federal direta, autárquica e fundacional.

4.3.15. Instrução Normativa nº 7/2018: Altera a Instrução Normativa nº 5, de 26 de maio de 2017, que dispõe sobre as regras e diretrizes do procedimento de contratação de serviços sob o regime de execução indireta no âmbito da Administração Pública federal direta, autárquica e fundacional.

4.3.16. Instrução Normativa SLTI/MP 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.

4.3.17. Instrução Normativa Nº 73 de 5 de agosto de 2020, que dispõe sobre os procedimentos administrativos básicos para a realização de pesquisa de preços para aquisição de bens e contratação de serviços em geral.

4.3.18. Instrução Normativa SLTI/MP nº 01/2010: Dispõe sobre os critérios de sustentabilidade ambiental na aquisição de bens, contratação de serviços ou obras pela Administração Pública Federal direta, autárquica e fundacional e dá outras providências.

4.3.19. Norma Complementar nº 14/IN01/DSIC/GSIPR: Dispõe sobre princípios, diretrizes e responsabilidades relacionados à segurança da informação para o tratamento da informação em ambiente de computação em nuvem.

4.3.20. Orientações Gerais para a contratação de serviços terceirizados na área de tecnologia da informação da AGU, Memorando-circular n. 00006/2018/CONJUR-MJ/CGU/AGU (00734.002278/2018-74).

4.4. **Requisitos de Manutenção**

4.4.1. **Características Gerais**

4.4.1.1. Para a execução do suporte técnico, durante todo o período de vigência do Contrato a empresa a ser contratada deverá fornecer uma Central de Atendimento (sítio na Internet, e-mail), sem custo adicional à CONTRATANTE para consultas, aberturas de chamados técnicos e envio de arquivos para análise, durante 24 (vinte e quatro) horas por dia, 7 (sete) dias por semana, 365 (trezentos e sessenta e cinco) dias por ano, obrigatoriamente em Português Brasileiro.

4.4.1.2. Não há limitação para o número de chamados técnicos.

4.4.1.3. Forma de atendimento: remoto ou presencial. No caso de atendimento remoto, a CONTRATADA deve informar por e-mail ao fiscal técnico do Contrato, assim que o atendimento for iniciado, e após sua conclusão, contendo evidências das atividades executadas. Caso haja necessidade de intervenção local, esta poderá ser executada.

4.4.1.4. A lista a seguir não é exaustiva, mas contém os principais serviços de

manutenção, atualização de versão e suporte técnico, a serem executados durante a vigência contratual:

4.4.1.4.1. Correções de problemas e anomalias (bugs) nos softwares, atualizações de versões e releases;

4.4.1.4.2. Solução de dúvidas e acompanhamento para a operação, configuração, upgrade e instalação das ferramentas disponibilizadas para gestão do ambiente;

4.4.1.4.3. Garantir que novas versões de firmware ou atualizações dos produtos sob contrato de manutenção tenham a perfeita compatibilidade com o ambiente operacional em uso nas instalações computacionais do Ministério da Justiça e Segurança Pública.

4.4.1.5. Deverão ser fornecidas automaticamente todas as atualizações de versão que ocorrerem durante a vigência contratual. Entende-se como "atualização" o provimento de toda e qualquer evolução de software, incluindo correções, "patches", "fixes", "updates", "service packs", novas "releases", "versions", "builds", "upgrades", englobando inclusive versões não sucessivas, nos casos em que a liberação de tais versões ocorra durante o período de garantia especificado.

4.4.1.6. A FABRICANTE/CONTRATADA deverá garantir a atualização dos microcódigos, firmwares, drivers e softwares instalados, provendo o fornecimento de novas versões por necessidade de correção de problemas ou por implementação de novos releases, a partir do recebimento definitivo pelo Ministério da Justiça e Segurança Pública, durante o período de garantia.

4.4.1.7. Caso seja necessário substituir licenças equivalentes durante a vigência do Contrato, isso deverá ocorrer sem qualquer ônus para o Ministério da Justiça e Segurança Pública.

4.4.1.8. Os serviços deverão contemplar a resolução de qualquer problema nas licenças e serviços descritos neste documento, sem nenhum ônus adicional para o Ministério da Justiça e Segurança Pública.

4.4.1.9. O Ministério da Justiça e Segurança Pública somente autorizará que a CONTRATADA faça inventários nos equipamentos/serviços/softwares quando solicitado formalmente.

4.5. **Requisitos Temporais**

4.5.1. A reunião inicial de alinhamento deverá ocorrer após a assinatura do Contrato e ser executada em, no máximo, 5 (cinco) dias úteis após a assinatura do Contrato.

4.5.2. O prazo de disponibilização dos documentos que comprovem o fornecimento do licenciamento e todas as demais obrigações da CONTRATADA será de no máximo 15 (quinze) dias corridos a partir da abertura da Ordem de Fornecimento de Serviço.

4.5.3. Para os itens 1 e 3 a CONTRATADA deverá atender aos Chamados Técnicos de acordo com o item Níveis Mínimos de Serviços Exigidos neste Termo de Referência.

4.5.4. Para os itens 2 e 4 a CONTRATADA deverá atender às ordens de serviço emitidas, de acordo com o item Níveis Mínimos de Serviços Exigidos neste Termo de Referência.

4.5.5. Para os itens 2 e 4 a prestação de serviços ocorrerá nas dependências da CONTRATANTE, de acordo com as necessidades elencadas, preferencialmente nos dias úteis (de segunda a sexta-feira), no horário de 08hs às 18hs.

4.6. **Requisitos de Segurança**

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

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

4.6.3. Demais requisitos de segurança são abordados no item requisitos de segurança da informação.

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

4.7.1. A CONTRATADA deverá adotar práticas de sustentabilidade ambiental na execução do objeto, quando couber, conforme disposto na Instrução Normativa SLTI/MP nº 01/2010, de 19 de janeiro de 2010.

4.7.2. Os serviços prestados pela CONTRATADA deverão pautar-se sempre no uso racional de recursos e equipamentos, de forma a evitar e prevenir o desperdício de insumos e materiais consumidos bem como a geração excessiva de resíduos, a fim de atender às diretrizes de responsabilidade ambiental adotadas pela CONTRATANTE.

4.7.3. Sem prejuízo aos demais critérios de sustentabilidade aplicados a CONTRATADA, deverá ainda ser observados os critérios estabelecidos na legislação ambiental.

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

4.8. **Requisitos de Arquitetura Tecnológica**

4.8.1. **Características Gerais - Item 1**

4.8.1.1. A Contratada deverá efetuar a instalação e as configurações iniciais, em conjunto com a Contratante, para uso da solução proposta, incluindo criação de scans, relatórios, filtros, permissões de usuários e demais funcionalidades da solução.

4.8.1.2. A instalação e configuração da solução deverá ocorrer de acordo com as melhores práticas com a inclusão mínima dos seguintes entregáveis:

4.8.1.2.1. Planejamento e desenho da instalação e configuração;

4.8.1.2.2. Criação de políticas de scan;

4.8.1.2.3. Configuração de dashboards, queries e alertas iniciais;

4.8.1.2.4. Entrega de documentação com as principais informações do ambiente e futuras recomendações;

4.8.1.2.5. Instalação de scanners e agentes on-premises, quando aplicável.

4.8.1.3. A solução deve ser capaz de realizar varreduras (scans) de vulnerabilidades, avaliação de configuração e conformidade (baseline e compliance), indícios e padrões de códigos maliciosos conhecidos (malwares).

4.8.1.4. A solução deve ser capaz de realizar avaliação da configuração segura dos servidores no data center para garantir que eles estejam configurados com segurança.

4.8.1.5. A solução deve possuir recurso de varredura ativa, onde o scanner comunica-se com os alvos (ativos) por meio da rede.

4.8.1.6. A solução de avaliação de vulnerabilidades deve suportar varreduras de dispositivos de IoT.

4.8.1.7. Deve ser capaz de identificar no mínimo 50.000 CVEs (Common Vulnerabilities and Exposures).

4.8.1.8. A solução deve ter a capacidade de adicionar etiquetas (tags) aos ativos de maneira automática, manual e possibilitar o uso de regras com parâmetros específicos para aplicação das mesmas.

4.8.1.9. Deve atribuir a todas as vulnerabilidades uma severidade baseada no CVSSv3 score.

4.8.1.10. A solução deve fornecer criptografia de ponta a ponta dos dados de vulnerabilidades.

4.8.1.11. A solução deve possuir a capacidade de armazenar informações dos ativos descobertos no ambiente.

4.8.1.12. Deve possuir um sistema de busca de informações de um determinado ativo com no mínimos as seguintes características:

4.8.1.13. Por sistema operacional;

a) Por um determinado software instalado;

b) Por Ativos impactados por uma determinada vulnerabilidade;

c) Por tipo de ativo.

d) Lista de todos os sistemas operacionais encontrados ;

e) Lista de Web Servers;

f) Lista de Web Clients;

4.8.1.14. A solução deve possuir suporte para a adição de detecções personalizadas usando o OVAL (Open Vulnerability Assessment Language).

4.8.1.15. A solução deve fornecer gerenciamento de fluxo de trabalho de correção com base em políticas, incluindo a criação e atribuição automática de registro de problema.

4.8.1.16. Deve permitir aceitar o risco de uma determinada vulnerabilidade encontrada no ambiente.

4.8.1.17. Possibilitar alterar a criticidade de determinada vulnerabilidade de forma manual.

4.8.1.18. A solução deve possuir um sistema de pontuação e priorização das vulnerabilidades.

4.8.1.19. A solução deve ser capaz de aplicar algoritmos de aprendizagem de máquina (machine learning) para analisar as características relacionadas a vulnerabilidades.

4.8.1.20. O sistema de pontuação e priorização de vulnerabilidades deve avaliar no mínimo as seguintes características:

a) CVSSv3 Impact Score;

b) Idade da Vulnerabilidade;

c) Se existe ameaça ou exploit que explore a vulnerabilidade;

d) Número de produtos afetados pela vulnerabilidade;

4.8.1.21. Deve ser capaz de fazer a correlação de ameaças em tempo real ou por meio da console central contra vulnerabilidades encontradas, incluindo feeds de inteligência de ameaças ao vivo.

4.8.1.22. Deve possuir uma API para automação de processos e integração com aplicações terceiras permitindo a extração de dados para carga no SIEM e com aplicações ITSM para as vulnerabilidades encontradas, permitindo o agrupamento no chamado por ações corretivas.

4.8.1.23. A solução deve permitir a instalação de agentes, quando aplicável, em estações de trabalho e servidores para varredura diretamente no sistema operacional.

4.8.1.24. A solução deve suportar conectores para, no mínimo, as seguintes plataformas:

a) Amazon Web Service (AWS);

b) Microsoft Azure;

c) Google Cloud Platform; e

d) Oracle Cloud.

4.8.1.25. Na inexistência do conector previsto no item 4.8.1.24, a solução deverá fornecer ou permitir a varredura por meio da utilização de APIs, instalação de agentes ou varredura ativa, sem impacto nos custos para o MJSP.

4.8.1.26. Os conectores devem ser fornecidos pela contratada, quando necessário, sem custos adicionais.

4.8.1.27. A solução deve ser capaz de produzir relatórios, no mínimo, nos seguintes formatos: PDF ou CSV ou HTML.

4.8.1.28. A solução deve possuir recurso de monitoria passiva do tráfego de rede ou através de varreduras agendadas periodicamente para identificação de anomalias, novos dispositivos e

desvios de padrões observados.

4.8.1.29. A solução deve ser licenciada para o uso ilimitado de sensores passivos de rede para realizar o monitoramento em tempo real.

4.8.1.30. A solução deve ser licenciada para realizar scans de conformidade e compliance de forma ilimitada;

4.8.1.31. A solução deve fornecer dashboards visuais, contendo as verificações e controles de segurança verificados com indicação de sucesso ou falha compatíveis, no mínimo, com os frameworks de segurança abaixo:

a) Família ISO 27.000;

b) NIST Cybersecurity Framework;

c) CIS Benchmarks;

d) NIST SP 800-53

4.8.1.32. Execução de verificação completa do sistema (rede), adequada para qualquer host;

4.8.1.33. A solução deve possuir sensores, no mínimo, com as seguintes funcionalidades:

a) Execução de verificação completa do sistema (rede), adequada para qualquer host;

b) verificação sem recomendações da rede, para que se possa personalizar totalmente as configurações da verificação;

c) Autenticação de hosts e enumeração de atualizações ausentes;

d) Execução de varredura simples para descobrir hosts ativos e portas abertas;

e) Avaliação de dispositivos móveis;

f) Auditoria de configuração de serviços em nuvem de terceiros;

g) Auditoria de configuração dos gerenciadores de dispositivos móveis;

h) Auditoria de configuração dos dispositivos de rede;

i) Detecção de desvio de segurança Intel AMT;

j) Verificação de malware nos sistemas Windows e Linux;

4.8.1.34. Deve ser possível determinar em tempo real quais portas de serviços (UDP/TCP) estão abertas em determinado ativo.

4.8.1.35. A solução deve ser capaz de realizar em tempo real ou através de varreduras agendadas periodicamente para descoberta de novos ativos para no mínimo:

4.8.1.35.1. Bancos de dados;

4.8.1.35.2. Hypervisors (no mínimo VMWare ESX/ESXi e Hyper-V);

4.8.1.35.3. Dispositivos móveis;

4.8.1.35.4. Dispositivos de rede;

4.8.1.35.5. Endpoints; e

4.8.1.35.6. Aplicações.

4.8.1.36. Deve realizar em tempo real a identificação de informações sensíveis no tráfego de rede do ambiente.

4.8.1.37. Permitir identificar vulnerabilidades associadas a servidores SQL no tráfego de rede em tempo real ou através de varreduras agendadas periodicamente.

4.8.1.38. A solução deve possuir interface para integração com as principais soluções de SIEM de mercado, tais como Microsoft Azure Sentinel, IBM QRadar, Microfocus ArcSight e Splunk.

4.8.1.39. A solução pode ser baseada em nuvem pública com scanners próprios localizados em nuvem pública e scanners instalados na infraestrutura do cliente (on-premises).

4.8.1.40. A solução deve possibilitar a realização de cópias de segurança, funcionamento em alta disponibilidade e criptografia de todos os dados armazenados, além de incluir todo o software e licenciamento necessários para o funcionamento completo de acordo com as funcionalidades previstas neste Termo de Referência.

4.8.1.41. A atualização das ameaças deve ocorrer diariamente e sem interrupção dos serviços.

4.8.1.42. A atualização da infraestrutura da solução (servidores, bancos de dados, aplicações, sistemas operacionais e configurações), bem como a indisponibilidade da solução não devem provocar tempo de parada (downtime) superior a 7,3 (sete vírgula três) horas por mês.

4.8.1.43. Configuração de segurança e acesso à gerência da solução:

a) Todos os dados armazenados nos servidores da solução devem ser criptografados e possuir logs de acesso;

b) A solução deve permitir a criação de, no mínimo, 20 contas para gerência e acesso aos relatórios, sem custo adicional.

4.8.1.44. Todas as licenças de uso de software devem ser registradas, na data da entrega, em nome da Contratante no site do fabricante.

4.8.1.45. A solução deve permitir mecanismo de varredura baseado em inferência com técnicas de varredura não intrusivas.

4.8.1.46. A solução proposta no **Item 01 do Grupo 01** deve ser de mesmo fabricante, permitindo soluções on-premise, em nuvem ou híbrida, sem adaptações ou alterações não efetuadas pelo fabricante, disponível para gerenciamento em console web, sendo toda infraestrutura de aplicações, bancos de dados de vulnerabilidades, dashboards, agentes e plugins também mantidas pelo mesmo fabricante, oferecidas como serviço padrão.

4.8.1.47. Se houver a necessidade, deverá ser fornecido o licenciamento dos bancos de dados corporativo e sistemas operacionais para a instalação e monitoração da solução.

4.8.1.48. O fornecedor assinará, no ato da entrega das licenças e do serviço, Termo de Compromisso (conforme Anexo I-F), em que se comprometerá a não acessar sem autorização,

não divulgar e proteger todos os dados de infraestrutura e de vulnerabilidades do contratante a que tiver acesso, que abrangerá todos os seus colaboradores e terceiros, sob as penas da lei.

4.8.1.49. A solução deve possibilitar a criação de relatórios baseados na seleção de ativos, permitindo inclusive a seleção de todos os ativos existentes.

4.8.1.50. Deve ser capaz de executar relatórios periódicos de acordo com a frequência estabelecida pelo administrador, bem como a geração de relatórios sob demanda.

4.8.1.51. Deve suportar a criação de relatórios criptografados (protegidos por senha configurável).

4.8.1.52. A solução deve suportar o envio automático de relatórios para destinatários específicos.

4.8.1.53. Deve ser possível definir a frequência na geração dos relatórios para no mínimo: Diário, Mensal, Semanal ou Anual.

4.8.1.54. Permitir especificar níveis de permissão nos relatórios para usuários e grupos específicos.

4.8.1.55. A solução deve fornecer relatórios gerenciais para as partes interessadas da empresa.

4.8.1.56. A solução deve fornecer relatórios de correções aplicadas, classificados pelos seguintes critérios:

a) tendência de ticket(Etiquetas dos ativos);

b) por grupo de ativos;

c) usuários; e

d) vulnerabilidades.

4.8.1.57. A solução deve possuir relatórios pré-configurados ou criar templates com as seguintes informações:

a) Hosts verificados sem credenciais;

b) Top 100 Vulnerabilidades mais críticas;

c) Top 10 Hosts infectados por Malwares;

d) Hosts exploráveis por Malwares;

e) Total de vulnerabilidades que podem ser exploradas pelo Metasploit;

f) Vulnerabilidades críticas e exploráveis; e

g) Máquinas com vulnerabilidades que podem ser exploradas.

4.8.1.58. A solução deve possuir dashboards customizáveis onde o administrador pode criar, editar ou remover painéis de acordo com a necessidade.

4.8.1.59. A solução deve ser capaz de inventariar todos os ativos da rede local e publicados na Internet, sem limites de endereços IPs.

4.8.2. **Características Gerais - Item 3**

4.8.2.1. A Contratada deverá efetuar a instalação e as configurações iniciais, em conjunto com a Contratante, para uso da solução proposta, incluindo criação de scans, relatórios, filtros, permissões de usuários e demais funcionalidades da solução.

4.8.2.2. A instalação e configuração da solução deverá ocorrer de acordo com as melhores práticas com a inclusão mínima dos seguintes entregáveis:

4.8.2.2.1. Planejamento e desenho da instalação e configuração;

4.8.2.2.2. Criação de políticas de scan;

4.8.2.2.3. Configuração de dashboards, queries e alertas iniciais;

4.8.2.2.4. Entrega de documentação com as principais informações do ambiente e futuras recomendações;

4.8.2.2.5. Instalação de scanners e agentes on-premises, quando aplicável.

4.8.2.3. A solução deve ser capaz de realizar varreduras (scans) de vulnerabilidades, avaliação de configuração e conformidade (baseline e compliance), indícios e padrões de códigos maliciosos conhecidos.

4.8.2.4. A solução deve fornecer criptografia de ponta a ponta dos dados de vulnerabilidades.

4.8.2.5. A solução deve fornecer gerenciamento de fluxo de trabalho de correção com base em políticas, incluindo a criação e atribuição automática de registro de problema.

4.8.2.6. A solução deve ser capaz de aplicar algoritmos de aprendizagem de máquina (machine learning) ou inteligência artificial (IA) para analisar as características relacionadas a vulnerabilidades.

4.8.2.7. Deve possuir uma API para automação de processos e integração com aplicações terceiras permitindo a extração de dados para carga no SIEM e com aplicações ITSM para as vulnerabilidades encontradas, permitindo o agrupamento no chamado por ações corretivas.

4.8.2.8. A solução pode ser baseada em nuvem pública com scanners próprios localizados em nuvem pública e scanners instalados na infraestrutura do cliente (on-premises).

4.8.2.9. A solução deve possibilitar a realização de cópias de segurança, funcionamento em alta disponibilidade e criptografia de todos os dados armazenados, além de incluir todo o software e licenciamento necessários para o funcionamento completo de acordo com as funcionalidades previstas neste Termo de Referência.

4.8.2.10. A atualização das ameaças deve ocorrer periodicamente, no mínimo, uma vez por mês sem interrupção dos serviços.

4.8.2.11. A atualização da infraestrutura da solução (servidores, bancos de dados, aplicações, sistemas operacionais e configurações), bem como a indisponibilidade da solução não devem provocar tempo de parada (downtime) superior 7,3 (sete vírgula três) horas por mês.

4.8.2.12. Configuração de segurança e acesso à gerência da solução:

a) Todos os dados armazenados nos servidores da solução devem ser criptografados e possuir logs de acesso;

b) A solução deve permitir a criação de, no mínimo, 20 contas para gerência e acesso aos relatórios, sem custo adicional.

4.8.2.13. Todas as licenças de uso de software devem ser registradas, na data da entrega, em nome da Contratante no site do fabricante.

4.8.2.14. A solução proposta no **Item 03 do Grupo 02** deve ser de mesmo fabricante, permitindo soluções on-premise, em nuvem ou híbrida, sem adaptações ou alterações não efetuadas pelo fabricante, disponível para gerenciamento em console web, sendo toda infraestrutura de aplicações, bancos de dados de vulnerabilidades, dashboards, agentes e plugins também mantidas pelo mesmo fabricante, oferecida como serviço padrão.

4.8.2.15. Se houver a necessidade, deverá ser fornecido o licenciamento do banco de dado corporativo para a instalação e monitoração da solução.

4.8.2.16. O fornecedor assinará, no ato da entrega das licenças e do serviço, Termo de Compromisso (conforme Anexo I-F), em que se comprometerá a não acessar sem autorização, não divulgar e proteger todos os dados de infraestrutura e de vulnerabilidades do contratante a que tiver acesso, que abrangerá todos os seus colaboradores e terceiros, sob as penas da lei.

4.8.2.17. Possibilitar a realização de análises e gestão de vulnerabilidades:

4.8.2.17.1. Análise Dinâmica em aplicações web (DAST).

4.8.2.17.2. O suporte técnico remoto é uma obrigação assessória do licenciamento das ferramentas e deverá estar disponível conforme descrito no item Níveis mínimos de serviços exigidos .

4.8.2.18. As ferramentas que compõem a solução devem permitir realizar análises dinâmicas (DAST) nas aplicações Web, assim como apresentar indicadores de risco, analisar as evidências de falhas identificadas nas aplicações Web;

4.8.2.19. Integração com LDAP, permitindo assim especificar usuários que deverão ter acesso a ferramenta baseado nas credenciais internas;

4.8.2.20. A solução não deverá restringir o cadastro de usuários habilitados para uso da solução. O controle de uso deverá ser por aplicação cadastrada na solução;

4.8.2.21. Deve ser possível acessar a solução pelos principais dispositivos de acesso, incluindo: computadores do tipo desktop e notebooks, com os seguintes sistemas operacionais: Linux 32/64bits e Windows 32/64bits, através de navegadores de internet padrão (W3C);

4.8.2.22. Implementar rotinas de backup e recuperação das bases de dados de configurações, usuários, perfis e informações/transações;

4.8.2.23. Garantir a integridade das informações, ou seja, ter a capacidade de desfazer transações incompletas e manter a consistência das informações na base de dados;

4.8.2.24. Implementar o acesso simultâneo e concorrente de múltiplos usuários à solução, para pesquisa e edição, preservando a integridade dos dados;

4.8.2.25. A solução deverá possuir um banco de vulnerabilidades atualizado: informações utilizadas pelas ferramentas que permitem que se encontrem vulnerabilidades conhecidas;

4.8.2.26. A solução deverá permitir as atualizações dos softwares de acordo com o lançamento de novas versões e pacotes de atualizações corretivas;

4.8.2.27. Disponibilizar funcionalidade de alertas para permitir a correção proativa de possíveis falhas de segurança;

4.8.2.28. Agrupar os resultados das análises executadas ao longo do tempo para permitir o acompanhamento e monitoramento dos níveis de maturidade de segurança;

4.8.2.29. Contemplar o conjunto de funcionalidades descritas neste documento, compondo uma solução única, integrando um ou mais softwares, desde que do mesmo fornecedor e preservando a total integração entre seus módulos e funcionalidades de forma nativa, além de uma interface de apresentação padronizada, em língua portuguesa ou inglesa e com painel de gerenciamento via web;

4.8.2.30. Possuir parâmetros que permitam a definição de horário, data e frequência de buscas de vulnerabilidades;

4.8.2.31. Deve permitir a visualização de todos os ativos cadastrados, com as seguintes informações:

4.8.2.31.1. Número de páginas/URLs encontradas;

4.8.2.31.2. A frequência definida para a realização de testes.

4.8.2.32. Permitir a visualização cumulativa dos últimos resultados obtidos para cada um dos ativos, por meio gráfico e informativo, facilitando o acompanhamento da evolução das medidas corretivas ao longo do tempo;

4.8.2.33. Permitir a visualização de todas as atividades de escaneamento realizadas pela solução em ordem cronológica ou por meio de busca de períodos;

4.8.2.34. Permitir a execução e paralização de varredura de forma manual;

4.8.2.35. Permitir a visualização das varreduras enquanto estas são executadas, a fim de acompanhar o progresso e as vulnerabilidades encontradas em tempo real;

4.8.2.36. Permitir a visualização de todas as vulnerabilidades encontradas para uma determinada aplicação, agrupadas em tipo e classe de ataque;

4.8.2.37. Permitir a visualização de todas as informações, evidências e referências técnicas relativas à vulnerabilidade encontrada;

4.8.2.38. Recomendar o melhor ponto para a correção das vulnerabilidades encontradas;

4.8.2.39. Permitir a visualização, inserção e edição de informações ou anotações específicas para cada uma das vulnerabilidades encontradas, incluindo itens como: usuário responsável, nível de risco para o negócio, dentre outros;

4.8.2.40. Permitir a marcação do estado de falso-positivo, assegurando que eventuais "falsos problemas" de vulnerabilidades detectadas sejam removidos nas varreduras futuras;

4.8.2.41. Disponibilizar uma seção que permita visualizar a evolução das vulnerabilidades ao longo do tempo, falhas em aberto, falsos-positivos, falhas corrigidas e histórico de atividades e também proporcionar a alteração do estado de cada uma das vulnerabilidades, permitindo remover

falsos-positivos, corrigir manualmente as vulnerabilidades ou retorná-las para o estado "aberto";

4.8.2.42. Deverá disponibilizar os seguintes relatórios, em formatos distintos incluindo PDF e XML. Os relatórios devem estar de acordo com o padrão da indústria e em conformidade com OWASP Top 10 e SANS CWE Top 25:

4.8.2.42.1. Relatório técnico de vulnerabilidades, a exemplo de Top 100 Vulnerabilidades mais críticas;

4.8.2.42.2. Relatório executivo de vulnerabilidades;

4.8.2.42.3. Relatório de sequência com a lista de URLs navegadas (para auditoria dos testes em aplicações web);

4.8.2.42.4. Relatório técnico de vulnerabilidades de aplicação, contendo apenas falhas relativas a uma determinada aplicação web;

4.8.2.42.5. Gráfico consolidado e cumulativo do número de vulnerabilidade ao longo do tempo;

4.8.2.42.6. Gráfico consolidado dos principais tipos de vulnerabilidades encontrados nos ativos avaliados;

4.8.2.42.7. Indicador gráfico da situação atual de risco dos ativos avaliados, classificando-a como "crítica", "alta", "média" ou "baixa";

4.8.2.42.8. Gráfico comparativo de vulnerabilidades entre aplicações cadastradas;

4.8.2.42.9. Relatório gerencial com o ranking das principais aplicações afetadas de acordo com a quantidade e criticidade de vulnerabilidades;

4.8.2.42.10. Relatório gerencial com o ranking dos principais ativos por classificação de risco para o negócio;

4.8.2.42.11. Relatório gerencial com o ranking das principais vulnerabilidades existentes.

4.8.2.43. Deve permitir a inserção de filtros nos relatórios, excluindo dos resultados informações que não sejam relevantes para a análise;

4.8.2.44. Permitir a configuração de envio de alertas via e-mail:

4.8.2.44.1. Quando uma varredura for iniciada;

4.8.2.44.2. Quando uma varredura for concluída.

4.8.2.45. Prover interface de Administração que será utilizada para desempenhar as seguintes atividades:

4.8.2.45.1. Cadastro e manutenção de políticas de varredura;

4.8.2.45.2. Cadastro e manutenção de novos componentes de varredura;

4.8.2.45.3. Cadastro e manutenção de novos grupos de ativos;

4.8.2.45.4. Cadastro e manutenção dos servidores de varredura;

4.8.2.45.5. Manutenção de falso-positivos marcados no módulo de gestão de vulnerabilidades;

4.8.2.45.6. Definir os usuários com permissões específicas (perfis) para gerenciamento de aplicações, varreduras, atualização de base de conhecimento de regras e administração da ferramenta.

4.8.2.46. A interface administrativa da solução deve possuir mecanismos de auditoria que permitam identificar eventos que envolvam: autenticação de usuários, gerenciamento de usuários, regras de varredura e gerenciamento das varreduras realizado;

4.8.2.47. A configuração de parâmetros automáticos de gestão de vulnerabilidades deverá incluir:

4.8.2.47.1. Lista de usuários responsáveis por tratar cada uma das vulnerabilidades, incluindo separação por ativos/aplicações;

4.8.2.47.2. Possibilidade de parametrização do risco para o negócio com base no nível de criticidade técnico da vulnerabilidade.

4.8.2.48. A solução deve permitir a criação de novas regras de análise, bem como permitir a customização de regras já existentes. As regras criadas ou customizadas devem estar disponíveis para novas análises;

4.8.2.49. Possuir capacidade de análise incremental, que realiza análise somente em conjunto de código/páginas modificadas a partir de uma “baseline” determinada, possibilitando a redução do tempo total de análise;

4.8.2.50. A solução deve permitir a inclusão de comentários, devendo ainda permitir registrar o nome do usuário responsável por estas marcações, além da inserção de comentários adicionais nas vulnerabilidades encontradas, mantendo-se o histórico nas análises subsequentes;

4.8.2.51. A solução deverá ser fornecida junto com a documentação técnica completa e atualizada, contendo manuais, guias de instalação e configuração, melhores práticas, dentre outros, em formato de arquivo eletrônico “Portable Document Format” (PDF) ou em páginas “HTML”, por meio de endereços de acesso eletrônico ao repositório da referida documentação.

4.8.2.52. Capacidade para produzir alertas para cada tipo de vulnerabilidade que for identificada. Tais alertas devem conter as seguintes informações:

4.8.2.52.1. Descrição da Vulnerabilidade;

4.8.2.52.2. Código de referência de bases de vulnerabilidades conhecidas, tais como: CVE, CWE ID e NIST 800-53, se houver;

4.8.2.52.3. Nível de severidade;

4.8.2.52.4. Guia de remediação;

4.8.2.52.5. Exemplos de remediação.

4.8.2.53. Permitir o agrupamento de vulnerabilidades em pacotes para facilitar o processo de triagem e correção;

4.8.2.54. Possibilitar ao usuário a definição de filtros para os resultados de uma varredura, permitindo focar em determinados tipos de apontamento, tais como: tipo de vulnerabilidade, risco, grau de confiabilidade, API onde foi encontrado, arquivo ou diretório onde se encontra o código fonte, etc;

4.8.2.55. Permitir ao usuário desabilitar regras de análise e permitir identificar quais regras de vulnerabilidades foram desabilitadas;

4.8.2.56. Permitir que o usuário crie regras de detecção, identificando uma vulnerabilidade que a ferramenta não foi capaz de detectar automaticamente;

4.8.2.57. A solução deverá exibir de forma visual as informações para a identificação da vulnerabilidade, incluindo o ponto de entrada na aplicação, as saídas, bem como em quaisquer outros pontos intermediários;

4.8.2.58. A solução deve possibilitar a criação de relatórios baseados na seleção de aplicações, permitindo inclusive a seleção de todas as aplicações existentes.

4.8.2.59. Deve ser capaz de gerar relatórios periódicos de acordo com a frequência estabelecida pelo administrador, bem como sob demanda.

4.8.2.60. A solução deve suportar o envio automático de relatórios para destinatários específicos.

4.8.2.61. Deve ser possível definir a frequência na geração dos relatórios para no mínimo: Diário, Mensal, Semanal e Anual.

4.8.2.62. Permitir especificar níveis de permissão nos relatórios para usuários e grupos específicos.

4.8.2.63. A solução deve fornecer relatórios gerenciais para as partes interessadas da empresa.

4.8.2.64. A solução deve fornecer relatórios de correções aplicadas, classificados pelos seguintes critérios:

a) tendência de ticket (Etiquetas dos ativos);

b) por grupo de aplicações;

c) usuários; e

d) vulnerabilidades.

4.8.2.65. A solução deve possuir dashboards customizáveis onde o administrador pode criar, editar ou remover painéis de acordo com a necessidade.

4.8.3. **ITEM 1 – Plataforma de Software para Avaliação de Vulnerabilidades**

4.8.3.1. A plataforma de software deve ser capaz de realizar varreduras (scans) de vulnerabilidades, de acordo com a quantidade de endereços IP licenciados.

4.8.3.2. A plataforma de software deve ser licenciada para um número ilimitado de scanners.

4.8.3.3. Deve permitir a configuração de vários painéis e widgets.

4.8.3.4. Deve ser capaz de medir e reportar ameaças.

4.8.3.5. Deve ser capaz de visualizar ameaças críticas ao ambiente monitorado.

4.8.3.6. A plataforma de software deve realizar varreduras em uma variedade de sistemas operacionais, suportando pelo menos hosts baseados em Windows, Linux e Mac OS, bem como appliances virtuais.

4.8.3.7. A plataforma de software deve suportar vários mecanismos de varredura distribuídos em diferentes localidades e regiões e gerenciar todos por uma console central.

4.8.3.8. A plataforma de software deve fornecer agentes instaláveis em sistemas operacionais, pelo menos Windows, Linux e Mac OS, para o monitoramento contínuo de configurações e vulnerabilidades.

4.8.3.9. Deve ser capaz de realizar varreduras em dispositivos móveis suportando no mínimo sistemas Android e IOS.

4.8.3.10. A plataforma de software deve permitir o monitoramento sem a necessidade de agentes instalados, até o limite de licenças adquiridas, para varredura diretamente no sistema operacional.

4.8.3.11. A plataforma de software deve ser configurável para permitir a otimização das parametrizações de varredura.

4.8.3.12. A plataforma de software deve incluir a capacidade de programar períodos de tempo e data onde varreduras não podem ser executadas, como por exemplo em determinados dias do mês ou determinados horários do dia.

4.8.3.13. No caso onde uma atividade de varredura seja interrompida por invadir o período não permitido, o mesmo deve ser capaz de ser reiniciado de onde parou.

4.8.3.14. A plataforma de software deve permitir a entrada e o armazenamento seguro de credenciais do usuário, incluindo contas locais, de domínio (LDAP e Active Directory) e root para sistemas Linux.

4.8.3.15. A plataforma de software deve fornecer a capacidade de escalar privilégios nos destinos, do acesso de usuário padrão até acesso de sistema ou administrativo.

4.8.3.16. A plataforma de software deve ser capaz de realizar pesquisas de dados confidenciais.

4.8.4. **ITEM 3 – Solução de Análise de Segurança em Aplicações Web**

4.8.4.1. Descrição da solução de análise dinâmica de aplicações (DAST)

4.8.4.1.1. A solução de análise dinâmica de vulnerabilidades deve permitir no mínimo 10 (dez) varreduras simultâneas de aplicações e 05 usuários conectados simultaneamente;

4.8.4.1.2. Varreduras simultâneas são as execuções de testes de vulnerabilidade para identificação de vulnerabilidades em aplicações diferentes realizadas paralelamente e ao mesmo tempo;

4.8.4.1.3. Suportar os seguintes protocolos:

4.8.4.1.3.1. HTTP 1.1;

4.8.4.1.3.2. HTTP 1.0;

4.8.4.1.3.3. SSL/TLS;

4.8.4.1.3.4. HTTP Keep-Alive;

4.8.4.1.3.5. HTTP Compression;

4.8.4.1.3.6. Configuração de HTTP User Agent string.

4.8.4.1.4. Suportar os seguintes protocolos de proxy: Proxy HTTP 1.0 e Proxy HTTP 1.1;

4.8.4.1.5. Suportar os seguintes esquemas de autenticação: Básica, Digest e HTTP Negotiate (NTLM e Kerberos).

4.8.4.1.6. Deve ser capaz de importar scripts de autenticação previamente configurados pelo usuário.

4.8.4.1.7. Suportar HTML baseado em formulários: Automatizado, Scripted; Não automatizado, Single Sign On, Certificados de Cliente SSL e Implementações customizadas.

4.8.4.1.8. Suportar os seguintes aspectos relacionados à gestão de sessão:

4.8.4.1.8.1. Compreender que a aplicação está pedindo para iniciar uma nova sessão, usando certo tipo de token como um método de identificar unicamente esta sessão;

4.8.4.1.8.2. Realizar uma atualização de token de sessão, quando instruído a fazê-lo pela aplicação;

4.8.4.1.8.3. Detectar que uma sessão realizada atualmente foi invalidada pelo aplicativo (sessão expirada);

4.8.4.1.8.4. Saber como iniciar uma nova sessão e readquirir tokens de sessão, no caso de uma sessão atual expirar.

4.8.4.1.9. Suportar os seguintes tokens de gerenciamento de sessão:

4.8.4.1.9.1. Cookies HTTP (RFC 2965);

4.8.4.1.9.2. Parâmetros de HTTP;

4.8.4.1.9.3. Caminho da URL HTTP.

4.8.4.1.10. Ter capacidade para realização de testes de segurança com serviços HTTP REST, incluindo fuzzing de diferentes verbos e parâmetros dos pedidos;

4.8.4.1.11. Permitir configuração para detecção automática de token de sessão atualização de Valor: O scanner tentará detectar tokens de sessão por conta própria e vai decidir quais tokens devem ser automaticamente rastreados/atualizados durante a varredura;

4.8.4.1.12. Permitir Configuração Manual de Token de Sessão: O usuário definirá o que denota um token de sessão, baseado em parâmetros HTTP, cookies ou qualquer outro tipo de configuração que é relevante (por exemplo, analisar partes da resposta e extrair alguns dados dela, que servem como o valor de token de sessão);

4.8.4.1.13. A configuração de sessão da ferramenta deverá permitir ao usuário definir quando, ou durante qual fase da varredura, os tokens de sessão serão atualizados. As seguintes opções deverão estar disponíveis:

4.8.4.1.13.1. Valor Fixo de Token de Sessão: quando um token de sessão está marcado para usar um valor fixo, esse valor nunca mudará durante a verificação;

4.8.4.1.13.2. Valor de Token fornecido durante processo de Login: quando o scanner de aplicação web "logar" na aplicação extrairá valores de token que foram emitidos como parte do processo de login, e vai usá-los até que ele detecte que a sessão foi invalidada;

4.8.4.1.13.3. Valor de Token Dinâmico: o scanner utilizará sempre o valor mais recente da sessão de token, como fornecida pela aplicação em todos os momentos. Isto significa que se durante a fase de rastreamento ou teste do scan um novo valor for detectado, o scanner irá parar e atualizar todos os pedidos HTTP subsequentes, com o valor mais recente.

4.8.4.1.14. Ser capaz de realizar o rastreamento de objetos / páginas, obedecendo aos seguintes critérios:

4.8.4.1.14.1. Fornecer ao usuário a opção de definir uma URL inicial;

4.8.4.1.14.2. Fornecer ao usuário a opção de definir nomes de host adicionais (os endereços IP) em uma lista ou um intervalo;

4.8.4.1.15. Fornecer ao usuário a opção de definir exclusões para:

4.8.4.1.15.1. Hostnames ou endereços IP's específicos;

4.8.4.1.15.2. URLs específicas ou padrões de URL (expressões regulares);

4.8.4.1.15.3. Extensões de arquivo específicas;

4.8.4.1.15.4. Parâmetros específicos.

4.8.4.1.16. Fornecer ao usuário a capacidade de limitar os pedidos redundantes. A capacidade de otimizar (tuning) um rastreador para limitar os pedidos para essas páginas redundantes deve existir;

4.8.4.1.17. Fornecer ao usuário a opção de suportar sessões simultâneas;

4.8.4.1.18. Fornecer ao usuário a capacidade de especificar um atraso de requisição;

4.8.4.1.19. Fornecer ao usuário a opção de definir uma profundidade máxima de rastreamento;

4.8.4.1.20. Durante sua execução, o rastreador deverá ser capaz de:

4.8.4.1.20.1. Identificar os hostnames recém-descobertos;

4.8.4.1.20.2. Suportar o envio de formulário automatizado;

4.8.4.1.20.3. Detectar páginas de erro e respostas 404 personalizadas;

4.8.4.1.20.4. Suportar redirecionamento HTTP, Meta Refresh e JavaScript;

4.8.4.1.20.5. Identificar e aceitar cookies, armazená-los e passá-los de volta ao servidor web enquanto faz o rastreamento;

4.8.4.1.20.6. Suportar aplicações AJAX de forma que seja capaz de submeter automaticamente requisições XML HTTP que são encontradas durante o processo de rastreamento.

4.8.4.1.21. Deverá ser capaz de analisar, no mínimo, os seguintes tipos de conteúdo para extrair informações sobre a estrutura e funcionalidade da aplicação:

4.8.4.1.21.1. HTML;

4.8.4.1.21.2. JavaScript;

4.8.4.1.21.3. XML;

4.8.4.1.21.4. Plaintext;

4.8.4.1.21.5. Applets Java;

4.8.4.1.21.6. CSS (Cascading Style Sheets).

4.8.4.1.21.7. JSON

4.8.4.1.21.8. Elementos DOM.

4.8.4.1.22. Deverá ser capaz de analisar e compreender, no mínimo, o conteúdo codificado nos seguintes tipos de codificação: IS0-8859-1 e UTF-8.

4.8.4.1.23. Deverá ser capaz de identificar e testar os seguintes problemas de vulnerabilidades e fraquezas de arquitetura relacionados à autenticação:

4.8.4.1.23.1. Autenticação Insuficiente;

4.8.4.1.23.2. Falta de SSL em páginas de login e áreas de acesso restrito;

4.8.4.1.23.3. Autocompletar não desabilitado em parâmetros de senha.

4.8.4.1.24. Deverá ser capaz de identificar e testar os seguintes problemas de vulnerabilidades e fraquezas de arquitetura relacionados à autorização:

4.8.4.1.24.1. Previsão de Credencial/Sessão;

4.8.4.1.24.2. Token de Sessão Sequencial;

4.8.4.1.24.3. Token de Sessão Não-Aleatória.

4.8.4.1.24.4. Autorização Insuficiente:

4.8.4.1.24.4.1. Habilidade para forçar a navegar por URL sem estar autorizado (navegar "logado", sem logar);

4.8.4.1.24.4.2. Habilidade para forçar a navegar por URL com alto privilégio enquanto "logado" com uma conta de baixo privilégio. Adulteração de método HTTP.

4.8.4.1.24.4.3. Expiração de sessão Insuficiente;

4.8.4.1.24.5. Fixação de sessão:

4.8.4.1.24.5.1. Incapacidade de gerar ID de nova sessão após login;

4.8.4.1.24.5.2. Gerenciamento de sessão permissiva.

4.8.4.1.24.6. Fraquezas de Sessão:

4.8.4.1.24.6.1. Token de sessão passado em URL;

4.8.4.1.24.6.2. Cookie de sessão não configurado com atributo de Segurança;

4.8.4.1.24.6.3. Cookie de sessão não configurado com atributo HTTPOnly;

4.8.4.1.24.6.4. Cookie de sessão não aleatório suficientemente;

4.8.4.1.24.6.5. Site não força conexão SSL;

4.8.4.1.24.6.6. Site usa SSL, mas referencia objetos inseguros;

4.8.4.1.24.6.7. Site Suporta Cifras SSL fracas.

4.8.4.1.25. Deverá ser capaz de identificar e testar os seguintes problemas de vulnerabilidades e fraquezas de arquitetura relacionadas a ataques do lado do cliente:

4.8.4.1.25.1. Falsificação de conteúdo (spoofing);

4.8.4.1.25.2. Cross-site Scripting (XSS);

4.8.4.1.25.3. Cross-Site Scripting Refletido;

4.8.4.1.25.4. Cross-Site Scripting Persistente;

4.8.4.1.25.5. Cross-Site Scripting DOM-based.

4.8.4.1.25.6. Cross-Frame Scripting;

4.8.4.1.25.7. HTML Injection;

4.8.4.1.25.8. Falsificação de requisição Cross-Site.

4.8.4.1.26. Deverá ser capaz de identificar e testar os seguintes problemas de vulnerabilidades e fraquezas de arquitetura relacionados à execução e injeção de comandos:

4.8.4.1.26.1. Ataque de Formato String;

4.8.4.1.26.2. Injeção de LDAP;

4.8.4.1.26.3. Injeção de comando de Sistema Operacional;

4.8.4.1.26.4. SQL Injection;

4.8.4.1.26.5. Blind SQL Injection;

4.8.4.1.26.6. Injeção de SSI;

4.8.4.1.26.7. Injeção de XPath;

4.8.4.1.26.8. Injeção de cabeçalho HTTP / Response Splitting;

4.8.4.1.26.9. Inclusão de Arquivo remoto;

4.8.4.1.26.10. Inclusão de Arquivo local;

4.8.4.1.26.11. Uploads de arquivos potencialmente maliciosos.

4.8.4.1.27. Deverá ser capaz de identificar e testar os seguintes problemas de vulnerabilidades e fraquezas de arquitetura relacionados à divulgação de informações:

4.8.4.1.27.1. Lista de indexação;

4.8.4.1.27.2. Vazamento de Informações;

4.8.4.1.27.3. Informações sigilosas em comentários de código;

4.8.4.1.27.4. Mensagens de erro de aplicação detalhadas;

4.8.4.1.27.5. Arquivos de backup (home.old, home.bak, etc);

4.8.4.1.27.6. Divulgação de arquivo de código fonte.

4.8.4.1.27.7. Path Traversal;

4.8.4.1.27.8. Localização de Recurso Previsível;

4.8.4.1.27.9. Métodos HTTP inseguros habilitados;

4.8.4.1.27.10. WebDAV habilitado;

4.8.4.1.27.11. Arquivos padrão de Servidor Web;

4.8.4.1.27.12. Páginas de Testes e Diagnósticos (test.asp, phpinfo.htm, etc.);

4.8.4.1.27.13. Divulgação de endereço IP interno.

4.8.4.1.28. Deverá ser capaz de identificar e testar os seguintes problemas de vulnerabilidades e fraquezas de arquitetura relacionados a assinaturas de ataque:

4.8.4.1.28.1. Ter uma base extensiva de assinaturas de ataques conhecidas de pacotes e componentes de terceiros, tais como OWASP, NIST, SANS, CVE, etc., incluindo aplicações desenvolvidas em plataformas diversas;

4.8.4.1.28.2. Esta base de assinatura deverá ser atualizada frequentemente pela internet, e deverá possuir capacidade de reconhecimento de versão e vulnerabilidade de pacotes de terceiros, incluindo os mais utilizados tais como Wordpress, Drupal, Joomla e Plone.

4.8.4.1.29. Permitir a customização das políticas de testes por meio de configuração;

4.8.4.1.30. Permitir que o usuário modifique políticas de testes existentes;

4.8.4.1.31. Permitir ao usuário criar novas políticas de testes customizados;

4.8.4.1.32. Permitir ao usuário criar políticas de testes customizados que especifiquem quais testes incluir em uma varredura;

4.8.4.1.33. Ter a capacidade de executar varreduras de forma remota/distribuída;

4.8.4.1.34. Ter capacidade de executar varreduras simultaneamente;

4.8.4.1.35. Ter capacidade de agendar varreduras;

4.8.4.1.36. Ter capacidade de visualização em tempo real o estado das varreduras em execução;

4.8.4.1.37. Permitir a visualização de todas as páginas (URLs) encontradas na última avaliação, com a possibilidade de busca por palavra-chave;

4.8.4.1.38. Permitir a visualização de objetos relativos à aplicação web, incluindo hosts bloqueados, e-mails e cookies, com a possibilidade de busca por palavra chave;

4.8.4.1.39. Capacidade para suportar múltiplos usuários concorrentes;

4.8.4.1.40. Deverá ser capaz de produzir informações para cada tipo de vulnerabilidade identificada, classificando-as conforme a seguir:

4.8.4.1.40.1. Descrição da Vulnerabilidade;

4.8.4.1.40.2. Referência em mais de um banco de dados de registro de padrões de ataque, pelo menos CVE ou CWE ID;

4.8.4.1.40.3. Nível de severidade;

4.8.4.1.40.4. Pontuação CVSS, quando houver;

4.8.4.1.40.5. Guia de Remediação;

4.8.4.1.40.6. Exemplos de código de Remediação;

4.8.4.1.41. Evidências da execução dos ataques demonstrando os pontos onde a aplicação está vulnerável;

4.8.4.1.42. Deverá ser capaz de exibir as requisições da ferramenta e respostas dadas pela aplicação web durante o teste.

4.8.4.1.43. Permitir a seleção ou remoção de testes de segurança que possam causar indisponibilidade, tais como denial-of-service (DoS);

4.8.4.1.44. Permitir que toda a operação (comando e controle) seja feita através do Módulo de Gestão de Vulnerabilidades, incluindo:

4.8.4.1.44.1. Configuração de políticas e testes de segurança;

4.8.4.1.44.2. Agendamento e configuração de novos testes;

4.8.4.1.44.3. Gestão de falsos-positivos;

4.8.4.1.44.4. Gestão de relatórios e eventos de vulnerabilidades.

4.8.4.1.45. A solução de análise deve ser capaz de identificar vulnerabilidades de vazamento de dados como os de identificação pessoal.

4.8.4.1.46. A solução de análise deve suportar a integração com softwares de automação de testes.

4.8.4.1.47. Suporte a ferramentas para construção de requisições e análise de respostas de aplicações WEB, API's e WebServices, tais como Postman Collections.

4.8.4.1.48. Deve ser capaz de utilizar scripts customizados de crawling com parâmetros definidos pelo usuário.

4.8.4.1.49. Deve ser capaz de instituir no mínimo os seguintes limites:

4.8.4.1.49.1. Número máximo de URLs para crawling e navegação;

4.8.4.1.49.2. Número máximo de diretórios para varreduras;

4.8.4.1.49.3. Número máximo de elementos DOM;

4.8.4.1.49.4. Tamanho máximo de respostas;

4.8.4.1.49.5. Tempo máximo para a varredura;

4.8.4.1.49.6. Número máximo de conexões HTTP ou HTTPS ao servidor hospedando a aplicação Web; e

4.8.4.1.49.7. Número máximo de requisições HTTP ou HTTPS por segundo.

4.8.4.1.50. Deverá ser compatível com avaliação de web services REST e SOAP.

4.8.4.1.51. A solução deve ser compatível com as seguintes tecnologias, não se limitando às listadas a seguir:

4.8.4.1.51.1. WordPress;

4.8.4.1.51.2. IIS 6.x e IIS 10.x;

4.8.4.1.51.3. .NET 2;

4.8.4.1.51.4. Apache HTTPD 2.2.x e 2.4.x;

4.8.4.1.51.5. Tomcat 6.x, 7.x e 8.x;

4.8.4.1.51.6. Jetty 8;

4.8.4.1.51.7. Nginx;

4.8.4.1.51.8. Jboss 4.x e 7.x;

4.8.4.1.51.9. WildFly 8 e 10;

4.8.4.1.51.10. Plone 2.5.x e 4.3.x;

4.8.4.1.51.11. Zope;

4.8.4.1.51.12. J2EE;

4.8.4.1.51.13. Ansible;

4.8.4.1.51.14. Joomla;

4.8.4.1.51.15. Moodle;

4.8.4.1.51.16. Docker Container;

4.8.4.1.51.17. GIT;

4.8.4.1.51.18. Grafana; e

4.8.4.1.51.19. Redmine.

4.8.5. **ITEM 2 e Item 4 – Serviço Técnico Especializado**

4.8.5.1. **O Serviço Técnico Especializado** será prestado por meio da prestação de serviços nas dependências da CONTRATANTE ou de forma remota, de acordo com as necessidades elencadas, preferencialmente nos dias úteis (de segunda a sexta-feira), no horário de 08hs as 18hs, e deverão executar as seguintes atividades:

4.8.5.1.1. Acompanhar, quando solicitado por um usuário, todas as operações realizadas na solução durante determinado período de tempo;

4.8.5.1.2. Esclarecer dúvidas de usuários em relação à operação da solução;

4.8.5.1.3. Prestar serviços de suporte técnico para a solução de problemas que impeçam o perfeito funcionamento da solução;

4.8.5.1.4. Reportar à Contratante quaisquer outros problemas verificados durante o atendimento, relativos ou não à solução fornecida;

4.8.5.1.5. Fornecer informações aos usuários sobre a situação e o andamento de serviços de manutenção solicitados;

4.8.5.1.6. Diagnosticar a performance do software em seus aspectos operacionais;

4.8.5.1.7. Identificar problemas inerentes ao software e ao ambiente onde este se encontra instalado;

4.8.5.1.8. Discutir implementações de melhorias, visando possíveis adequações;

4.8.5.1.9. Apoiar no desenvolvimento de dashboads e solução de problemas internos, relativos às licenças adquiridas.

4.8.5.1.10. Integrar a solução com ferramentas de ITSM.

4.8.5.1.11. Verificar pendências de atualizações de versões de firmwares, engines, assinaturas ou qualquer componente da solução passível de atualização e recomendar as ações necessárias para regularização;

4.8.5.1.12. Serviços especializados para a configuração/integração da ferramenta com as demais soluções da CONTRATANTE. Tais como:

4.8.5.1.12.1. Planejamento e desenvolvimento de API's permitindo a importação e exportação de dados;

4.8.5.1.12.2. Transferência de conhecimento sobre as funcionalidades e Melhores práticas;

4.8.5.1.12.3. Auxílio na instalação, Configuração, teste e validação da solução;

4.8.5.1.12.4. Documentação e transferência de conhecimento das atividades técnicas realizadas.

4.8.5.1.12.5. Reinstalação da Solução, quando e se necessário;

4.8.5.2. Na prestação do serviço de técnico especializado a Contratada deverá utilizar profissionais com qualificação e treinamento adequados para o desenvolvimento das tarefas relacionadas anteriormente;

4.8.5.3. O espaço físico, o mobiliário e o ramal telefônico necessário para a execução dos serviços serão fornecidos pela Contratante. Caberá à Contratada providenciar todos os demais recursos que considerar necessários para a prestação dos serviços;

4.9. **Requisitos de Projeto e de Implementação**

A CONTRATADA deverá disponibilizar ao Órgão documentação onde constem as especificações técnicas detalhadas dos produtos e serviços ofertados.

4.9.1. Deverá disponibilizar ainda os requisitos de projeto e de implementação, incluindo a descrição dos padrões dos serviços e método de gestão relacionados na seção 2 (Descrição da Solução de TIC) e seção 6 (Modelo de execução do Contrato) deste Termo de Referência.

4.10. **Requisitos de Implantação**

4.10.1. Tendo em vista que a presente contratação diz respeito à contratação de serviços e de subscrição de licenças, a CONTRATADA, no que couber, será responsável pela implantação/disponibilização da solução contratada. Outrossim, a disponibilização das licenças demandadas deve ser feita de acordo com os prazos definidos no tópico Requisitos Temporais deste Termo de Referência

4.11. **Requisitos de Garantia**

4.11.1. Todo o software deve contemplar atualizações e garantia total por todo o período de vigência das licenças, caso haja renovação do licenciamento será também renovada a garantia, conforme quantidades, requisitos e especificações constantes deste documento.

4.11.2. A garantia técnica abrange a realização de todas as correções necessárias e será acionada por meio de chamados técnicos, igualmente aos requisitos do suporte técnico.

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

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

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

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

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

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

4.11.8.1. prejuízos advindos do não cumprimento do objeto do Contrato e do não adimplemento das demais obrigações nele previstas;

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

4.11.8.3. multas moratórias e punitivas aplicadas pela Administração à CONTRATADA; e

4.11.8.4. obrigações trabalhistas e previdenciárias de qualquer natureza e para com o FGTS, não adimplidas pela CONTRATADA, quando couber.

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

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

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

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

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

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

4.11.14. A CONTRATANTE executará a garantia na forma prevista na legislação que rege a matéria.

4.11.15. Será considerada extinta a garantia:

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

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

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

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

4.12. **Requisitos de Experiência Profissional**

4.12.1. Para os itens 1 e 3: os profissionais da CONTRATADA responsáveis pelo treinamento devem ter experiência mínima de 1 (um) ano trabalhando com treinamento na solução contratada.

4.12.2. Para o itens 2 e 4: os profissionais da CONTRATADA devem ter experiência mínima de 1 (um) ano trabalhando com serviço técnico especializado na solução contratada.

4.13. **Requisitos de Formação da Equipe**

4.13.1. Para os itens 1 e 3 os requisitos de Formação de Equipe não são aplicáveis quando o objeto da contratação envolver apenas o fornecimento de bens de TIC.

4.13.2. A formação da equipe que implantará a solução, que fornecerá o treinamento, bem como prestará o serviço técnico especializado ficará a critério da CONTRATADA, exigindo-se os respectivos perfis relacionados nas tabelas 5 e 6.

Tabela 5 - Perfil Instrutor

PERFIL – Para o item 1 e 3 Instrutor: Responsável por realizar as atividades relacionadas à capacitação na solução contratada.	
Experiência/Qualificação	**Modo de Comprovação**
Experiência mínima de 01 (um) ano em treinamento na solução contratada.	Registro em Carteira de Trabalho ou contrato(s) executado(s) pelo funcionário, além da devida documentação necessária para que se comprove a participação do funcionário na execução das atividades.
Formação	**Modo de Comprovação**
Curso superior completo na área de Tecnologia da Informação, ou qualquer formação de nível superior com pós-graduação na área de Tecnologia da Informação e certificação do fabricante na solução contratada.	Diploma, devidamente registrado, de conclusão de curso de graduação na área de Tecnologia da Informação ou nível superior em qualquer área com pós-graduação na área de Tecnologia da Informação em nível de especialização ou mestrado ou doutorado, fornecido por instituição de ensino superior reconhecido pelo Ministério da Educação – MEC. Certificado emitido pelo fabricante da solução contratada.

Tabela 6 - Perfil Profissional de Segurança da Informação

PERFIL – Para os itens 1 e 3: Profissional de Segurança da Informação: Responsável por realizar as atividades relacionadas à implantação da solução contratada; e **PERFIL – Para os itens 2 e 4: Profissional de Segurança da Informação:** Responsável por realizar as atividades relacionadas ao serviço técnico especializado.	
Experiência/Qualificação	**Modo de Comprovação**
Experiência mínima de 01 (um) ano em serviço técnico especializado na solução contratada.	Registro em Carteira de Trabalho ou contrato(s) executado(s) pelo funcionário, além da devida documentação necessária para que se comprove a participação do funcionário na execução das atividades.
Formação	**Modo de Comprovação**
Curso superior completo na área de Tecnologia da Informação, ou qualquer formação de nível superior com pós-graduação na área de Tecnologia da Informação e certificação do fabricante na solução contratada.	Diploma, devidamente registrado, de conclusão de curso de graduação na área de Tecnologia da Informação ou nível superior em qualquer área com pós-graduação na área de Tecnologia da Informação em nível de especialização ou mestrado ou doutorado, fornecido por instituição de ensino superior reconhecido pelo Ministério da Educação – MEC. Certificado emitido pelo fabricante da solução contratada.

4.14. **Requisitos de Metodologia de Trabalho**

4.14.1. Os requisitos de Metodologia de Trabalho estão detalhados nos tópicos modelo de execução do contrato e modelo de gestão do contrato do presente termo de referência.

4.15. **Requisitos de Segurança da Informação**

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

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

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

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

4.15.2. A CONTRATADA deverá instruir seus empregados quanto à necessidade de acatar as normas internas da Administração.

4.15.3. A CONTRATADA deverá instruir seus empregados a respeito das atividades a serem desempenhadas, alertando-os a não executar atividades não abrangidas pelo contrato, devendo a CONTRATADA relatar à CONTRATANTE toda e qualquer ocorrência neste sentido, a fim de evitar desvio de função.

4.15.4. A CONTRATADA não poderá se utilizar da presente contratação para obter qualquer acesso não autorizado as informações de propriedade do Ministério da Justiça e Segurança Pública.

4.15.5. A CONTRATADA não pode obter, capturar, copiar ou transferir qualquer tipo informação de propriedade do Ministério da Justiça e Segurança Pública, sem autorização.

4.15.6. A CONTRATADA deverá assinar Termo de Compromisso previsto no Anexo I - F.

4.15.7. O s empregados da CONTRATADA diretamente envolvidos no projeto no órgão devem assinar o Termo de Ciência - Anexo I - E.

4.15.8. Quando houver a custódia de conhecimentos, informações e dados pelo prestador de serviços, a CONTRATADA e a FABRICANTE/PROPRIETÁRIA deverão cumprir com as seguintes diretivas:

4.15.8.1. Garantia de foro brasileiro;

4.15.8.2. Garantia de que o acesso aos dados, metadados, informações e conhecimentos utilizados e/ou armazenados na solução, ferramentas, software, infraestrutura ou em qualquer outro recurso que a CONTRATADA/FABRICANTE utilize para a prestação de serviços somente serão acessados pelo CONTRATANTE e serão protegidos de acessos de outros clientes e de colaboradores da CONTRATADA/FABRICANTE;

4.15.8.3. Garantia de que, em qualquer hipótese, a Administração Pública Federal tenha a tutela absoluta sobre os conhecimentos, informações e dados produzidos pelos serviços;

4.15.8.4. Garantia de vedação de uso não corporativo dos conhecimentos, informações e dados pelo prestador de serviço, bem como a redundância não autorizada;

4.15.8.5. Garantia de que a solução faça uso de criptografia nas camadas e protocolos de redes de ativos computacionais para os dados em trânsito e/ou armazenados;

4.15.8.6. Garantia de acesso do CONTRATANTE a logs e mecanismos de auditoria; e

4.15.8.7. Garantia de manutenção de cópias de segurança (backup), durante toda a vigência contratual, de dados, metadados, informações e/ou conhecimentos custodiados pela CONTRATADA/FABRICANTE.

4.15.9. A CONTRATADA deve disponibilizar mecanismos para auditoria de atividades dos usuários e devem permitir diversos tipos de consulta aos logs, gerando relatórios customizados, quando necessário.

4.15.9.1. A CONTRATADA deve garantir junto ao fabricante, o registro em log todos os eventos de segurança (incluindo informação sobre sessões e transações) por um período de no mínimo 1 (um) ano e permitir o acesso e utilização dos registros de log gerados pela equipe da Contratante.

4.15.10. O acesso e uso de ferramentas de auditoria que interajam com os sistemas de informação do CONTRATANTE deverão estar devidamente segmentados e restritos para evitar comprometimentos e uso indevido de dados de log.

4.16. **Outros Requisitos Aplicáveis**

4.16.1. **Vistoria**

4.16.1.1. Para o correto dimensionamento e elaboração de sua proposta, será facultado à LICITANTE realizar vistoria para conhecer a infraestrutura e as instalações do CONTRATANTE. Para tanto poderá encaminhar representante capacitado para realizar visita às instalações do Órgão específico nos locais indicados no item Locais de entrega. Nesta ocasião a empresa assinará compromisso de guardar sigilo sobre todas as informações relativas ao contratante.

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

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

4.16.1.4. O agendamento deverá ser realizado de segunda a sexta, em horário comercial, por meio eletrônico email: crs@mj.gov.br. O Ministério recomenda que esta marcação seja feita com a maior antecedência possível, para evitar congestionamento de vistorias.

4.16.1.5. Quando da vistoria ao local dos serviços, as LICITANTES devem se inteirar de todos os aspectos referentes à execução do fornecimento, não se admitindo, posteriormente, qualquer alegação de desconhecimento dos mesmos.

4.16.1.6. Para todos os efeitos, considerar-se-á que a LICITANTE, optante pela realização de vistoria ou não, tem pleno conhecimento da natureza e do escopo dos serviços, não se admitindo, posteriormente, qualquer alegação de desconhecimento dos serviços e de dificuldades técnicas não previstas.

4.16.1.7. Efetuada a vistoria será lavrado, por representante da equipe técnica, designado para tanto, o respectivo Termo de Vistoria, conforme modelo do ANEXO I-D- MODELO DE DECLARAÇÃO DE VISTORIA, o qual deverá ser preenchido e assinado pelo interessado em participar da licitação, anexando, oportunamente, à sua habilitação.

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

4.16.1.9. Caso a LICITANTE renuncie à vistoria técnica aos locais de instalação das licenças, deverá entregar a Declaração de Renúncia à Vistoria, conforme modelo do ANEXO I - G - MODELO DE DECLARAÇÃO DE RENÚNCIA À VISTORIA, o qual deverá ser preenchido e assinado pelo interessado em participar da licitação, anexando, oportunamente, à sua habilitação.

4.16.2. **Do uso da ATA**

4.16.2.1. Devido ao fato de que a presente licitação se presta às necessidades do Ministério da Justiça e Segurança Pública e do CADE para o desenvolvimento de projetos que utilizem soluções comuns de tecnologia da informação, não será permitido o uso (adesão) da ata de registro de preços por outros órgãos e entidades, nem de forma tardia.

4.16.2.2. Não será permitida a participação de outros órgãos na Intenção de Registro de Preços.

4.16.3. **Subcontratação**

4.16.3.1. Não será admitida a subcontratação do objeto licitatório total ou parcial, não sendo permitida, outrossim, a associação da CONTRATADA com outrem, a cessão ou transferência total ou parcial do objeto do contrato.

5. RESPONSABILIDADES

5.1. **Deveres e responsabilidades da CONTRATANTE**

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

5.1.2. Encaminhar formalmente a demanda por meio de Ordem de Serviço ou de

Fornecimento de Bens, de acordo com os critérios estabelecidos no Termo de Referência ou Projeto Básico;

5.1.3. Receber o objeto fornecido pela contratada que esteja em conformidade com a proposta aceita, conforme inspeções realizadas;

5.1.4. Aplicar à contratada as sanções administrativas regulamentares e contratuais cabíveis, comunicando ao órgão gerenciador da Ata de Registro de Preços, quando aplicável;

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

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

5.1.7. Definir produtividade ou capacidade mínima de fornecimento da solução de TIC por parte da contratada, com base em pesquisas de mercado, quando aplicável; e

5.1.8. Prever que os direitos de propriedade intelectual e direitos autorais da solução de TIC sobre os diversos artefatos e produtos produzidos em decorrência da relação contratual, incluindo a documentação, o código-fonte de aplicações, os modelos de dados e as bases de dados, pertençam à Administração;
Exigir o cumprimento de todas as obrigações assumidas pela Contratada, de acordo com as cláusulas contratuais e os termos de sua proposta.

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

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

5.1.11. Permitir acesso dos empregados da Contratada às suas dependências para a execução dos serviços.

5.1.12. Prestar as informações e os esclarecimentos pertinentes que venham a ser solicitados pelo representante ou preposto da Contratada.

5.1.13. Não praticar atos para ingerência na administração da empresa contratada, especialmente quanto a direcionamento de escolha de possíveis trabalhadores;

5.1.14. Para contratos de prestação de serviços com regime de dedicação exclusiva de mão de obra, não praticar atos tendentes a gerar vínculo empregatício entre os empregados da empresa contratada e o Ministério, vedando-se qualquer relação entre estes que caracterize pessoalidade e subordinação direta, atentando-se às vedações explícitas no art. 5º da Instrução Normativa SEGES/MPOG nº 5, de 26 de maio de 2017; e

5.1.15. Notificar a Contratada, por escrito quando, verificados desvios de condutas, irregularidades, fraudes ou atos ilícitos, praticados na execução do contrato;

5.2. **Deveres e responsabilidades da CONTRATADA**

5.2.1. Indicar formalmente preposto apto a representá-lo junto à contratante, que deverá responder pela fiel execução do contrato;

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

5.2.3. 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;

5.2.4. Propiciar todos os meios necessários à fiscalização do contrato pela contratante, cujo representante terá poderes para sustar o fornecimento, total ou parcial, em qualquer tempo, sempre que considerar a medida necessária;

5.2.5. Manter, durante toda a execução do contrato, as mesmas condições da habilitação;

5.2.6. Quando especificada, manter, durante a execução do contrato, equipe técnica composta por profissionais devidamente habilitados, treinados e qualificados para fornecimento da solução de TIC;

5.2.7. Quando especificado, manter a produtividade ou a capacidade mínima de fornecimento da solução de TIC durante a execução do contrato; e

5.2.8. Ceder os direitos de propriedade intelectual e direitos autorais da solução de TIC sobre os diversos artefatos e produtos produzidos em decorrência da relação contratual, incluindo a documentação, os modelos de dados e as bases de dados à Administração.

5.2.9. Executar os serviços conforme especificações deste Termo de Referência e de sua proposta, além de fornecer os materiais e equipamentos, ferramentas e utensílios necessários, se for o caso, na qualidade e quantidade especificadas neste Termo de Referência e em sua proposta.

5.2.10. Responsabilizar-se pelos vícios e danos decorrentes da execução do objeto, de acordo com os artigos 14 e 17 a 27, do Código de Defesa do Consumidor (Lei nº 8.078, de 1990), ficando a CONTRATANTE autorizada a descontar da garantia, caso exigida no edital, ou dos pagamentos devidos à Contratada, o valor correspondente aos danos sofridos.

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

5.2.12. Responsabilizar-se por todas as obrigações trabalhistas, sociais, previdenciárias, tributárias e as demais previstas na legislação específica, cuja inadimplência não transfere responsabilidade à CONTRATANTE.

5.2.13. Relatar à CONTRATANTE toda e qualquer irregularidade verificada no decorrer da prestação dos serviços.

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

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

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

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

5.2.18. Auxiliar o CONTRATANTE na elaboração de políticas e procedimentos relacionados à gestão e uso dos serviços contratados, inclusive no que tange à implantação de medidas de racionalização e economia.

5.2.19. Ser responsável exclusivo por quaisquer acidentes na execução dos serviços contratados e pela destruição ou dano dos documentos por culpa ou dolo de seus agentes.

5.2.20. A CONTRATADA garante que os produtos licenciados para uso não infringem quaisquer patentes, direitos autorais ou trade-secrets, devendo a CONTRATADA se responsabilizar por quaisquer despesas relacionadas que ocorram.

5.2.21. O Contratante não aceitará, sob nenhum pretexto, a transferência de qualquer responsabilidade da Contratada para outras entidades, sejam fabricantes, técnicos, subcontratados, etc.

5.2.22. Assinar Termo de Confidencialidade no qual fica a contratada impedida de liberar informações do órgão para empresas terceiras.

5.2.23. Fica a contratada proibida de utilizar de dados ou informações do órgão para propaganda ou uso secundário não-autorizado.

5.2.24. Fica a contratada obrigada a assegurar o retorno integral dos dados e informações sob sua custódia ao órgão de origem, no caso de término do contrato.

5.2.25. O Contratante mantém direitos exclusivos sobre todas as informações e dados gerados durante o período contratado. Essa propriedade inclui qualquer cópia disponível, inclusive backups de segurança.

5.2.26. Informar prontamente ao CONTRATANTE sobre fatos e/ou situações relacionadas à prestação dos serviços contratados que representem risco ao êxito da contratação ou o cumprimento de prazos exigidos, além de responsabilizar-se pelo conteúdo e veracidade das informações prestadas - sob pena de incorrer em situações de dolo ou omissão.

5.2.27. Responsabilizar-se por todas as obrigações trabalhistas, sociais, previdenciárias, tributárias e as demais previstas na legislação específica, cuja inadimplência não transfere responsabilidade à CONTRATANTE.

5.2.28. O Contratante possui “Direito ao Esquecimento”, ou seja, fica a contratada obrigada a eliminar completamente qualquer dado ou informação obtida do órgão sob sua custódia ao término do contrato.

5.2.29. A contratada deve informar os dados de telefone celular dos responsáveis pela empresa, incluindo um número principal e um adicional, para casos de emergência em que a Administração precise contactar os responsáveis (Importante esclarecer que os contatos principais ainda serão os comerciais, e que tais números serão utilizados apenas para os casos de emergência).

5.2.30. É de responsabilidade da CONTRATADA fornecer a seus técnicos todas as ferramentas, softwares e instrumentos necessários para a execução dos serviços, bem como prover e se responsabilizar pela locomoção dos mesmos até o Órgão.

5.2.31. A CONTRATADA poderá substituir qualquer profissional durante o decorrer do contrato, desde que avise à CONTRATANTE do fato, e indique o substituto para esse profissional.

5.2.32. Estabelecer, em conformidade à Portaria MJSP nº 513, de 2020, normas gerais de integridade em até 3(três) meses após a assinatura do contrato, caso esse ultrapasse o valor previsto no inciso I ou II do Art. 1º da referida portaria;

5.2.32.1. A implantação ou a adequação do Programa de Integridade poderá ser comprovada por qualquer documento hábil a ser encaminhado à equipe de fiscalização do contrato, preferencialmente, em meio digital.

5.2.33. Orientar seus empregados alocados para a execução do contrato sobre as normas de integridade e a indispensabilidade de seu cumprimento;

5.2.34. Adotar práticas de governança e gestão capazes de identificar e mitigar desvios de conduta, irregularidades, fraudes e atos ilícitos, de acordo com as normas de integridade previstas na Lei nº 12.846, de 1º de agosto de 2013, e no Decreto nº 8.420, de 18 de março de 2015;

5.2.35. Relatar ao órgão contratante, por escrito, qualquer descumprimento das normas de integridade praticado por agentes públicos com os quais mantenha contato em decorrência da execução do contrato;

5.2.36. Substituir com presteza qualquer profissional que tenha cometido desvios de conduta, irregularidades, fraudes e atos ilícitos, conforme observado e notificado pelo agente público competente;

5.2.37. Apresentar, no momento da celebração do contrato, Declaração de Inexistência de Vínculo Familiar, nos termos do art. 7º do Decreto nº 7.203, de 4 de junho de 2010, em que é assumido o compromisso de não utilizar, na execução do contrato, mão de obra que seja cônjuge, companheiro ou parente em linha reta ou colateral, por consanguinidade ou afinidade, até o terceiro grau, de agente público que exerce cargo em comissão ou função de confiança no âmbito do Ministério da Justiça e Segurança Pública;

5.2.38. Apresentar à equipe de fiscalização do contrato, juntamente com o rol de documentos obrigatórios do empregado alocado para a execução do contrato, Termo de Ciência e Concordância, devidamente assinado pelo empregado, conforme modelo constante no anexo à Portaria MJSP nº 513, de 2020 e a este Projeto Básico;

5.2.39. Encaminhar à equipe de fiscalização do contrato, observados os prazos estabelecidos na alínea “a”, documentação que evidencie, em alinhamento com os parâmetros

do Capítulo IV do Decreto nº 8.420, de 2015, a realização das seguintes ações e atividades:

5.2.39.1. promoção e participação em reuniões, apresentações, palestras e quaisquer outros eventos de natureza semelhante que evidenciam o comprometimento da alta direção da empresa em temas relacionados à integridade;

5.2.39.2. mapeamento dos riscos de integridade e estabelecimento de ações mitigadoras, revisadas periodicamente;

5.2.39.3. canal de denúncia, aberto e amplamente divulgado, com garantia do devido sigilo ao denunciante;

5.2.39.4. código de ética ou de conduta aplicável a todos os dirigentes, administradores e empregados, independente de cargo, emprego, posto ou função exercidos;

5.2.39.5. treinamentos periódicos sobre o Programa de Integridade, que envolvam as vedações incidentes na relação público-privada;

5.2.39.6. promoção de campanhas para divulgar os princípios e valores que regem a empresa contratada e o serviço público, bem como outros temas sobre integridade e combate a desvios de conduta, fraudes, irregularidades e atos ilícitos;

5.2.39.7. adoção de medidas disciplinares, em caso de violação do Programa de Integridade, e de procedimentos e determinações que assegurem a pronta interrupção da tentativa ou da prática de desvios de conduta, fraudes, irregularidades e atos ilícitos;

5.2.39.8. monitoramento contínuo do Programa de Integridade, com objetivo de aperfeiçoar os mecanismos de prevenção de atos lesivos, bem como sua detecção e combate; e

5.2.39.9. encaminhamento semestral de relatório da execução do Programa de Integridade à equipe de fiscalização do contrato; e

5.2.40. Cumprir e exigir que os empregados alocados para a execução do contrato nas repartições administrativas cumpram, no que couber, as regras estabelecidas pelos órgãos do Ministério da Justiça e Segurança Pública

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

5.3.1. Efetuar o registro do licitante fornecedor e firmar a correspondente Ata de Registro de Preços;

5.3.2. Conduzir os procedimentos relativos a eventuais renegociações de condições, produtos ou preços registrados;

5.3.3. Definir mecanismos de comunicação com os órgãos participantes e não participantes, contendo:

5.3.3.1. As formas de comunicação entre os envolvidos, a exemplo de ofício (para a unidade CRS) ou e-mail (crs@mj.gov.br).

5.3.3.2. Definição dos eventos a serem reportados ao órgão gerenciador, com a indicação de prazo e responsável;

5.3.4. Definir mecanismos de controle de fornecimento da solução de TIC, observando, dentre outros:

5.3.4.1. A definição da produtividade ou da capacidade mínima de fornecimento da solução de TIC;

5.3.4.2. As regras para gerenciamento da fila de fornecimento da solução de TIC aos órgãos participantes e não participantes, contendo prazos e formas de negociação e redistribuição da demanda, quando esta ultrapassar a produtividade definida ou a capacidade mínima de fornecimento e for requerida pela contratada; e

5.3.4.3. As regras para a substituição da solução registrada na Ata de Registro de Preços, garantida a realização de Prova de Conceito, em função de fatores supervenientes que tornem necessária e imperativa a substituição da solução tecnológica.

6. MODELO DE EXECUÇÃO DO CONTRATO

6.1. Rotinas de Execução

6.1.1. Realização da Reunião Inicial

6.1.1.1. A CONTRATANTE convocará a CONTRATADA, imediatamente após a assinatura do CONTRATO, para reunião de alinhamento de entendimentos e expectativas – ora denominada REUNIÃO INICIAL – com o objetivo de:

6.1.1.1.1. Alinhar a forma de comunicação entre as partes, que deverá ocorrer preferencialmente entre o CONTRATANTE e o PREPOSTO da CONTRATADA.

6.1.1.1.2. Definir as providências necessárias para inserção da CONTRATADA no ambiente de prestação dos serviços.

6.1.1.1.3. Definir as providências de implantação dos serviços.

6.1.1.1.4. Alinhar entendimento quanto aos modelos de execução e de gestão do CONTRATO.

6.1.1.1.5. Emitir a ordem de serviço para fornecimento das licenças.

6.1.1.2. No decorrer da REUNIÃO INICIAL será apresentado à CONTRATADA o PLANO DE INSERÇÃO, documento que prevê as atividades de alocação de recursos necessários para a contratada iniciar o fornecimento da Solução de Tecnologia da Informação.

6.1.1.3. Havendo necessidade, outros assuntos de comum interesse poderão ser tratados na reunião inicial, além dos anteriormente previstos.

6.1.1.4. Reuniões de monitoramento dos serviços ou outras reuniões extraordinárias poderão ser convocadas pelo CONTRATANTE sendo obrigação da CONTRATADA atender às convocações.

6.1.1.5. Todas as atas de reuniões e as comunicações entre o CONTRATANTE e a CONTRATADA, assim como todas as demais intercorrências contratuais, positivas ou negativas, serão arquivadas em processo próprio para fins de manutenção do histórico de gestão do CONTRATO.

6.1.1.6. Na REUNIÃO INICIAL, a CONTRATADA deverá:

6.1.1.6.1. Apresentar seu PREPOSTO.

6.1.1.6.2. Entregar o **Termo de Ciência**, conforme descrito no Anexo do Termo de Referencia I-E, devidamente assinado por todos os funcionários que serão diretamente envolvidos na prestação dos serviços contratados.

6.1.1.6.3. Entregar o **Termo de Compromisso**, conforme descrito no Anexo do Termo de Referencia I-F, devidamente assinado pelo representante legal da contratada.

6.1.1.6.4. A CONTRATADA deverá apresentar os comprovantes de certificações e tempo de experiência dos profissionais que atuarão no projeto, conforme o tópico Requisitos de Formação da Equipe.

6.1.1.6.5. A CONTRATADA deverá apresentar declaração emitida pelo fabricante da solução ofertada onde comprova que ela está devidamente autorizada a comercializar, instalar, configurar e dar suporte técnico a seus produtos, especificamente para os produtos e serviços presentes para essa licitação. Na declaração deverá constar a data e número do presente pregão.

6.1.1.7. A CONTRATADA deverá apresentar declaração emitida pelo fabricante comprovando a descoberta de vulnerabilidades de dia zero considerando o prazo de até um ano antes da data de assinatura do contrato. Na declaração deverá constar a data da descoberta da vulnerabilidade, a descrição da vulnerabilidade e o link para averiguação da implementação na solução.

6.1.1.8. A CONTRATADA deverá, num prazo de até 5 (cinco) dias úteis, a partir da reunião inicial, apresentar Cronograma de Execução dos serviços, com as respectivas datas.

6.1.2. **Procedimentos para encaminhamento e controle de solicitações**

6.1.2.1. Item 1 e 3: será(ão) emitida(s) ordem(ns) de serviço com as licenças relacionadas e demais serviços/itens.

6.1.2.2. Item 1 e 3: Treinamento por profissional certificado pelo fabricante, será(ão) emitida(s) ordem(ns) de serviço para as turmas oferecidas.

6.1.2.3. Item 2 e 4: Serviço Técnico Especializado: deverão ser solicitados mediante a emissão de Ordem de Serviço (OS), conforme ANEXO I - B, por meio da qual será definido o escopo de atuação da CONTRATADA..

6.1.3. **Forma de execução e acompanhamento dos serviços**

6.1.3.1. A forma de execução e acompanhamento dos serviços devem ser desenvolvidas conforme o item níveis mínimos de serviços.

6.1.3.2. Para acompanhamento do conjunto de elementos que devem ser acompanhados pelos Fiscais do contrato durante a execução contratual, permitindo à Administração o registro e a obtenção de informações padronizadas e de forma objetiva, serão utilizados os itens que compõem o MODELO DE PLANO DE FISCALIZAÇÃO , conforme Anexo do Termo de Referência I-I.

6.1.4. **Prazos, horários de fornecimento de bens ou prestação dos serviços**

6.1.4.1. A atuação da CONTRATADA deverá ser preferencialmente em horário comercial.

6.1.4.2. De forma excepcional, é possível agendar atendimento fora deste período, ou seja, em horário não comercial a critério da CONTRATANTE, não extrapolando 25% do serviço contratado.

6.1.4.3. A execução de trabalhos em horário não comercial dar-se-á única e exclusivamente por solicitação da CONTRATANTE.

6.1.4.4. Uma mesma OS poderá conter várias atividades planejadas, sendo observadas as especificidades de cada atividade.

6.1.5. **Locais de entrega**

6.1.5.1. O fornecimento de licenças e os serviços serão executados nos locais apresentados na tabela 7.

Tabela 7 - Endereços

ÓRGÃO GERENCIADOR: MINISTÉRIO DA JUSTIÇA E SEGURANÇA PÚBLICA	
LOCALIZAÇÃO	**ENDEREÇO**
SEDE	Esplanada dos Ministérios, Palácio da Justiça, Bloco T, Edifício sede Sala 314 – CEP: 70064900 E-mail: crs@mj.gov.br Contato: Ivanildo de Oliveira da Silva JR
ÓRGÃO PARTÍCIPE: CADE	
LOCALIZAÇÃO	**ENDEREÇO**
SEDE	SEPN 515, Conjunto D, Lote 4, Edicio Carlos Taurisano, Bairro Asa Norte, Brasília/DF, CEP 70770-504 E-mail: vinicius.reis@cade.gov.br Contato: Vinicius Eloy dos Reis

6.1.6. Os endereços listados foram levantados no momento da elaboração do termo de referência e podem sofrer alterações até a execução do contrato. No decorrer do certame e, posteriormente, na execução do contrato, a contratada deverá validar tais localidades junto ao(s) Contratante(s).

6.1.7. **Papéis por parte da contratante e da contratada**

6.1.7.1. A fiscalização não exclui nem reduz a responsabilidade da CONTRATADA, inclusive perante terceiros, por qualquer irregularidade, ainda que resultante de imperfeições técnicas, vícios redibitórios, ou emprego de material inadequado ou de qualidade inferior e, na ocorrência desta, não implica em corresponsabilidade do CONTRATANTE ou de seus agentes e prepostos, de conformidade com o art. 70 da Lei nº 8.666, de 1993.

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

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

6.1.7.3.1. **Fiscal(is) Técnico(s):**

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

b) Identificar não conformidade com os termos contratuais;

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

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

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

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

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

h) Promover o registro das ocorrências verificadas, adotando as providências necessárias ao fiel cumprimento das cláusulas contratuais.

6.1.7.3.2. **Fiscal(is) Administrativo(s):**

a) Verificar aderência aos termos contratuais;

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

6.1.7.3.3. **Fiscal(is) Requisitante(s):**

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

b) Identificar não conformidades com os termos contratuais;

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

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

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

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

6.1.7.3.4. **Gestor do Contrato:**

a) Promover a realização da reunião inicial;

b) Encaminhar a indicação de sanções para a Área Administrativa;

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

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

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

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

g) Manter registro de aditivos;

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

i) Encaminhar à CONTRATADA deficiências;

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

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

l) Os fiscais comunicarão, por escrito, as deficiências porventura verificadas no fornecimento, para imediata correção, sem prejuízo das sanções e glosas cabíveis.

6.1.7.4. **Preposto:**

a) representante da contratada, responsável por acompanhar a execução do contrato;

b) atuar como interlocutor principal junto à contratante, incumbido de receber, diligenciar, encaminhar e responder as principais questões técnicas, legais e administrativas referentes ao andamento contratual.

6.1.8. **Formas de transferência de conhecimento**

6.1.8.1. A transferência de conhecimento será garantido logo após a assinatura do contrato, com o treinamento incluído nos itens 1 e 3 e deverá manter-se constante até a finalização do contrato.

6.1.9. **Procedimentos de transição e finalização do contrato**

6.1.10. Os procedimentos de transição e o encerramento do contrato deverão observar as atividades e prazos da Tabela 8.

Tabela 8 - Atividades e prazos para a transição e encerramento do contrato.

Atividade ou Produto	Responsável	Prazo
1. Elaborar artefatos para nova contratação do mesmo objeto	CONTRATANTE	180 dias do encerramento contratual
2. Elaborar e entregar o Plano de Transição Contratual	CONTRATADA	120 dias do encerramento contratual
3. Entregar todo o conhecimento desenvolvido que deverá ser repassado à Contratada/Nova empresa	CONTRATADA	30 dias do encerramento contratual
4. Convocar reunião de encerramento/transição contratual	CONTRATANTE	10 dias do encerramento contratual
5. Realizar reunião de encerramento/transição contratual	CONTRATANTE e CONTRATADA	5 dias do encerramento contratual
6. Elaborar Termo de Recebimento Definitivo do Contrato	CONTRATANTE	1 dia após o encerramento definitivo do contrato
TOTAL		180 dias

6.1.11. No encerramento do contrato os responsáveis por sua gestão deverão elaborar e instruir o processo administrativo com um relatório final acerca das ocorrências da fase de execução contratual, a ser utilizado como fonte de informações para as futuras contratações, encaminhando-o à CGL para as devidas providências de encerramento de contrato.

6.2. **Quantidade mínima de bens ou serviços para comparação e controle**

6.2.1. A Quantidade mínima de bens ou serviços para comparação e controle estão relacionadas no item Prazos, horários de fornecimento de bens ou prestação dos serviços.

6.3. **Mecanismos formais de comunicação**

6.3.1. O modelo de prestação de serviços prevê que a Contratada seja integralmente responsável pela gestão de seu pessoal em todos os aspectos, sendo vedado à equipe do contratante, formal ou informalmente, qualquer tipo de ingerência ou influência sobre a administração da mesma, ou comando direto sobre seus empregados, fixando toda negociação na pessoa do preposto da Contratada ou seu substituto.

6.3.2. São instrumentos formais de comunicação entre a Contratante e a Contratada:

a) Ordem de Serviço (OS);

b) Plano de Inserção;

c) Termos de Recebimento;

d) Termo de Encerramento de OS;

e) Ofício;

f) Ata de Reunião;

g) Relatório;

h) Carta;

i) E-mail institucional/corporativo;

j) Ferramenta Web para registro de chamados.

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

6.3.4. A formalização dos documentos, a intimação e a notificação ao particular, bem como peticionamento de documentos serão realizados, preferencialmente, por meio do sistema SEI!

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

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

6.4.2. O Termo de Compromisso (anexo I - F), contendo declaração de manutenção de sigilo e respeito às normas de segurança vigentes na entidade, deverá ser assinado pelo representante legal da Contratada.

6.4.3. O Termo de Ciência (Anexo I - E), deverá a ser assinado por todos os empregados da CONTRATADA diretamente envolvidos na contratação.

7. MODELO DE GESTÃO DO CONTRATO

7.1. Critérios de aceitação

7.1.1. Visando atender ao padrão de qualidade dos serviços exigidos pelo CONTRATANTE, a CONTRATADA deverá:

7.1.1.1. Prestar os serviços dentro dos parâmetros e rotinas estabelecidos, com observância às recomendações aceitas pela boa técnica, normas e legislação, bem como observar conduta adequada na utilização dos materiais, equipamentos e ferramentas.

7.1.1.2. Fiscalizar regularmente os seus recursos técnicos designados para a prestação dos serviços verificando as condições em que as atividades estão sendo realizadas.

7.1.1.3. Refazer todos os serviços que, a juízo do representante do CONTRATANTE, de forma fundamentada, não forem considerados satisfatórios, sem que caiba qualquer acréscimo no custo contratado, independentemente das penalidades previstas.

7.1.1.4. Executar fielmente o objeto contratado de acordo com as normas legais, em conformidade com a proposta apresentada e com as orientações do CONTRATANTE, observando sempre os critérios de qualidade.

7.1.1.5. Adequar a redação de documentos e relatórios quanto à clareza, objetividade, detalhamento técnico e conformidade com as boas práticas e normas aplicáveis.

7.1.1.6. Caso os produtos entregues estejam fora dos padrões de qualidade será exigida a readequação dos mesmos, sem prejuízo das penalidades aplicáveis.

7.1.1.7. Serão pagos à CONTRATADA os serviços efetivamente prestados, considerando-se o atendimento aos requisitos de disponibilidade e os níveis mínimos de serviço exigidos para esta contratação. Do valor total dos serviços prestados, o CONTRATANTE descontará valor referente aos redutores de pagamento para se chegar ao valor total que deverá constar na nota fiscal emitida pela CONTRATADA. Serão pagos os serviços prestados mediante pareceres favoráveis da equipe de fiscalização do contrato, e também mediante a apresentação dos documentos comprobatórios de conformidade comercial, fiscal e trabalhista, apresentados pela CONTRATADA.

7.1.2. Os descumprimentos poderão implicar em glosas cumulativas.

7.1.3. A partir da segunda glosa poderá haver encaminhamento para análise e aplicação de sanção.

7.1.4. Os serviços serão executados conforme discriminado neste Termo de Referência e anexos.

7.2. Procedimentos de Teste e Inspeção

7.2.1. O acompanhamento e a fiscalização da execução do Contrato serão realizados por servidores da CONTRATANTE, em atendimento ao disposto no Art. 67 da Lei 8.666/93, designados como Fiscais do Contrato, os quais obedecerão às disposições de normas e resoluções internas do órgão, bem assim ao contido no artigo 29 da INSTRUÇÃO NORMATIVA Nº 1 da SGD/ME, de 04 de abril de 2019.

7.3. Níveis mínimos de serviços exigidos

7.3.1. Os serviços deverão ser executados com base no Item níveis mínimos de serviço exigidos.

7.3.2. O descumprimento total ou parcial das demais obrigações e responsabilidades assumidas pela CONTRATADA ensejará a aplicação de sanções administrativas, previstas neste Termo de Referência e na legislação vigente, podendo culminar em rescisão contratual, conforme disposto nos artigos 77 e 87 da Lei nº 8.666, de 1993.

7.3.3. **Para os itens 1 e 3:**

7.3.3.1. As licenças deverão ser fornecidas no prazo de até 15 dias úteis após a assinatura do contrato. A não disponibilização no prazo determinado poderá resultar nas sanções previstas no presente instrumento.

7.3.3.2. O Chamado técnico, que poderá ser remoto, consiste na prestação de serviço especializado para resolução de problemas, de mau funcionamento e ajustes em sua configuração e é uma obrigação assessória do licenciamento das ferramentas.

7.3.3.3. O serviço de chamado técnico deverá contemplar todos os programas ou produtos fornecidos para atendimento dos requisitos do edital.

7.3.3.4. A CONTRATADA deverá prover um mecanismo de abertura e acompanhamento de chamado através de sistema em site on-line, email e por telefone. Para acesso a este site, serão fornecidas ao órgão todas as informações necessárias para ingresso no sistema, inclusive senhas de uso exclusivo.

7.3.3.5. A CONTRATADA deve disponibilizar um mecanismo de abertura e acompanhamento de chamado técnico através de sistema em site on-line, email e por telefone. A CONTRATADA deverá ofertar ferramenta de gestão de chamados.

7.3.3.6. A CONTRATANTE abrirá um chamado técnico para cada problema reportado, sendo iniciada a contagem do tempo de atendimento a partir da hora de acionamento.

7.3.3.7. Na abertura de chamados técnicos, serão fornecidas informações de identificação do produto, anormalidade observada, nome do responsável pela solicitação do serviço, prioridade do chamado e demais informações conforme o modelo de RELATÓRIO DE CHAMADO TÉCNICO – RCTA, disponível no anexo I-C.

7.3.3.8. Os serviços de atualização de licenças deverão ser realizados nas instalações do Órgão ou remotamente, no prazo máximo de 15 dias a contar da divulgação de nova versão, salvo as exceções permitidas sob a anuência do órgão, sem ônus adicional para o CONTRATANTE.

7.3.3.9. A CONTRATADA deve fornecer, para cada chamado técnico aberto, um número único de registro para acompanhamento pela CONTRATANTE.

7.3.3.10. Na ocorrência de uma situação emergencial, em que já exista chamado técnico aberto, é esperado que tanto o atendimento quanto o restabelecimento do serviço sejam feitos de forma imediata, sem a necessidade de abertura de novo chamado.

7.3.3.11. Todos os serviços serão prestados esperando-se a aplicação das melhores práticas e recomendações do mercado e do fabricante.

7.3.3.12. A forma de atendimento dos chamados técnicos poderá ser remota ou presencial. No caso de atendimento remoto, a CONTRATADA deve informar por e-mail ao fiscal técnico do contrato, assim que o atendimento for iniciado, e após sua conclusão, contendo evidências das atividades executadas.

7.3.3.13. Os chamados técnicos somente deverão ser encerrados após expressa anuência do Gestor do Contrato ou do Fiscal Técnico.

7.3.3.14. Para o fechamento do chamado devem ser relacionadas as evidências de seu atendimento, diagnóstico e solução do problema tais como imagens de tela, fotos e registros gerados pelos equipamentos e demais informações conforme o modelo de RELATÓRIO DE CHAMADO TÉCNICO – RCTA, disponível no anexo I-C.

7.3.3.15. Os critérios definidos nas tabelas Critério do Impacto e Critério da Urgência são balizadores para a categorização dos chamados.

7.3.3.16. A partir das classificações de impacto e urgência, e do cruzamento destas informações, é determinada a prioridade de cada chamado, de acordo com a tabela de Matriz de Definição da Prioridade no Atendimento.

7.3.3.17. A cada valor de prioridade entre um e quatro está associado um nível de serviço relativo ao tempo de início de atendimento e ao tempo total para a solução.

7.3.3.18. Na tabela 9 estão relacionados os critérios para definição do impacto dos chamados técnicos.

Tabela 9 - Critério do Impacto

Impacto	**Fatos Determinantes**
Alto	· Qualquer incidente relativo à indisponibilidade ou mau funcionamento generalizado da solução. · Qualquer incidente ou requisição reportado pela equipe de fiscalização. · A falha impossibilita o trabalho diário de um ou mais usuários (ex. emissão de relatório de vulnerabilidades, indisponibilidade da estação de trabalho do usuário quando escaneada pela ferramenta). · O serviço fornecido está operacional, mas apresenta algumas funções principais, ou partes delas, com erros, provocando assim uma queda na qualidade do trabalho normal.
Médio	· A falha afeta o trabalho diário de um ou mais usuários. · O serviço de uso coletivo encontra-se operando de modo normal, mas algumas funções secundárias apresentam falhas ou lentidão. · Trata-se de chamado técnico cujo não atendimento imediato impeça o trabalho principal do usuário.
Baixo	· O serviço apresenta falha, mas por necessidade do usuário não há possibilidade de intervenção imediata ou de paralisação. · O chamado pode ser atendido em algum horário posterior sem que haja prejuízo do desempenho das atividades do usuário.

7.3.3.19. Na tabela 10 estão relacionados os critérios para definição da urgência dos chamados técnicos.

Tabela 10 - Critério da Urgência

Urgência	**Fatos Determinantes**
Alta	O serviço precisa ser restabelecido imediatamente. O sistema ou recurso é crítico ou sensível. Qualquer incidente ou requisição reportado pela equipe de fiscalização. O serviço precisa ser restabelecido o mais rápido possível.
Média	O equipamento ou o serviço deve ser restabelecido assim que possível.
Baixa	Por necessidade do cliente não há possibilidade de intervenção imediata. O serviço pode ser agendado para uma data específica, a posteriori.

7.3.3.20. A tabela 11 apresenta a Matriz de Definição da Prioridade no Atendimento, em Função do Impacto e da Urgência.

Tabela 11 - Matriz de Definição da Prioridade no Atendimento

IMPACTO	URGÊNCIA		
	BAIXA	MÉDIA	ALTA
ALTO	2	1	1
MÉDIO	3	3	2
BAIXO	4	3	2

7.3.3.21. As classificações de "impacto" e "urgência" poderão ser revistas, de acordo com a necessidade da CONTRATANTE. Sempre que o atendimento do serviço puder ser agendado para data posterior, ele deverá ter o "impacto" e a "urgência" definidos como "baixos", e deverá ser definido um prazo para sua execução conforme regra deste Termo de Referência.

7.3.3.22. O Tempo Máximo para Solução do Chamado (TMSC) é o tempo máximo para a resolução de um chamado, contado do momento do registro do chamado até o encerramento no sistema.

7.3.3.23. Os prazos máximos para solução dos chamados técnicos, de acordo com o nível de prioridade de atendimento, estão descritos na Tabela 12.

Tabela 12 - Tempo Máximo por Prioridade de Atendimento

Prioridade	Chamado Técnico
	Tempo Máximo para Solução do Chamado (TMSC)
1	Em até 2 horas
2	Em até 4 horas
3	Em até 8 horas
4	Em até 24 horas

7.3.3.24. Para o descumprimento dos níveis de serviços dos chamados técnicos que possam impactar na solução contratada serão aplicadas as sanções previstas no presente instrumento.

7.3.3.25. No caso de reiterados descumprimentos, a partir de 3 (três) vezes, de níveis de serviços de impacto alto e urgência média, poderá, a critério da administração, configurar nessa hipótese, descumprimento parcial da obrigação assumida.

7.3.3.26. Após 36 (trinta e seis) horas de atraso e a critério da Administração, no caso de execução com atraso, poderá configurar, nessa hipótese, inexecução total da obrigação assumida, sem prejuízo da rescisão unilateral da avença.

7.3.3.27. Somente serão aceitas justificativas para o não atendimento a um chamado técnico, caso o fato seja gerado por motivo de força maior ou por dependência do Ministério da Justiça e Segurança Pública. Neste caso, a CONTRATADA deve formalizar antecipadamente ao Gestor do Contrato ou ao Fiscal Técnico os motivos que impedem a execução do serviço.

7.3.3.28. Caso o tempo de parada da solução (downtime) seja superior 7,3 (sete vírgula três) horas por mês serão aplicadas as sanções previstas no presente instrumento.

7.3.4. **Para os itens 1 e 3: Treinamento por profissional certificado pelo fabricante**:

7.3.4.1. O treinamento deverá ser avaliado pelos participantes de acordo com o modelo de avaliação apresentado no anexo I-K.

7.3.4.2. Ao término do treinamento o instrutor deverá informar aos participantes, que preencham a avaliação, exigência necessária para obtenção do certificado.

7.3.4.3. O certificado de participação do curso deverá ser fornecido após o preenchimento da ficha de avaliação.

7.3.4.4. A avaliação deverá ser disponibilizada pelo CONTRATANTE à CONTRATADA, em formato eletrônico ou impresso para preenchimento dos participantes.

7.3.4.4.1. Caso seja utilizado o formato impresso, a contratada deverá entregar as fichas de avaliação preenchidas ao contratante, no mesmo dia.

7.3.4.5. O treinamento somente será considerado aceito pela fiscalização quando:

7.3.4.5.1. A média das avaliações de todos os participantes for maior ou igual a 60%.

7.3.4.5.2. O certificado de conclusão for entregue aos participantes.

7.3.4.6. A contratada será notificada acerca do resultado das avaliações do treinamento, em até 3 (três) dias úteis após o recebimento das avaliações pela equipe de fiscalização.

7.3.4.7. Caso o resultado das avaliações seja inferior a 60%:

7.3.4.7.1. A CONTRATADA deverá realizar um segundo treinamento sem ônus adicional.

7.3.4.7.2. A CONTRATADA deverá reformular o curso de acordo com a CONTRATANTE, podendo inclusive substituir o instrutor, caso solicitado.

7.3.5. **Para os itens 2 e 4, Serviço Técnico Especializado:**

7.3.5.1. As horas de serviço técnico especializado deverão ser solicitadas mediante a emissão de uma Ordem de Serviço (OS), conforme ANEXO I - B, por meio da qual será definido o escopo de atuação da CONTRATADA.

7.3.5.2. Os serviços técnicos especializados são aqueles com os quais a CONTRATANTE poderá realizar melhorias no ambiente inicialmente implementado, a partir do aproveitamento dos conhecimentos da CONTRATADA nas soluções fornecidas.

7.3.5.3. A quantidade de horas prevista na OS deverá ser objeto de acordo entre a CONTRATANTE e CONTRATADA de acordo com a complexidade do serviço a ser executado.

7.3.5.4. Para o agendamento de atuação presencial da CONTRATADA, deverá ser respeitada a antecedência mínima de 2 (dois) dias úteis entre a data de emissão da OS e a data prevista para a execução dos serviços.

7.3.5.5. Para o agendamento de atuação remota da CONTRATADA, deverá ser respeitada a antecedência mínima de 1 (um) dia útil entre a data de emissão da OS e a data prevista para a execução dos serviços.

7.3.5.6. Para os casos em que a atuação da CONTRATADA seja remota e presencial, as antecedências previstas anteriormente devem ser observadas de acordo com cada tipo de atividade planejada.

7.3.5.7. Os prazos acima estipulados podem ser encurtados de comum acordo entre CONTRATANTE e CONTRATADA.

7.3.5.8. A medição será realizada compreendendo o período entre a emissão da ordem de serviço e o último dia do cronograma constante da ordem de serviço.

7.3.5.9. O Relatório de encerramento da Ordem de Serviço deverá ser emitido pelo preposto da CONTRATADA, contendo no mínimo:

a) Identificação do Relatório de Atividades;

b) Data de Emissão;

c) Número do Contrato;

d) Mês/Ano de Referência;

e) Data e hora de início de serviços;

f) Item;

g) Descrição dos serviços executados;

h) Quantidade de horas;

i) Data e hora de encerramento de serviços;

j) Demais anotações que se fizerem pertinentes;

k) Poderão ser solicitados outros itens de verificação além dos informados acima.

7.3.5.9.1. Deverá ser elaborado em língua portuguesa obedecendo a norma culta padrão e entregue ao CONTRATANTE após a execução do serviço.

7.3.5.9.2. Como critério de conformidade, a letra "g" do item 7.3.5.9 será considerada como parâmetro para avaliação e aceitação do serviço, com as respectivas evidências, o qual será comparado com os serviços a executar descritos na Ordem de Serviço (Anexo I-B Modelo de Ordem de Serviço - O.S (doc. Sei 14648174).

7.3.5.9.3. Como critério de aceitação do serviço será considerado o Índice de qualidade do relatório conforme os parâmetros definidos no item 7.3.5.9 - Relatório de encerramento da Ordem de Serviço.

7.3.5.9.4. A forma de cálculo do índice será dada como a soma das inconformidades identificadas, a unidade de medida será a quantidade de inconformidades e a meta exigida será 0 (zero).

7.3.5.9.5. Quando da ocorrência de qualquer inconformidade de itens mínimos ou dos critérios supramencionados, poderá ocorrer a não-aceitação do objeto, devendo a contratada sanar as inconformidades apontadas dentro do prazo acordado inicialmente.

7.3.6. Para a Ordem de Serviço que ultrapassar o prazo previsto para entrega do serviço, a cada 24 horas de atraso, será aplicado, glosa de 1,0% sobre o valor da Ordem de Serviço, limitada a incidência a 360(trezentos e sessenta) horas, ou seja, 15% (quinze) por cento de glosa. Após o limite estabelecido e a critério da Administração, no caso de execução com atraso, poderá ocorrer a não-aceitação do objeto, de forma a configurar, nessa hipótese, inexecução total da obrigação assumida, sem prejuízo da rescisão unilateral da avença.

7.3.7. Em caso de atraso na execução superior ao previsto no subitem acima, caso haja aceitação do objeto será considerada inexecução parcial da obrigação assumida.

7.4. **Sanções administrativas e procedimentos para retenção no pagamento**

7.4.1. Comete infração administrativa nos termos da Lei nº 10.520, 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 Administração pode aplicar à CONTRATADA as seguintes sanções:

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

7.4.2.2. Multa de:

7.4.2.2.1. 0,1% (um décimo por cento) por dia sobre o valor adjudicado do item em caso de atraso na execução dos serviços, limitada a incidência a 15 (quinze) dias. Após o décimo quinto dia e a critério da Administração, no caso de execução com atraso, poderá ocorrer a não-aceitação do objeto, de forma a configurar, nessa hipótese, inexecução total da obrigação

assumida, sem prejuízo da rescisão unilateral da avença;

7.4.2.2.2. 10% (dez por cento) sobre o valor adjudicado do item, em caso de atraso na execução do objeto, por período superior ao previsto no subitem acima, ou de inexecução parcial da obrigação assumida;

7.4.2.2.3. 15% (quinze por cento) sobre o valor adjudicado do item, em caso de inexecução total da obrigação assumida;

7.4.2.2.4. 0,01% a 1,6% por HORA ou DIA, conforme detalhamento constante das **tabelas 13 e 14**, abaixo; e

7.4.2.2.5. 0,07% (sete centésimos por cento) do valor do contrato por dia de atraso na apresentação da garantia (seja para reforço ou por ocasião de prorrogação), observado o máximo de 2% (dois por cento). O atraso superior a 25 (vinte e cinco) dias autorizará a Administração CONTRATANTE a promover a rescisão do contrato;

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

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

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

7.4.2.4.1. A Sanção de impedimento de licitar e contratar prevista neste subitem também é aplicável em quaisquer das hipóteses previstas como infração administrativa no subitem 7.4.1 deste Termo de Referência.

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

7.4.2.6. As sanções previstas nos subitens 7.4.2.1, 7.4.2.3, 7.4.2.4 e 7.4.2.5 poderão ser aplicadas à CONTRATADA juntamente com as de multa, descontando-a dos pagamentos a serem efetuados.

7.4.2.7. Para efeito de aplicação de multas, às infrações são atribuídos graus, de acordo com as tabelas 13 e 14:

Tabela 13 - Gradação das multas

GRAU	**CORRESPONDÊNCIA**
1	0,1% ao dia sobre o valor da ordem de serviço, limitado a incidência de 15 (quinze) dias.
2	0,2% ao dia sobre o valor da ordem de serviço, limitado a incidência de 15 (quinze) dias.
3	0,3% ao dia sobre o valor da ordem de serviço, limitado a incidência de 15 (quinze) dias.
4	1,6% ao dia sobre o valor da ordem de serviço, limitado a incidência de 15 (quinze) dias.
5	0,01% (um centésimo por cento) por hora sobre o valor adjudicado para o item, em caso de atraso na execução do chamado, limitada a incidência a 0,36% (trinta e seis centésimos por cento), ou seja, 36 (trinta e seis) horas.
6	1% (um por cento), por ocorrência, sobre o valor adjudicado para o item, limitada a incidência de 5% (cinco por cento).

Tabela 14 - Infrações

INFRAÇÃO		
Item do contrato	**DESCRIÇÃO**	**GRAU**
2 e 4	Suspender ou interromper, salvo motivo de força maior ou caso fortuito, os serviços contratuais por dia e por unidade de atendimento.	04
2 e 4	Manter funcionário sem qualificação para executar os serviços contratados, por empregado e por dia.	03
2 e 4	Recusar-se a executar serviço determinado pela fiscalização, por serviço e por dia.	02
1 e 3	Ultrapassar o limite máximo de tempo definido para o Chamado Técnico, de acordo o nível de serviço.	05
1 e 3	Ultrapassar o tempo de parada (downtime) de 7,3 (sete vírgula três) horas por mês.	06
Para os itens a seguir, deixar de:		
2 e 4	Cumprir determinação formal ou instrução complementar do órgão fiscalizador, por ocorrência.	02
1 e 3	Cumprir determinação formal ou instrução complementar do órgão fiscalizador, por ocorrência.	06

2 e 4	Substituir empregado que se conduza de modo inconveniente ou não atenda às necessidades do serviço, por funcionário e por dia.	01
2 e 4	Cumprir quaisquer dos itens do Edital e seus Anexos não previstos nesta tabela de multas, após reincidência formalmente notificada pelo órgão fiscalizador, por item e por ocorrência.	03
1 e 3	Cumprir quaisquer dos itens do Edital e seus Anexos não previstos nesta tabela de multas, após reincidência formalmente notificada pelo órgão fiscalizador, por item e por ocorrência.	06
1, 2, 3 e 4	Indicar e manter durante a execução do contrato os prepostos previstos no edital/contrato.	06
1 e 3	Apresentar declaração do fabricante que comprove a descoberta de vulnerabilidades de dia zero considerando o prazo de até um ano antes da data de assinatura do contrato.	06

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.

7.4.5.1. Caso a Contratante determine, a multa deverá ser recolhida no prazo máximo de 15 (quinze) dias, a contar da data do recebimento da comunicação enviada pela autoridade competente.

7.4.6. 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.

7.4.7. 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.

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

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

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

7.4.11. As penalidades serão obrigatoriamente registradas no SICAF.

7.5. **Do Pagamento**

7.5.1. A emissão da Nota Fiscal/Fatura deve ser precedida do termo de recebimento definitivo dos serviços, nos termos abaixo.

7.5.1.1. No prazo de até 5 (cinco) dias corridos do adimplemento da parcela, a CONTRATADA deverá entregar toda a documentação comprobatória do cumprimento da obrigação contratual.

7.5.1.2. O recebimento provisório será realizado pelo fiscal técnico e setorial ou pela equipe de fiscalização após a entrega da documentação acima, da seguinte forma:

7.5.1.2.1. A CONTRATANTE realizará inspeção minuciosa de todos os serviços executados, por meio de profissionais técnicos competentes, acompanhados dos profissionais encarregados pelo serviço, com a finalidade de verificar a adequação dos serviços e constatar e relacionar os arremates, retoques e revisões finais que se fizerem necessários.

7.5.1.2.2. Para efeito de recebimento provisório, ao final de cada período de faturamento, o fiscal técnico do contrato irá apurar o resultado das avaliações da execução do objeto e, se for o caso, a análise do desempenho e qualidade da prestação dos serviços realizados em consonância com os indicadores previstos, que poderá resultar no redimensionamento de valores a serem pagos à contratada, registrando em relatório a ser encaminhado ao gestor do contrato.

7.5.1.2.3. A CONTRATADA fica obrigada a reparar, corrigir, remover, reconstruir ou substituir, às suas expensas, no todo ou em parte, o objeto em que se verificarem vícios, defeitos ou incorreções resultantes da execução ou materiais empregados, cabendo à fiscalização não atestar a última e/ou única medição de serviços até que sejam sanadas todas as eventuais pendências que possam vir a ser apontadas no

Recebimento Provisório.

7.5.1.3. O recebimento provisório também ficará sujeito, quando cabível, à conclusão de todos os testes de campo e à entrega dos Manuais e Instruções exigíveis.

7.5.1.4. No prazo de até 10 *dias úteis* a partir do recebimento dos documentos da CONTRATADA, cada fiscal ou a equipe de fiscalização deverá elaborar Relatório Circunstanciado em consonância com suas atribuições, e encaminhá-lo ao gestor do contrato.

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

7.5.1.4.2. Será considerado como ocorrido o recebimento provisório com a entrega do relatório circunstanciado ou, em havendo mais de um a ser feito, com a entrega do último.

7.5.1.4.2.1. Na hipótese de a verificação a que se refere o item anterior não ser procedida tempestivamente, reputar-se-á como realizada, consumando-se o recebimento provisório no dia do esgotamento do prazo.

7.5.1.5. No prazo de até *10 (dez) dias úteis* a partir do recebimento provisório dos serviços, o Gestor do Contrato deverá providenciar o recebimento definitivo, ato que concretiza o ateste da execução dos serviços, obedecendo as seguintes diretrizes:

7.5.1.5.1. Realizar a análise dos relatórios e de toda a documentação apresentada pela fiscalização e, caso haja irregularidades que impeçam a liquidação e o pagamento da despesa, indicar as cláusulas contratuais pertinentes, solicitando à CONTRATADA, por escrito, as respectivas correções;

7.5.1.5.2. Emitir Termo Circunstanciado para efeito de recebimento definitivo dos serviços prestados, com base nos relatórios e documentações apresentadas; e

7.5.1.5.3. Comunicar a empresa para que emita a Nota Fiscal ou Fatura, com o valor exato dimensionado pela fiscalização.

7.5.2. O recebimento provisório ou definitivo do objeto não exclui a responsabilidade da CONTRATADA pelos prejuízos resultantes da incorreta execução do contrato, ou, em qualquer época, das garantias concedidas e das responsabilidades assumidas em contrato e por força das disposições legais em vigor.

7.5.3. 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 corrigidos/refeitos/substituídos no prazo fixado pelo fiscal do contrato, às custas da CONTRATADA, sem prejuízo da aplicação de penalidades.

7.5.4. 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:

a) não produziu os resultados acordados;

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

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

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

7.5.6. Para fins de cálculos serão considerados até dois dígitos após a vírgula decimal.

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

7.5.8. 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.

7.5.9. 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.

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

7.5.11. o prazo de validade;

a) a data da emissão;

b) os dados do contrato e do órgão contratante;

c) o período de prestação dos serviços;

d) o valor a pagar; e

e) eventual destaque do valor de retenções tributárias cabíveis.

7.5.12. Havendo erro na apresentação da Nota Fiscal/Fatura, ou circunstância que impeça a liquidação da despesa, 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 o CONTRATANTE.

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

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

7.5.15. 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.

7.5.16. 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.

7.5.17. 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.

7.5.18. 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.

7.5.19. 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.

7.5.19.1. 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.

7.5.20. Quando do pagamento, será efetuada a retenção tributária prevista na legislação aplicável, em especial a prevista no artigo 31 da Lei 8.212, de 1993, nos termos do item 6 do Anexo XI da IN SEGES/MP n. 5/2017, quando couber.

7.5.20.1. Considerando que a prestação dos serviços será realizada em Brasília, com o intuito de evitar quaisquer problemas no momento do pagamento, no que diz respeito ao recolhimento de tributos, sugere-se que, caso a empresa vencedora da licitação não seja domiciliada em Brasília, providencie seu Cadastro Fiscal do Distrito Federal, antes da emissão da Nota Fiscal.

7.5.20.2. Visando manter a segurança jurídica durante o procedimento licitatório e segundo a Lei Complementar nº 116, de 31 de julho de 2003, o ISS é devido no local onde se situa o estabelecimento do prestador, salvo nos casos previstos na Lei Complementar. O Decreto nº 25.508, de 19 de janeiro de 2005 (RISS-DF), caracteriza estabelecimento como "o local, público ou privado, edificado ou não, próprio ou de terceiro, onde o contribuinte desenvolva a atividade de prestar serviços, de modo permanente ou temporário, e que configure unidade econômica ou profissional, sendo irrelevantes para caracterizá-lo as denominações de sede, filial, agência, posto de atendimento, sucursal, escritório de representação ou contato ou quaisquer outras que venham a ser utilizadas." É considerado "unidade econômica ou profissional, para os efeitos deste artigo, a existência de um dos seguintes elementos: I - pessoal, material, máquinas, instrumentos e/ou equipamentos necessários à execução dos serviços; II - estrutura organizacional ou administrativa; III - inscrição nos órgãos previdenciários, fazendários, fiscalizadores de exercício profissional, nos cartórios ou na Junta Comercial; IV - permanência ou ânimo de permanecer no local, para exploração econômica de atividade de prestação de serviços, exteriorizados pela indicação do endereço em impressos, formulários ou correspondência, em contrato de locação de imóvel, propaganda ou publicidade, ou em conta de telefone, de fornecimento de energia elétrica ou água, em nome do prestador, seu representante ou preposto. Logo, se o contratado prestar seus serviços in loco dentro do território do DF, ele sofrerá a retenção de ISS relativo ao serviço aqui prestado por caracterizar unidade econômica profissional.

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

7.5.22. 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 fórmula da tabela 15.

Tabela 15 - Cálculo para eventuais atrasos

$EM = I \times N \times P$
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, no valor de 0,00016438, assim apurado:
$I = (6\%) / 365$
Sendo:
6% = Percentual da taxa anual

7.6. **Do Controle e Fiscalização do Contrato**

7.6.1. Caberá à equipe de fiscalização do contrato acompanhar o cumprimento do prazo para apresentação dos documentos comprobatórios quanto à obrigação prevista no na portaria 513 do MJSP (15531434).

7.6.2. Após análise da conformidade das informações, a equipe de fiscalização do contrato deverá dar ciência à unidade do Ministério da Justiça e Segurança Pública responsável pelo Programa

de Integridade e à empresa contratada.

7.6.3. Em caso de descumprimento da obrigação de apresentar o Programa de Integridade dentro dos prazos estabelecidos, a equipe de fiscalização deverá tomar as providências cabíveis para a aplicação de penalidade à empresa contratada.

7.6.4. Após a implementação ou adequação do Programa de Integridade pela contratada, a equipe de fiscalização deverá realizar acompanhamento da execução do programa, por meio do relatório encaminhado pela empresa contratada, semestralmente.

7.6.5. Em caso de descumprimento do envio do relatório semestral, a equipe de fiscalização deverá notificar a empresa contratada e proceder com o registro do ocorrido.

8. ESTIMATIVA DE PREÇOS DA CONTRATAÇÃO

8.1. O valor total estimado da presente contratação é de R$ 9.315.109,66 (nove milhões, trezentos e quinze mil cento e nove reais e sessenta e seis centavos), sendo R$ 6.269.942,51 (seis milhões, duzentos e sessenta e nove mil novecentos e quarenta e dois reais e cinquenta e um centavos) do Ministério da Justiça e Segurança Pública e R$ 3.045.167,15 (três milhões, quarenta e cinco mil cento e sessenta e sete reais e quinze centavos) do Conselho Administrativo de Defesa Econômica - CADE.

8.2. No valor 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.

9. ADEQUAÇÃO ORÇAMENTÁRIA E CRONOGRAMA FÍSICO-FINANCEIRO

9.1. As despesas decorrentes da presente contratação correrão à conta da Dotação Orçamentária da União, conforme detalhamento a seguir:

9.1.1. Programa de Trabalho: 04122003220000001

9.1.2. Natureza da Despesa: 339040.06 (Itens 1 e 3 - Subscrição de software) e 339035.04 (Itens 2 e 4 - Serviço Técnico Especializado em TIC)

9.1.3. Plano Interno (PI): GL67OTCGLTI

9.1.4. Plano de Trabalho Resumido (PTRES): 172184

9.1.5. Fonte: 0100

9.1.6. Ação: 2000

9.1.7. Plano Orçamentário (PO): 000C

10. DA VIGÊNCIA DO CONTRATO

10.1. O prazo de vigência do Contrato é de 24 (vinte e quatro) meses, podendo ser prorrogado por interesse das partes até o limite de 48 (quarenta e oito) meses, com base no artigo 57, IV, da Lei 8.666, de 1993.

10.2. Quanto a prorrogação do contrato, poderá ser prorrogado por interesse das partes, desde que haja autorização formal da autoridade competente e observados os seguintes requisitos:

10.2.1. Os serviços tenham sido prestados regularmente;

10.2.2. A Administração mantenha interesse na realização do serviço;

10.2.3. O valor do Contrato permaneça economicamente vantajoso para a Administração; e

10.2.4. A CONTRATADA manifeste expressamente interesse na prorrogação.

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

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

11. DO REAJUSTE DE PREÇOS

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

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

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

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

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

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

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

11.8. O reajuste será realizado por apostilamento.

12. DOS CRITÉRIOS DE SELEÇÃO DO FORNECEDOR

12.1. **Regime, tipo e Modalidade de Licitação**

12.1.1. Regime

12.1.1.1. O regime de execução será a de empreitada por preço unitário.

12.1.2. Tipo

12.1.2.1. O tipo de licitação será a de menor preço por grupo - quando o critério de seleção da proposta mais vantajosa para a Administração determinar que será vencedor o

licitante que apresentar a proposta de acordo com as especificações do edital e ofertar o menor preço.

12.1.3. Modalidade

12.1.4. Será adotada a licitação na modalidade de pregão.

12.2. **Justificativa para aplicação do Direito de Preferência e Margens de Preferência**

12.2.1. Em virtude da justificativa técnica de agrupamento dos itens da presente licitação, bem como de seu valor estimado, não haverá destinação de item ou cota exclusiva para as micro e pequenas empresas.

12.3. **Critérios de qualificação Técnica e Habilitação**

12.3.1. **Grupo 1 - item 1**: No mínimo, 1 (um) Atestado de Capacidade Técnica, fornecido por pessoa jurídica de direito público ou privado, comprovando que a empresa já executou ou esteja executando, em empresa ou órgão da Administração Pública, de forma satisfatória, o fornecimento de, licenciamento referente à plataforma de avaliação de vulnerabilidades e auditoria de configurações de ativos de rede, no mínimo, de 450 (quatrocentos e cinquenta) IP´s.

12.3.2. **Grupo 2 - item 3**: No mínimo, 1 (um) Atestado de Capacidade Técnica, fornecido por pessoa jurídica de direito público ou privado, comprovando que a empresa já executou ou esteja executando, em empresa ou órgão da Administração Pública, de forma satisfatória, o fornecimento de licenciamento para solução de análise em aplicações Web ou o fornecimento, instalação, configuração e suporte continuado, por no mínimo 12 meses de solução de segurança para aplicações web.

12.3.3. Quando couber, a documentação relativa à qualificação técnica do licitante deverá constar em dispositivo editalício específico, quando a situação demandada a exigir.

12.3.4. Todos os documentos apresentados poderão ser alvo de diligência por parte da CONTRATANTE, sendo desclassificado o licitante que apresentar documentação falsa ou incompleta, estando sujeito, ainda, às penalidades previstas em lei;

12.3.5. No caso de atestados emitidos por empresa da iniciativa privada, não serão considerados aqueles emitidos por empresas pertencentes ao mesmo grupo empresarial da empresa proponente. Serão considerados como pertencentes ao mesmo grupo empresarial da empresa proponente, empresas controladas ou controladoras da empresa proponente, ou que tenha pelo menos uma mesma pessoa física ou jurídica que seja sócio da empresa emitente e da empresa proponente.

12.3.6. As competências exigidas correspondem às quantidades relevantes dos itens mais críticos para assegurar que a LICITANTE tenha efetiva capacidade de prestar os serviços considerando a complexidade da infraestrutura de TI da CONTRATANTE.

12.3.7. Deverá ser entregue a Declaração de vistoria, conforme Anexo I-D deste Termo de Referência, devidamente preenchido e assinado em conjunto pelo representante do Órgão e pelo representante da empresa licitante.

12.3.8. Em caso de opção pela não realização da vistoria, deverá ser entregue a Declaração de Renúncia à Vistoria, conforme Anexo I-G, devidamente preenchido e assinado pelo representante da empresa licitante.

13. DA EQUIPE DE PLANEJAMENTO DA CONTRATAÇÃO E DA APROVAÇÃO

13.1. A equipe de Planejamento da Contratação designada por intermédio da Portaria SAA nº 64, de 9 de julho de 2021 (15257536), apresenta este Termo de Referência para aprovação.

I - **Integrante Requisitante**: representante da Área Requisitante da Solução:

Titular: Ivanildo de Oliveira da Silva JR, Matrícula Siape nº 1535600;

II - **Integrante Requisitante substituto**: representante da Área Requisitante da Solução:

Joédes Cardoso da Silva, Matrícula Siape nº 3730955;

III - **Integrante Técnico**: representante da Área de Tecnologia da Informação:

Titular: Lucas Reinehr de Andrade, Matrícula Siape nº 3223177;

III - Integrante Técnico substituto: representante da Área de Tecnologia da Informação e Comunicação:

Luis Claudio Rodrigues Morais, Matrícula Siape nº 3214091;

III - **Integrante Administrativo**: representante da Área Administrativa:

Titular: Vinícius Augusto Bittencourt Dalcól, Matrícula Siape nº 1764266.

Aprovo o presente Termo de Referência nos termos do Art. 11 da Portaria SE nº 1.008, de 28 de Setembro de 2020.

Diretor de Tecnologia da Informação e Comunicação

RODRIGO LANGE

Matrícula: 1558579

14. ANEXOS

14.1. São partes integrantes deste Termo de Referência os seguintes anexos (15527738), (15356773) e (15531434).

14.1.1. ANEXO I - A - PROPOSTA DE PREÇOS (15527738).

14.1.2. ANEXO I - B - MODELO DE ORDEM DE SERVIÇO – O.S (15527738).

14.1.3. ANEXO I - C - RELATÓRIO DE CHAMADO TÉCNICO – RCTA (15527738).

14.1.4. ANEXO I - D - MODELO DE DECLARAÇÃO DE VISTORIA (15527738).

14.1.5. ANEXO I - E - TERMO DE CIÊNCIA (15527738).

14.1.6. ANEXO I - F - TERMO DE COMPROMISSO (15527738).

14.1.7. ANEXO I - G - MODELO DE DECLARAÇÃO DE RENÚNCIA À VISTORIA (15527738).

14.1.8. ANEXO I - H - MODELO DE PLANO DE INSERÇÃO (15527738).

14.1.9. ANEXO I - I - MODELO DE PLANO DE FISCALIZAÇÃO (15527738).

14.1.10. ANEXO I - J - MODELO DE DECLARAÇÃO DE SUSTENTABILIDADE AMBIENTAL (15527738).

14.1.11. ANEXO I - K - PLANILHA DE AVALIAÇÃO DE TREINAMENTO (15527738).

14.1.12. ANEXO I - L - ESTUDO TÉCNICO PRELIMINAR (15356773).

14.1.13. ANEXO I - M - PORTARIA 513 MJSP(15531434).

Documento assinado eletronicamente por **ALEXANDRA LACERDA FERREIRA RIOS**, **Pregoeiro(a)**, em 13/09/2021, às 13:43, com fundamento no § 3º do art. 4º do Decreto nº 10.543, de 13 de novembro de 2020.

A autenticidade do documento pode ser conferida no site http://sei.autentica.mj.gov.br informando o código verificador **15796716** e o código CRC **8CA390FD**
O trâmite deste documento pode ser acompanhado pelo site http://www.justica.gov.br/acesso-a-sistemas/protocolo e tem validade de prova de registro de protocolo no Ministério da Justiça e Segurança Pública.

MINISTÉRIO DA JUSTIÇA

ANEXOS I-A À I-K DO TERMO DE REFERÊNCIA

ANEXO I-A

PROPOSTA DE PREÇOS
(EMITIR EM PAPEL TIMBRADO DA EMPRESA)

PROPOSTA DE PREÇOS

Objeto: Contratação de empresa especializada, mediante Sistema de Registro de Preços, para prestação de serviços de implementação de solução para avaliação de vulnerabilidades em ativos de tecnologia da informação e aplicações web ao Ministério da Justiça e Segura Pública, compreendendo: a subscrição de licenças de software, abarcando a atualização, o treinamento e o suporte técnico (24x7); e o serviço técnico especializado, conforme as especificações e demais condições de execução contidas no Termo de Referência e seus anexos.

À COORDENAÇÃO DE PROCEDIMENTOS LICITATÓRIOS

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

Grupo	Item	Código SIASG	DESCRIÇÃO	Quantidade			Unidade de Medida	Valor Unitário para 2 anos	Valor Total
				CADE	MJSP	TOTAL			
1	1	27502	Licenciamento de plataforma de avaliação de vulnerabilidades e auditoria de configurações de ativos de rede, contemplando no mínimo 1.000 endereços IP, por ano de uso, com suporte técnico (24x7), treinamento e atualização upgrade/update, por 24 (vinte e quatro) meses	03	09	12	Licença		
	2	27340	Serviço Técnico Especializado para avaliação de vulnerabilidades	960	960	1.920	Horas		
2	3	27340	Licenciamento para solução de análise de segurança em aplicações Web, pacote para 8 (oito) domínios (FQDN), por ano de uso, com suporte técnico (24x7), treinamento e atualização upgrade/update, por 24 (vinte e quatro) meses	01	01	02	Licença		
	4	27340	Serviço Técnico Especializado para avaliação de vulnerabilidades	960	960	1.920	Horas		

Tabela 1 - Quantitativos a serem registrados

Dados da Empresa

Razão Social:
CNPJ (MF) nº:
Representante (s) legal (is) com poderes para assinar o contrato:
CPF: RG:
Inscrição Estadual nº:
Endereço completo (com CEP):
Telefones:
E-mail:
Dados Bancários(nº Banco, nº agência, nº cc):
Contato: Fone/Ramal:
Declarações
Validade da Proposta (mínimo 60 dias), conforme o artigo 64, § 3° da Lei 8.666/93.:
Declaramos que nos preços propostos estão incluídos todos os custos e despesas de qualquer natureza, incidentes sobre os objetos desta proposta.
Declaramos total conhecimento e concordância dos termos do edital do pregão e dos seus anexos.
Assinatura
Local e data:
Nome do Representante Legal:
Identidade do Representante Legal:

ANEXO I-B

MODELO DE ORDEM DE SERVIÇO – O.S

NUMERO DO CONTRATO /		DATA:	
Nº ORDEM DE SERVIÇO		HORA:	
1. IDENTIFICAÇÃO DO SOLICITANTE			
Nome:	E-mail:		

Fone/Ramal:	Assinatura do Solicitante:		
2. SERVIÇO A EXECUTAR			
PRAZO ESTIMADO PARA CONCLUSÃO DOS SERVIÇOS (em horas) :			
EMPRESA RESPONSÁVEL:			
LOCAL/REFERÊNCIA:			
HORARIO/DIA P/ EXECUÇÃO:			
OBS.:			
3. AUTORIZAÇÃO P/ EXECUÇÃO DOS SERVIÇOS SEM ACOMPANHAMENTO DO SETOR SOLICITANTE			
Autorizo o pessoal abaixo a realizar os serviços acima nos termos definidos em Contrato.			
Data ___/__/___	Hora ___:___ hs	Ass. e carimbo solicitante:	
4. FUNCIONÁRIO (S) RESPONSÁVEL (IS) PELO SERVIÇO A SEREM EXECUTADOS			
	Nome do funcionário		Cargo/função
1			
2			
3			
5. CRONOGRAMA DE ATIVIDADES A SEREM DESENVOLVIDAS			
Item	Descrição	Unidade/Tipo	Quantidade/Horas
1			
2			
3			
Total de horas			
6. DATA E HORA PREVISTA PARA ENTREGA DO SERVIÇO: Data ___/__/___ Hora ___:___ hs			
7. DATA E HORÁRIO DO INÍCIO E TÉRMINO DOS SERVIÇOS REALIZADOS (desconsiderar intervalos)			
Data de início do serviço	Hora	Data de término do serviço	Hora
___/__/___	___:___ hs	___/__/___	___:___ hs
8. ACEITE DO SERVIÇO			
Serviço executado por completo: ( )Sim ( )Não *Observações:*			
Declaro que o serviço acima solicitado, foi executado, considerando aceito o serviço			
Data ___/__/___	Hora ___:___ hs	Ass. e carimbo solicitante:	

ANEXO I-C

RELATÓRIO DE CHAMADO TÉCNICO – RCTA

CHAMADO TÉCNICO Nº:		***DATA:***	
		HORA:	
1. ***IDENTIFICAÇÃO DO SOLICITANTE***			
Resp. Solicitante:			
E-mail:			
Fone/Ramal:		*Ass. e carimbo:*	
2. ***DESCRIÇÃO DO PROBLEMA***			

Prioridade do chamado:	*1 - Alta*	*2 - Média*	*3 - Baixa*	*4 - Não crítica*
Empresa Responsável:				
Nome do(a) atendente:				

1. ***HORÁRIO (SLA – ATENDIMENTO)***	
Início:	
Término:	
Total de horas:	

2. ***SERVIÇO EXECUTADO (PARECER)***		
Serviço executado por completo:	*Sim*	*Não*
Observações:		

3. ***TÉCNICOS RESPONSÁVEIS (NOME COMPLETO)***	***Nº MATRÍCULA***	***CARGO/FUNÇÃO***

	Sim	*Não*
PROGRAMAR NOVO ATENDIMENTO PARA CONCLUSÃO DOS SERVIÇOS:		
HAVERÁ IMPACTO NAS OPERAÇÕES DA CONTRATANTE?		
JUSTIFICATIVA (Se o serviço não for concluído):		

4. ***COMENTÁRIO DA CONTRATANTE***

DATA:	___ /__ /__	***NOME:***		***ASSINATURA:***	

ANEXO I-D

MODELO DE DECLARAÇÃO DE VISTORIA

DECLARAÇÃO DE VISTORIA

(EMITIR EM PAPEL TIMBRADO DA EMPRESA)

Pela presente, declaramos conhecer e compreender por inteiro o teor do PREGÃO ELETRÔNICO nº ___/2021, cujo objeto é a registro de preço por menor preço global para contratação de empresa especializada no fornecimento de subscrição de licenças de software, aplicativos e sistemas operacionais, destinados aos equipamentos, estações de trabalho e servidores de rede do _____, incluindo suporte técnico e

garantia de atualização das versões pelo período de 24 meses, nas condições estabelecidas neste Termo de Referência e seus anexos, pelo que aceitamos seus termos e comprometemo-nos a observá-los integralmente. Declaramos, outrossim, ter visitado o local dos serviços a serem executados em companhia do representante da Tecnologia da Informação.

Empresa:_____

C.N.P.J.(MF):_____Tel/Fax:_____

Endereço:_____

Nome do Representante: _____

Endereço Eletrônico (e-mail): _____

Brasília-DF, ...de.....de 20...

_____

Representante da Empresa

Carteira de Identidade - Órgão Emissor

Declaro que o Representante da empresa acima identificada visitou os locais de execução dos serviços.

Brasília-DF, ...de.....de 20....

_____

Nome

Carteira de Identidade - Órgão Emissor

ANEXO I-E

TERMO DE CIÊNCIA

INTRODUÇÃO			
Visa obter o comprometimento formal dos empregados da CONTRATADA diretamente envolvidos no projeto sobre o conhecimento da declaração de manutenção de sigilo e das normas de segurança vigentes na Instituição.			
IDENTIFICAÇÃO			
Contrato N°:			
Objeto:			
Contratante:			
Gestor do Contrato:		Matr.:	
Contratada:		CNPJ:	
Preposto da Contratada:		CPF:	
Por este instrumento, os funcionários abaixo-assinados declaram ter ciência e conhecer o teor do Termo de Compromisso de Manutenção de Sigilo e as normas de segurança vigentes na Contratante.			
CIÊNCIA			
CONTRATADA – Funcionários			
_____ ***<Nome>*** **Matrícula: <*Matr.*>**		_____ ***<Nome>*** **Matrícula: <*Matr.*>**	
_____ ***<Nome>*** **Matrícula: <*Matr.*>**		_____ ***<Nome>*** **Matrícula: <*Matr.*>**	
_____ ***<Nome>*** **Matrícula: <*Matr.*>**		_____ ***<Nome>*** **Matrícula: <*Matr.*>**	

_____,_____ de _____ de 20__.

ANEXO I-F

TERMO DE COMPROMISSO

O <NOME DO ÓRGÃO>, sediado em <ENDEREÇO>, CNPJ n° <CNPJ>, doravante denominado CONTRATANTE, e, de outro lado, a <NOME DA EMPRESA>, sediada em <ENDEREÇO>, CNPJ n° <CNPJ>, doravante denominada CONTRATADA;
CONSIDERANDO que, em razão do CONTRATO N.º XX/20XX doravante denominado CONTRATO PRINCIPAL, a CONTRATADA

poderá ter acesso a informações sigilosas do CONTRATANTE;
CONSIDERANDO a necessidade de ajustar as condições de revelação destas informações sigilosas, bem como definir as regras para o seu uso e proteção;
CONSIDERANDO o disposto na Política de Segurança da Informação da CONTRATANTE;
Resolvem celebrar o presente TERMO DE COMPROMISSO DE MANUTENÇÃO DE SIGILO, doravante TERMO, vinculado ao CONTRATO PRINCIPAL, mediante as seguintes cláusulas e condições:

Cláusula Primeira – DO OBJETO
Constitui objeto deste TERMO o estabelecimento de condições específicas para regulamentar as obrigações a serem observadas pela CONTRATADA, no que diz respeito ao trato de informações sigilosas, disponibilizadas pela CONTRATANTE, por força dos procedimentos necessários para a execução do objeto do CONTRATO PRINCIPAL celebrado entre as partes e em acordo com o que dispõem a Lei 12.527, de 18/11/2011 e os Decretos 7.724, de 16/05/2012 e 7.845, de 14/11/2012, que regulamentam os procedimentos para acesso e tratamento de informação classificada em qualquer grau de sigilo.

Cláusula Segunda – DOS CONCEITOS E DEFINIÇÕES
Para os efeitos deste TERMO, são estabelecidos os seguintes conceitos e definições:
INFORMAÇÃO: dados, processados ou não, que podem ser utilizados para produção e transmissão de conhecimento, contidos em qualquer meio, suporte ou formato.
INFORMAÇÃO SIGILOSA: aquela submetida temporariamente à restrição de acesso público em razão de sua imprescindibilidade para a segurança da sociedade e do Estado.
CONTRATO PRINCIPAL: contrato celebrado entre as partes, ao qual este TERMO se vincula.

Cláusula Terceira – DA INFORMAÇÃO SIGILOSA
Serão consideradas como informação sigilosa, toda e qualquer informação classificada ou não nos graus de sigilo ultrassecreto, secreto e reservado. O TERMO abrangerá toda informação escrita, verbal, ou em linguagem computacional em qualquer nível, ou de qualquer outro modo apresentada, tangível ou intangível, podendo incluir, mas não se limitando a: know-how, técnicas, especificações, relatórios, compilações, código fonte de programas de computador na íntegra ou em partes, fórmulas, desenhos, cópias, modelos, amostras de ideias, aspectos financeiros e econômicos, definições, informações sobre as atividades da CONTRATANTE e/ou quaisquer informações técnicas/comerciais relacionadas/resultantes ou não ao CONTRATO PRINCIPAL, doravante denominados INFORMAÇÕES, a que diretamente ou pelos seus empregados, a CONTRATADA venha a ter acesso, conhecimento ou que venha a lhe ser confiada durante e em razão das atuações de execução do CONTRATO PRINCIPAL celebrado entre as partes;

Cláusula Quarta – DOS LIMITES DO SIGILO
As obrigações constantes deste TERMO não serão aplicadas às INFORMAÇÕES que:
I – sejam comprovadamente de domínio público no momento da revelação, exceto se tal fato decorrer de ato ou omissão da CONTRATADA;
II – tenham sido comprovadas e legitimamente recebidas de terceiros, estranhos ao presente TERMO;
III – sejam reveladas em razão de requisição judicial ou outra determinação válida do Governo, somente até a extensão de tais ordens, desde que as partes cumpram qualquer medida de proteção pertinente e tenham sido notificadas sobre a existência de tal ordem, previamente e por escrito, dando a esta, na medida do possível, tempo hábil para pleitear medidas de proteção que julgar cabíveis.

Cláusula Quinta – DOS DIREITOS E OBRIGAÇÕES
As partes se comprometem a não revelar, copiar, transmitir, reproduzir, utilizar, transportar ou dar conhecimento, em hipótese alguma, a terceiros, bem como a não permitir que qualquer empregado envolvido direta ou indiretamente na execução do CONTRATO PRINCIPAL, em qualquer nível hierárquico de sua estrutura organizacional e sob quaisquer alegações, faça uso dessas INFORMAÇÕES, que se restringem estritamente ao cumprimento do CONTRATO PRINCIPAL.
Parágrafo Primeiro – A CONTRATADA se compromete a não efetuar qualquer tipo de cópia da informação sigilosa sem o consentimento expresso e prévio da CONTRATANTE.
Parágrafo Segundo – A CONTRATADA compromete-se a dar ciência e obter o aceite formal da direção e empregados que atuarão direta ou indiretamente na execução do CONTRATO PRINCIPAL sobre a existência deste TERMO bem como da natureza sigilosa das informações.
I – A CONTRATADA deverá firmar acordos por escrito com seus empregados visando garantir o cumprimento de todas as disposições do presente TERMO e dará ciência à CONTRATANTE dos documentos comprobatórios.
Parágrafo Terceiro – A CONTRATADA obriga-se a tomar todas as medidas necessárias à proteção da informação sigilosa da CONTRATANTE, bem como evitar e prevenir a revelação a terceiros, exceto se devidamente autorizado por escrito pela CONTRATANTE.
Parágrafo Quarto – Cada parte permanecerá como fiel depositária das informações reveladas à outra parte em função deste TERMO.
I – Quando requeridas, as INFORMAÇÕES deverão retornar imediatamente ao proprietário, bem como todas e quaisquer cópias eventualmente existentes.
Parágrafo Quinto – A CONTRATADA obriga-se por si, sua controladora, suas controladas, coligadas, representantes, procuradores, sócios, acionistas e cotistas, por terceiros eventualmente consultados, seus empregados, contratados e subcontratados, assim como por quaisquer outras pessoas vinculadas à CONTRATADA, direta ou indiretamente, a manter sigilo, bem como a limitar a utilização das informações disponibilizadas em face da execução do CONTRATO PRINCIPAL.
Parágrafo Sexto – A CONTRATADA, na forma disposta no parágrafo primeiro, acima, também se obriga a:
I – Não discutir perante terceiros, usar, divulgar, revelar, ceder a qualquer título ou dispor das INFORMAÇÕES, no território brasileiro ou no exterior, para nenhuma pessoa, física ou jurídica, e para nenhuma outra finalidade que não seja exclusivamente relacionada ao objetivo aqui referido, cumprindo-lhe adotar cautelas e precauções adequadas no sentido de impedir o uso indevido por qualquer pessoa que, por qualquer razão, tenha acesso a elas;
II – Responsabilizar-se por impedir, por qualquer meio em direito admitido, arcando com todos os custos do impedimento, mesmo judiciais, inclusive as despesas processuais e outras despesas derivadas, a divulgação ou utilização das INFORMAÇÕES por seus agentes, representantes ou por terceiros;
III – Comunicar à CONTRATANTE, de imediato, de forma expressa e antes de qualquer divulgação, caso tenha que revelar qualquer uma das INFORMAÇÕES, por determinação judicial ou ordem de atendimento obrigatório determinado por órgão competente; e
IV – Identificar as pessoas que, em nome da CONTRATADA, terão acesso às informações sigilosas.

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

Cláusula Sétima – DAS PENALIDADES
A quebra do sigilo e/ou da confidencialidade das INFORMAÇÕES, devidamente comprovada, possibilitará a imediata aplicação de penalidades previstas conforme disposições contratuais e legislações em vigor que tratam desse assunto, podendo até culminar na rescisão do CONTRATO PRINCIPAL firmado entre as PARTES. Neste caso, a CONTRATADA, estará sujeita, por ação ou omissão, ao pagamento ou recomposição de todas as perdas e danos sofridos pela CONTRATANTE, inclusive as de ordem moral, bem como as de responsabilidades civil e criminal, as quais serão apuradas em regular processo administrativo ou judicial, sem prejuízo das demais sanções legais cabíveis, conforme Art. 87 da Lei nº. 8.666/93.

Cláusula Oitava – DISPOSIÇÕES GERAIS
Este TERMO de Confidencialidade é parte integrante e inseparável do CONTRATO PRINCIPAL.
Parágrafo Primeiro – Surgindo divergências quanto à interpretação do disposto neste instrumento, ou quanto à execução das obrigações dele decorrentes, ou constatando-se casos omissos, as partes buscarão solucionar as divergências de acordo com os princípios de boa fé, da equidade, da razoabilidade, da economicidade e da moralidade.
Parágrafo Segundo – O disposto no presente TERMO prevalecerá sempre em caso de dúvida e, salvo expressa determinação em contrário, sobre eventuais disposições constantes de outros instrumentos conexos firmados entre as partes quanto ao sigilo de informações, tal como aqui definidas.
Parágrafo Terceiro – Ao assinar o presente instrumento, a CONTRATADA manifesta sua concordância no sentido de que:
I – A CONTRATANTE terá o direito de, a qualquer tempo e sob qualquer motivo, auditar e monitorar as atividades da CONTRATADA;
II – A CONTRATADA deverá disponibilizar, sempre que solicitadas formalmente pela CONTRATANTE, todas as informações requeridas pertinentes ao CONTRATO PRINCIPAL.
III – A omissão ou tolerância das partes, em exigir o estrito cumprimento das condições estabelecidas neste instrumento, não constituirá novação ou renúncia, nem afetará os direitos, que poderão ser exercidos a qualquer tempo;
IV – Todas as condições, TERMOS e obrigações ora constituídos serão regidos pela legislação e regulamentação brasileiras pertinentes;
V – O presente TERMO somente poderá ser alterado mediante TERMO aditivo firmado pelas partes;
VI – Alterações do número, natureza e quantidade das informações disponibilizadas para a CONTRATADA não descaracterizarão ou reduzirão o compromisso e as obrigações pactuadas neste TERMO, que permanecerá válido e com todos seus efeitos legais em qualquer uma das situações tipificadas neste instrumento;

VII – O acréscimo, complementação, substituição ou esclarecimento de qualquer uma das informações disponibilizadas para a CONTRATADA, serão incorporados a este TERMO, passando a fazer dele parte integrante, para todos os fins e efeitos, recebendo também a mesma proteção descrita para as informações iniciais disponibilizadas, sendo necessário a formalização de TERMO aditivo 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
A CONTRATANTE elege o foro da <CIDADE DA CONTRATANTE>, onde está localizada a sede da CONTRATANTE, para dirimir quaisquer dúvidas originadas do presente TERMO, com renúncia expressa a qualquer outro, por mais privilegiado que seja.

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

DE ACORDO

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

_____, _____ de _____ de 20____

ANEXO I-G

MODELO DE DECLARAÇÃO DE RENÚNCIA À VISTORIA

DECLARAÇÃO DE RENÚNCIA À VISTORIA

(EMITIR EM PAPEL TIMBRADO DA EMPRESA)

Pela presente, declaramos RENUNCIAR a vistoria técnica aos locais e as instalações para prestação dos serviços constantes do objeto do PREGÃO ELETRÔNICO nº ___/2021, bem como seus anexos, pelo que aceitamos seus termos e comprometemo-nos a observá-los integralmente. Declaramos, outrossim, NÃO ter visitado o local dos serviços a serem executados, motivo esse que não poderei alegar o desconhecimento de fatos evidentes à época da vistoria para solicitar qualquer alteração do valor do contrato que vier a celebrar.

Empresa:_____
C.N.P.J.(MF):_____Tel/Fax:_____
Endereço:_____
Nome do Representante: _____
Endereço Eletrônico (e-mail): _____

Brasília-DF, ...de.....de 202...

_____

Representante da Empresa

Carteira de Identidade - Órgão Emissor

ANEXO I-H

MODELO DE PLANO DE INSERÇÃO

INTRODUÇÃO
O Plano de Inserção descreverá as atividades de alocação de recursos e preparação das condições necessárias para a contratada iniciar o fornecimento da Solução de TI.

1 – IDENTIFICAÇÃO	
Contratada	
Nº. do Contrato	
Área Requisitante da Solução	
Gestor do Contrato	
Fiscal Requisitante	
Fiscal Técnico	
Fiscal administrativo	

2 – VISÃO GERAL DO PROJETO
Justificativa da Contratação
Objetivos da Contratação

3 – METODOLOGIA DE TRABALHO	
Forma de Comunicação	
Forma de Encaminhamento das Ordens de Serviço	
Modelo de execução do contrato	

4 – EXECUÇÃO DO CONTRATO			
Ferramentas de Controle			
Id	**Ferramenta**	**Controles**	

DOCUMENTAÇÃO MÍNIMA EXIGIDA	
Documento	**Finalidade do documento**

PAPEIS E RESPONSABILIDADES			
Id	**Papel**	**Responsabilidades**	

PARTES INTERESSADAS		
Id	**Área/Órgão/Setor**	**Impacto**

FATORES CRÍTICOS DE SUCESSO	

PREMISSAS DA CONTRATAÇÃO	

RESTRIÇÕES DA CONTRATAÇÃO		

ENTREGAS PLANEJADAS				
Id	**Entrega**	**Marco**	**Duração**	**Data de Entrega**

INFRAESTRUTURA A SER DISPONIBILIZADA À CONTRATADA			
Id	**Recurso**	**Início**	**Fim**

CRITÉRIO DE ACEITAÇÃO – MÉTRICA E PERIODICIDADE	
Métrica 1	
Indicador de Qualidade	
Mínimo aceitável	

Métrica	
Ferramentas	
Periodicidade Aferição	
Métrica "N"	
Indicador de Qualidade	
Mínimo aceitável	
Métrica	
Ferramentas	
Periodicidade Aferição	

RESULTADOS ESPERADOS		
Id	**Entrega**	**Benefícios**

5 – INSTRUÇÕES COMPLEMENTARES

6 - CIÊNCIA		
Fiscais do Contrato		
Fiscal Técnico	Fiscal Requisitante	Fiscal Administrativo
_____ *<Nome>* **Matrícula: <*Matr.*>**	_____ ***<Nome>*** **Matrícula: <*Matr.*>**	_____ ***<Nome>*** **Matrícula: <*Matr.*>**
Gestor do Contrato		
_____ <Nome> Matrícula: <*Matr.*>		
Contratada		
_____ <Nome> CPF/CNPJ: <...>		
Brasília-DF, ...de.....de 202...		

ANEXO I-I

MODELO DE PLANO DE FISCALIZAÇÃO

INTRODUÇÃO
O Plano de Fiscalização descreverá as atividades de acompanhamento e fiscalização da execução do contrato de fornecimento da Solução de TI

1 – IDENTIFICAÇÃO DO CONTRATO	
Contrato nº:	
Contratante	
Área Requisitante da Solução	
Fiscal Requisitante	
Fiscal Técnico	
Fiscal Administrativo	
Gestor do Contrato	
Contratada	
CNPJ	

2 – PROCEDIMENTOS DE TESTE DE INSPEÇÃO	

CRITÉRIO DE ACEITAÇÃO – MÉTRICA E PERIODICIDADE

Métrica 1	
Indicador de Qualidade	
Mínimo aceitável	
Métrica	
Ferramentas	
Periodicidade Aferição	

3 – CONFIGURAÇÃO/CRIAÇÃO DE FERRAMENTAS PARA IMPLANTAÇÃO E ACOMPANHAMENTO DE INDICADORES
4 – ELABORAÇÃO/REFINAMENTO DAS LISTAS DE VERIFICAÇÃO E DOS ROTEIROS DE TESTE

FISCAIS DO CONTRATO		
Fiscal Técnico	Fiscal Requisitante	Fiscal Administrativo
_____ ***<Nome>*** **Matrícula: <*Matr.*>**	_____ ***<Nome>*** **Matrícula: <*Matr.*>**	_____ ***<Nome>*** **Matrícula: <*Matr.*>**

GESTOR DO CONTRATO
_____ ***<Nome>*** **Matrícula: <*Matr.*>**

CONTRATADA
_____ ***<Nome>*** **CPF/CNPJ: <...>**
Brasília-DF, ...de.....de 202...

ANEXO I-J

MODELO DE DECLARAÇÃO DE SUSTENTABILIDADE AMBIENTAL

DECLARAÇÃO DE SUSTENTABILIDADE AMBIENTAL

(EMITIR EM PAPEL TIMBRADO DA EMPRESA)

Empresa:_____

C.N.P.J.(MF):_____Tel/Fax:_____

Endereço:_____

Nome do Representante: _____

Endereço Eletrônico (e-mail): _____

Declaro, sob as penas da Lei nº 6.938/1981, na qualidade de proponente do procedimento licitatório, sob a modalidade Pregão Eletrônico nº _____, instaurado pelo Processo de nº 08006.001082/2020-13, que atendemos aos critérios de qualidade ambiental e sustentabilidade socioambiental, respeitando as normas de proteção do meio ambiente.

Estou ciente da obrigatoriedade da apresentação das declarações e certidões pertinentes dos órgãos competentes quando solicitadas como requisito para habilitação e da obrigatoriedade do cumprimento integral ao que estabelece o art. 6º e seus incisos, da Instrução Normativa nº 01, de 19 de janeiro de 2010, do Ministério do Planejamento, Orçamento e Gestão – MPOG.

Por ser a expressão da verdade, firmamos a presente.

Brasília-DF, ...de.....de 20...

_____

Representante da Empresa

Carteira de Identidade - Órgão Emissor

ANEXO I-K

PLANILHA DE AVALIAÇÃO DE TREINAMENTO

Curso:		
Local:	Data:	Carga Horária:
Órgão:		
INFORMAÇÕES 1. A finalidade deste instrumento é avaliar o curso que você participou. 2. O objetivo principal é verificar se o curso teve uma avaliação satisfatória. 3. Solicitamos sua colaboração respondendo todas as questões formuladas		
Avalie os critérios abaixo numa escala de 0 (zero) a 10(dez) ou N/A, onde: a nota 0 significa uma péssima avaliação e a nota 10 significa uma excelente avaliação, N/A significa não se aplica.		

CONTEÚDO PROGRAMÁTICO	**Nota**
Material didático (apostilas, livros, exercícios, etc.)	
O conteúdo da matéria apresentada durante o curso	
Ordem e distribuição dos assuntos apresentados	
Cumprimento da carga horária do curso	
Recursos audiovisuais (quadro, retroprojetor, micros, apresentações, etc.)	
Condições de equipamentos utilizados (micros, retroprojetor, etc.)	
INSTRUTOR	**Nota**
Domínio do assunto referente ao curso	
Facilidade em transmitir o conhecimento técnico (didática)	
Clareza/objetividade para esclarecer dúvidas (didática)	
Estímulo ao grupo na participação das atividades	
Relacionamento com os alunos	
Pontualidade quanto ao cumprimento do horário	
Aproveitamento do tempo quanto ao cumprimento do treinamento	

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

ANEXO I-L DO TERMO DE REFERÊNCIA

ESTUDO TÉCNICO PRELIMINAR DA CONTRATAÇÃO
PROCESSO Nº 08006.001082/2020-13

INTRODUÇÃO

Conforme previsto no Art. 11 da IN 01 SGD/ME nº 2019, a elaboração do Estudo Técnico Preliminar tem por objetivo identificar e analisar os cenários para o atendimento da demanda que consta no Documento de Oficialização da Demanda, bem como demonstrar a viabilidade técnica e econômica das soluções identificadas, fornecendo as informações necessárias para subsidiar o respectivo processo de contratação.

A presente análise tem por objetivo demonstrar a **viabilidade técnica e econômica da contratação** de empresa especializada para o fornecimento de Serviço de Suporte Técnico Especializado em Segurança da Informação e Serviço de Gestão de Vulnerabilidade, por meio da **contratação de empresa especializada para fornecimento e instalação de solução de gestão de vulnerabilidades em ativos de tecnologia da informação e aplicações web, compreendendo a aquisição de serviços de Consultoria Especializada, suporte 24x7, com garantia (manutenção e suporte técnico)** para o Ministério da Justiça e Segurança Pública (MJSP), incluindo a garantia de atualização das versões, pelo período de 24(vinte e quatro meses), podendo ser prorrogada até o prazo máximo de 48(quarenta e oito) meses, para o atendimento das necessidades da Diretoria de Tecnologia da Informação e Comunicação - DTIC do MJSP bem como fornecer informações necessárias para subsidiar o respectivo processo.

1. DEFINIÇÃO DAS NECESSIDADES E REQUISITOS

1.1. As organizações, sejam elas de qualquer segmento ou tamanho, cada vez mais utilizam os serviços da TIC - Tecnologia da Informação e Comunicação como meio para atingirem seus objetivos. Aliado a isso, o aumento da conectividade dos computadores à rede mundial contribuiu para o crescimento dos incidentes de segurança.

1.2. Conforme apresentado na imagem 1, o Centro de Estudos, Resposta e Tratamento de Incidentes de Segurança no Brasil (CERT.BR), em 2001 houve 12.301 incidentes reportados. Dez anos depois, em 2011 , foi registrado um número 32,48 vezes maior com 399.515 incidentes reportados. No de 2019 houve 875.327 incidentes, número 71,16 vezes maior. Conforme apresentado na Imagem 1.

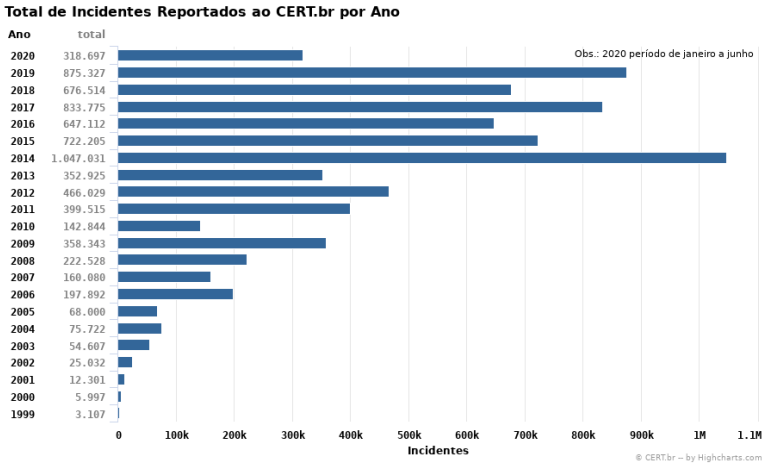


Imagem 1 - Total de incidentes reportados - Fonte: CERT.br disponível em https://www.cert.br/stats/incidentes/ acesso em 11/01/2021

1.3. O trabalho de manter os ativos de rede seguros vai além do da utilização de antivírus nos computadores. Softwares desatualizados em estações de trabalho e servidores, aliado a más práticas de configurações de serviços criam alvos fáceis para exploradores de vulnerabilidades. A utilização de firewall não é uma solução definitiva, visto que, muitas portas legítimas podem estar vulneráveis, como é o caso da porta 80 que hospeda websites vulneráveis.

1.4. Este Estudo Técnico Preliminar aborda os principais tipos de vulnerabilidades, softwares maliciosos e ataques e procura demonstrar a importância e necessidade da aquisição de uma solução de análise de vulnerabilidade. O intuito da utilização desse tipo de software é automatizar e facilitar a descoberta de vulnerabilidades em uma rede, para correção, antes que as mesmas sejam exploradas por atacantes.

1.5. **Normas e Definições**

1.6. Segurança da Informação é tratada pelo Comitê Brasileiro de Computadores e Processamento de Dados (ABNT/CB-21) e pela Comissão de Estudo de Segurança Física em Instalações de Informática através da norma ABNT NBR ISO/IEC 27002:2013.

1.7. Segundo a ISO/IEC 27000:2014, a informação é um ativo que, como outros ativos importantes, é essencial para os negócios de uma organização e, consequentemente precisa ser adequadamente protegido. As informações podem ser armazenadas de várias formas, incluindo: formulário digital (por exemplo, arquivos de dados armazenados em mídia eletrônica ou óptica), formulário material (por exemplo, em papel), bem como informações não representadas na forma de conhecimento dos funcionários.

1.8. Ainda segundo a ISO/IEC 27000:2014, as informações podem ser transmitidas por vários meios, incluindo: correio, comunicação eletrônica ou verbal. Qualquer que seja a forma da informação, ou o meio pelo qual a informação é transmitida, ela sempre precisa de proteção adequada.

1.9. Segundo a Instrução Normativa GSI/PR nº1, de 13 de junho de 2008, entende-se por Segurança da Informação e Comunicações, ações que objetivam viabilizar e assegurar a disponibilidade, a integridade, a confidencialidade e a autenticidade das informações.

1.10. A Segurança da Informação tem que ser vista pelas organizações como algo estratégico, pois elas estão muito dependentes dos serviços da Tecnologia da Informação (TI), como por exemplo:

- 1.10.1. Web Site: Como canal de divulgação da organização ou até mesmo para a geração, divulgação ou venda de produtos e serviços.
- 1.10.2. E-mail: Para troca de informações.
- 1.10.3. Videoconferência: Utilizado para realizar reuniões à distância.
- 1.10.4. Telefonia Ip: Fazer ligações entre as unidades de uma organização a um custo reduzido.

- 1.10.5. Sistema de Informação Computadorizado: Para armazenar e gerir informações conforme o modelo de negócio da organização.

1.11. Para o negócio, a proteção da informação, dos serviços e da rede como um todo é muito importante para garantir a continuidade do negócio, minimizar o risco ao negócio, maximizar o retorno sobre os investimentos e as oportunidades de negócio.

1.12. São vários casos famosos de falhas de segurança da informação que comprometeram grandes organizações e governos com prejuízos financeiros causados por falhas de Sistemas de Informação devido a indisponibilidade de sistemas. Além da falha em sistemas, a indisponibilidade pode ser causada por malwares. Os danos com malware poderiam ser diminuídos, por exemplo, com a conscientização dos usuários e com a utilização de um controle de proteção e detecção de malwares.

1.13. Os aspectos da Segurança da Informação são formados pela tríade confidencialidade-integridade-disponibilidade, definidos como:

- 1.13.1. Confidencialidade: propriedade de que a informação não esteja disponível ou revelada a pessoa física, sistema, órgão ou entidade não autorizado e credenciado;
- 1.13.2. Integridade: propriedade de que a informação não foi modificada ou destruída de maneira não autorizada ou acidental;
- 1.13.3. Disponibilidade: propriedade de que a informação esteja acessível e utilizável sob demanda por uma pessoa física ou determinado sistema, órgão ou entidade.

1.14. **Vulnerabilidades**

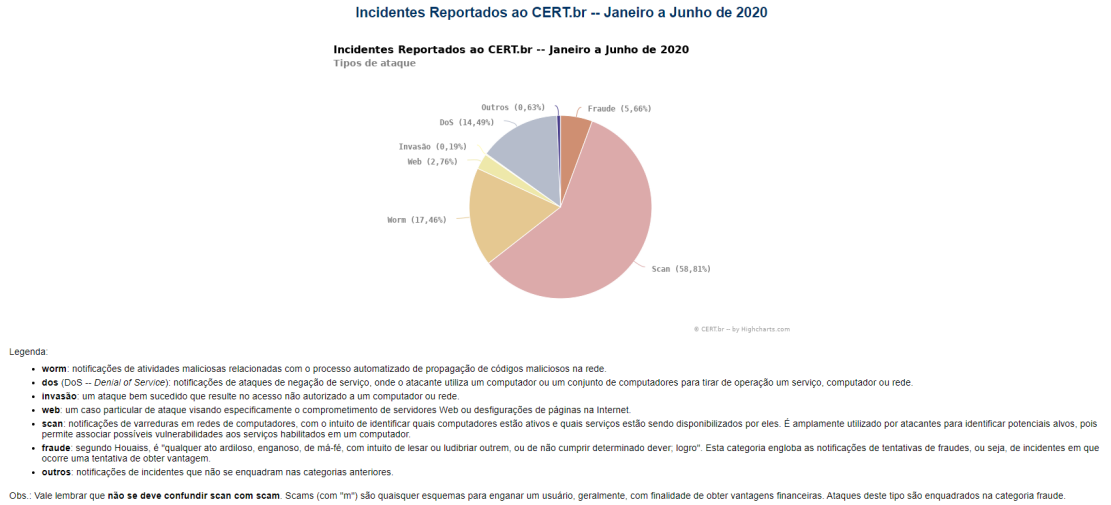
1.15. Vulnerabilidade é um conjunto de fatores internos ou causa potencial de um incidente indesejado, que podem resultar em risco para um sistema ou organização, os quais podem ser evitados por uma ação interna de segurança da informação. (NC 04/IN01/DSIC/GSI/PR)

1.16. Já segundo Cert.br, uma vulnerabilidade é definida como uma condição que, quando explorada por um atacante, pode resultar em uma violação de segurança.

1.17. As vulnerabilidades são originadas de falhas na maioria das vezes não intencionais. Estas falhas podem ser:

- 1.17.1. Físicas: Acesso a ativos por pessoas não autorizadas, devido à falta de controle de acesso. Por exemplo, uma empresa terceirizada de limpeza desligar um switch por engano.
- 1.17.2. Hardware: Falhas no Hardware que ocasionam indisponibilidade no sistema ou perda dados. Outro item desta falha é a inclusão de um hardware malicioso como um Keylogger.
- 1.17.3. Naturais: Desastres naturais comprometendo a segurança dos dados armazenados.
- 1.17.4. Humanas: Operador de sistema utilizar erroneamente uma função, prejudicando o funcionamento do mesmo ou ocasionando perda de informações.
- 1.17.5. Software: Falhas de programação, abrindo brechas a serem exploradas.

1.18. As estatísticas de incidentes do Cert.br reportados de janeiro a junho de 2020, citadas na imagem 2, demonstram que 58,81% de incidentes são do tipo de ataque Scan, onde o atacante faz uma varredura de portas abertas em uma rede para identificar os serviços disponibilizados e suas possíveis vulnerabilidades.



Legenda:

- **worm**: notificações de atividades maliciosas relacionadas com o processo automatizado de propagação de códigos maliciosos na rede.
- **dos** (DoS -- *Denial of Service*): notificações de ataques de negação de serviço, onde o atacante utiliza um computador ou um conjunto de computadores para tirar de operação um serviço, computador ou rede.
- **invasão**: um ataque bem sucedido que resulte no acesso não autorizado a um computador ou rede.
- **web**: um caso particular de ataque visando especificamente o comprometimento de servidores Web ou desfigurações de páginas na Internet.
- **scan**: notificações de varreduras em redes de computadores, com o intuito de identificar quais computadores estão ativos e quais serviços estão sendo disponibilizados por eles. É amplamente utilizado por atacantes para identificar potenciais alvos, pois permite associar possíveis vulnerabilidades aos serviços habilitados em um computador.
- **fraude**: segundo Houaiss, é "qualquer ato ardiloso, enganoso, de má-fé, com intuito de lesar ou ludibriar outrem, ou de não cumprir determinado dever; logro". Esta categoria engloba as notificações de tentativas de fraudes, ou seja, de incidentes em que ocorre uma tentativa de obter vantagem.
- **outros**: notificações de incidentes que não se enquadram nas categorias anteriores.

Obs.: Vale lembrar que **não se deve confundir scan com scam**. Scams (com "m") são quaisquer esquemas para enganar um usuário, geralmente, com finalidade de obter vantagens financeiras. Ataques deste tipo são enquadrados na categoria fraude.

Imagem 2 - Incidentes reportados em 2020, Fonte: CERT.br disponível em https://www.cert.br/stats/incidentes/2020-jan-jun/tipos-ataque.html acesso em 11/01/2021

1.19. Muitas vulnerabilidades são exploradas ou criadas a partir de softwares desenvolvidos para este fim conhecidos como Malware. Proveniente do inglês malicious software o Malware é um programa que produz efeitos danosos e indesejados.

1.20. Os principais tipos de Malware encontrados hoje são:

1.20.1. Vírus: Programa capaz de se autoexecutar e infectar outros arquivos com seu próprio código.

1.20.2. Worm: Programa malicioso que se propaga sem a necessidade de infectar outros arquivos, diferentemente do vírus, sua propagação é feita sem intervenção humana utilizando vulnerabilidades em uma rede.

1.20.3. Bot e botnet: Bot é um programa que permite ser controlado remotamente para executar vários comandos maliciosos, como, por exemplo, ataque de negação de serviço a um site. Uma botnet é uma rede com vários bots no qual sua ação maliciosa é amplificada.

1.20.4. Spyware: Os Spywares coletam informações pessoais ou empresariais e as enviam para terceiros. O Keylogger é um tipo de Spyware que captura as teclas digitadas pelo usuário, geralmente utilizado para roubar senhas.

1.20.5. Backdoor: O Backdoor ou Porta do fundo é uma vulnerabilidade que abre uma brecha para o atacante obter acesso indevido.

1.20.6. Cavalo de tróia: Também conhecido como Trojan o Cavalo de Tróia é um programa malicioso que se disfarça por um programa bem intencionado. O usuário executa, sem saber, um código malicioso pensando que está executando apenas um programa legítimo. Eles geralmente são disseminados por e-mails e redes sociais se passando por cartões, álbum de fotos, jogos e etc.

1.20.7. Rootkit: Conjunto de programas utilizado por um atacante para ocultar sua invasão e facilitar um futuro ataque. Os Rootkits podem ser utilizados em outros malwares para dificultar a detecção destes.

1.21. A efetivação de um ataque é o exito na exploração de uma ou mais vulnerabilidades. As motivações para realizar um ataque segundo o Cert.br, podem ser financeiras, por prestígio, demonstração de poder, por ideologia ou comerciais. Com novas tecnologias novos ataques surgem, mas o principais ataques conhecidos atualmente são:

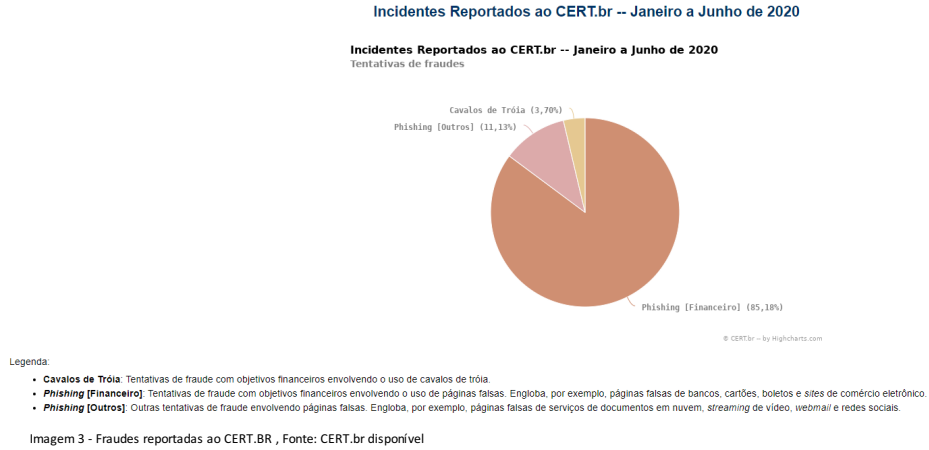
1.21.1. DoS e DDoS: Negação de Serviço do inglês Denial of Service, sigla DoS, ocorre quando um site (ou serviço) fica indisponível por receber uma grande quantidade de tráfego, não podendo atender as requisições legítimas. Os ataques DDoS (Distributed Denial of Service) são vários ataques DoS feitos de maneira distribuída dificultando assim o

bloqueio da origem os ataques. Geralmente estes ataques provêm de computadores infectados com Bots participantes de uma rede Botnet.

1.21.2. Buffer Overflow: ou Estouro de Buffer ocorre quando um espaço de memória com tamanho fixo recebe um dado maior que seu tamanho, ocorrendo assim um vazamento dados na memória sobrescrevendo a memória adjacente.

1.21.3. Spam: são e-mails não solicitados que são enviados em massa gerando tráfego desnecessário nas redes. Geralmente os Spams têm como intuito a divulgação de produtos, mas também são responsáveis por muitos golpes de Internet por disseminarem Malwares.

1.21.4. Phishing Scam: E-mails falsos que se passam por mensagens de instituições confiáveis, como bancos e órgãos governamentais. Seu intuito é induzir o usuário a instalar um programa malicioso ou visitar uma página falsa (cópia de uma verdadeira) para obter dados pessoais, como por exemplo, senhas e números de cartão de crédito. Segundo o Cert.br 87,05% das fraudes de janeiro a dezembro de 2019 eram de páginas falsas, conforme apresentado na imagem 3.



Legenda:

- **Cavalos de Tróia**: Tentativas de fraude com objetivos financeiros envolvendo o uso de cavalos de tróia.
- ***Phishing* [Financeiro]**: Tentativas de fraude com objetivos financeiros envolvendo o uso de páginas falsas. Engloba, por exemplo, páginas falsas de bancos, cartões, boletos e *sites* de comércio eletrônico.
- ***Phishing* [Outros]**: Outras tentativas de fraude envolvendo páginas falsas. Engloba, por exemplo, páginas falsas de serviços de documentos em nuvem, *streaming* de vídeo, *webmail* e redes sociais.

Imagem 3 - Frauds reportadas ao CERT.BR , Fonte: CERT.br disponível em https://www.cert.br/stats/incidentes/2020-jan-jun/fraude.html acesso em 13/01/2021

1.22. **Tipos de incidentes de segurança da informação:**

1.22.1. DNS Poisoning: Envenenamento de DNS é um ataque que forja um endereço falso no servidor de DNS. Assim, o atacante pode capturar senhas e números de cartões de crédito utilizando páginas clones do site original.

1.22.2. Ataque de Força Bruta: Programa que utiliza várias combinações de usuário e senha para conseguir acesso indevido a sistemas ou para descriptografar chaves e arquivos. Além do risco de acesso indevido, o Ataque de Força Bruta gera uma carga excessiva no alvo por ter responder e processar a várias tentativas de logins. Esta técnica é muito utilizada em servidores de SSH mal configurados.

1.22.3. Packet Sniffing: Packet Sniffing ou Farejamento de Pacotes é um método utilizado para capturar pacotes destinados a outras máquinas da mesma rede com objetivo de obter dados pessoais. Ativos de rede que utilizam broadcast de pacotes, como Hub, facilitam o farejamento dos pacotes. Em redes segmentadas por Switches o Packet Sniffing é possível com a utilização de outra técnica conhecida como Man-in-theMiddle (MiTM). Com MiTM o atacante forja a passagem dos pacotes da rede pela sua interface através do envenenamento da tabela ARP dos outros computadores.

1.22.4. Varreduras em Redes – Scan: Técnica onde o atacante descobre máquinas ativas e serviços disponíveis na rede. Em uma rede 192.1 68.0.0/24, por exemplo, o atacante envia ping para todos endereços possíveis para descobrir quais estão ativos. Com os endereços das máquinas ativas é feita uma nova varredura em cada máquina para descobrir suas portas abertas e seus respectivos serviços. Com isso o atacante pode explorar as vulnerabilidades destes serviços e prejudicar o computador alvo. Por exemplo, sabendo que o alvo possui a porta TCP 23 aberta, o atacante irá explorar vulnerabilidades de software ou configuração do serviço para obter acesso ao sistema.

1.22.5. SQL Injection: O ataque de Injeção de SQL consiste em inserir códigos SQL em um software vulnerável para obter ou danificar informações do Banco de dados.

1.22.6. CSS - Cross Site Scripting: XSS ou CSS o Cross Site Scripting é um ataque a um site vulnerável que aceita a inserção de códigos Javascript. Através do CSS o atacante pode inserir uma página externa para capturar logins e senhas.

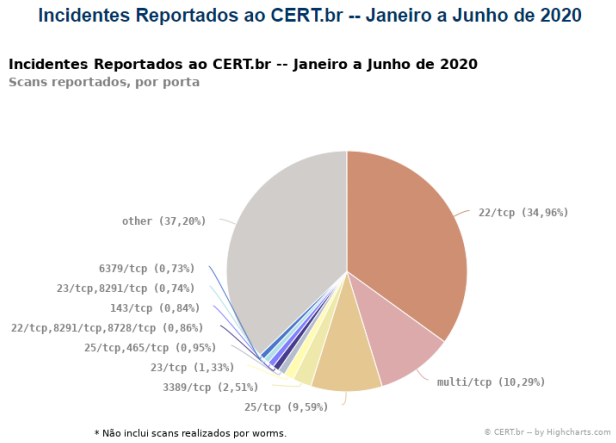


Imagem 4 - Scan reportados por porta - Fonte: CERT.br disponível em https://www.cert.br/stats/incidentes/2020-jan-jun/scan-portas.html acesso em 13/01/2021

2. DEFINIÇÃO DAS NECESSIDADES E REQUISITOS

2.1. **Ministério da Justiça e Segurança Pública**

2.2. O Ministério da Justiça e Segurança Pública possui um ambiente de Tecnologia da Informação e Comunicação (TIC) diversificado com vários recursos tecnológicos, sistemas legados e um grande número de usuários desses recursos, conforme apresentado nos relatórios (Docs SEI Nº 13742791, 13742757 e 13742631) e resumido abaixo:

Categoria	Total
Appliance de Segurança	14

Ativos de Rede	274
Host Físico no Datacenter	84
Sistemas Operacionais de Servidores	917
Armazenamento	21
Estação de Trabalho	4.334
Servidor de Aplicação	187
Sistemas Web	58
Serviços de rede	4
Total	5.893

Tabela 1 - Resumo do Parque de Ativos de TI

Nome	Domínios	Tipo de Domínio
consumidor.gov.br	consumidor.gov.br	Authoritative
defesadoconsumidor.gov.br	defesadoconsumidor.gov.br	Authoritative
infoseg.gov.br	infoseg.gov.br	Authoritative
justica.gov.br	justica.gov.br	Authoritative
justicagovbr.mail.onmicrosoft.com	justicagovbr.mail.onmicrosoft.com	Authoritative
migrantes.gov.br	migrantes.gov.br	Authoritative
mj.gov.br (default domain)	mj.gov.br	Authoritative
seguranca.gov.br	seguranca.gov.br	Authoritative
TOTAL DE DOMÍNIOS		8
TOTAL DE IP's		6.702

Tabela 2 - Domínios e IP's

2.3.

Imagem 5 - Força de trabalho do MJSP, Fonte: Portal Gestão de Pessoas, disponível em **https://justicagovbr.sharepoint.com/sites/intra-CGGP/SitePages/For%C3%A7a-de-Trabalho.aspx,** acesso em 14/01/2021.

2.4. Nesse cenário cresce a preocupação relacionada aos problemas com a segurança digital e o monitoramento das vulnerabilidades de segurança no ambiente computacional é absolutamente necessário para se manter a confidencialidade, a disponibilidade e a integridade das informações.

2.5. Em uma rede corporativa, com diversos usuários, manter os ativos livres de vulnerabilidades é um trabalho árduo para os administradores de rede. Alguns dos motivos que contribuem para este problema são:

- 2.6. Dificuldade em implantar uma política contra a instalação de novos softwares pelos usuários. Vários softwares possuem vulnerabilidades conhecidas em algumas de suas versões a exemplo leitores de PDF e navegadores Web;
- 2.7. Desconhecimento dos usuários sobre prevenção contra malwares, pois muitos através de e-mails falsos e mensagens em redes sociais instalam códigos maliciosos;
- 2.8. A diversidade de versões de softwares e sistemas operacionais;
- 2.9. Controle das atualizações dos softwares e sistemas operacionais; e
- 2.10. Impossibilidade dos profissionais de Tecnologia de Informação estarem cientes de todas vulnerabilidades descobertas, principalmente as mais recentes.

2.11. Diante destes fatores a Diretoria de Tecnologia da Informação e Comunicação - DTIC necessita de ferramentas que a auxilie a manter o parque computacional o menos vulnerável possível. É possível atender este requisito da Segurança da Informação com uma solução de gestão vulnerabilidades, a qual é composta, entre outros por um software conhecido como Scanner de Vulnerabilidade.

2.12. Desse modo, busca-se implementar soluções de software capazes de testar os ativos de TI e as aplicações web periodicamente em busca de quaisquer vulnerabilidades, sejam elas relativas a atualização de sistemas operacionais e servidores de aplicação, configurações de serviços ou outras falhas técnicas. Além disso, é preciso que as soluções forneçam relatórios para que seja possível o acompanhamento do trabalho de identificação e mitigação de riscos.

2.13. Segue abaixo a especificação das necessidades de negócio e tecnológicas, e dos requisitos necessários e suficientes à escolha da solução de TIC.

3. IDENTIFICAÇÃO DAS NECESSIDADES DE NEGÓCIO

Id	Funcionalidades
1.	Aumento da segurança da informação e comunicação no âmbito do Ministério da Justiça e Segurança Pública e o sigilo das informações do cidadão; Gerenciamento de Vulnerabilidades em ativos e Sistemas Operacionais; Gerenciamento de Vulnerabilidades em Sistemas e páginas WEB; Detecção e Correção de falhas de softwares que possam acarretar riscos na segurança, na funcionalidade e no desempenho dos sistemas; Implantação de mecanismos para realizar o bloqueio de ataques constantes; Identificação de novas soluções de segurança e realização de suas alterações; Foco na melhoria constante do sistema de segurança de dados corporativos; Auxílio na implementação de políticas de segurança; Agilidade na identificação de falhas.

3.1. Identificação das necessidades tecnológicas

Id	Necessidades Tecnológicas
1	Fornecimento de solução de segurança para proteção de aplicações, servidores físicos, virtuais e container com serviços de implementação e capacitação; Solução de análise de vulnerabilidades e Serviços técnicos especializados na área de Segurança da Informação; Análise de Vulnerabilidades; Gerenciamento de patches; Gerenciamento da configuração de segurança; Auditoria de software de alto risco; Detecção e mitigação de vulnerabilidades de dia zero; Aprimoramento da segurança dos servidores web.

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

Id	Demais necessidades
1	Integração e Customização dos Sistemas de Informação existentes; Otimização dos processos de infraestrutura da TIC conforme as melhores práticas; Testar os hosts (físicos e virtuais), comparando a bases de dados de vulnerabilidades mantidas por organizações especializadas em segurança da informação e por grandes fabricantes de software; Testar as aplicações e páginas web, internas e externas, comparando a bases de dados de vulnerabilidades mantidas por organizações especializadas em segurança da informação e por grandes fabricantes de software; Emitir relatórios de acompanhamento dos testes e das vulnerabilidades encontradas, apontando quando forem solucionadas. Aumento da proteção dos ativos de informação do Ministério da Justiça e Segurança Pública

4. ESTIMATIVA DA DEMANDA – QUANTIDADE DE BENS E SERVIÇOS

4.1. Para estimar a quantidade de bens e serviços necessários para a composição da solução a ser contratada é importante entender como funciona as ferramentas de gestão de vulnerabilidades, seu modelo de licenciamento e a estratégia de segurança da informação da Diretoria de Tecnologia da Informação e Comunicação - DTIC.

4.2. Um dos principais componentes das soluções de gestão de vulnerabilidades é o scan de vulnerabilidade, que tem por objetivo identificar os riscos e vulnerabilidades externas e internas de uma rede. O scan de vulnerabilidades é uma ferramenta que faz uma varredura em IP's externos ou ativos na rede interna, tipificando as vulnerabilidades por riscos, identificando e classificando as possíveis brechas de segurança presentes na rede.

4.3. O scan de vulnerabilidades é uma ferramenta muito eficaz, pois opera de maneira constante, detectando qualquer alteração que acontece dentro do período que foi configurado na ferramenta. Basicamente, o scan atua com duas estratégias: varreduras internas e externas da rede. Isso porque, ele realiza a varredura nos IP's, classificando vulnerabilidades e, assim, identificando as brechas de segurança da rede.

4.4. No caso das verificações externas de vulnerabilidades, eles identificam as maiores ameaças imediatas à rede, conferem as atualizações de softwares e firmwares necessárias para manutenção, portas e protocolos, ou seja, os pontos de entrada da rede e buracos no firewall de rede.

4.5. Já a varredura da vulnerabilidade interna, como o nome indica, tem como objetivo a rede interna. Elas podem ser aprimoradas com credenciais para efetuar login no dispositivo e executar verificações de conformidade e vulnerabilidades.

4.6. Além dessas estratégias, o scan utiliza a aquisição ativa e passiva de informações. A aquisição ativa compreende em enviar um grande número de pacotes, possuindo pontos característicos, que, na maior parte do tempo, não seguem as recomendações, analisando as respostas para determinar a versão da aplicação utilizada. Com efeito, cada aplicação utiliza os protocolos de uma maneira ligeiramente diferente, que permite distingui-los.

4.7. No caso, a aquisição passiva é menos intrusiva, correndo menos risco de ser detectada por um sistema de detecção de intrusos, o IDS. Ele funciona analisando os campos dos datagramas IP que circulam sobre uma rede, com a ajuda de um sniffer. A caracterização, na versão passiva, analisa a evolução dos valores dos campos sobre séries de fragmentos, o que implica um tempo de análise muito mais longo. Este tipo de análise é muito difícil, ou mesmo impossível de detectar.

4.8. **Plataforma de Gestão de Vulnerabilidades e Auditoria de Configurações de Ativos de Rede**

4.9. Uma vez entendido o funcionamento desse componente das ferramentas de gestão de vulnerabilidades fica fácil o entendimento do porquê o modelo de licenciamento atual de mercado para a plataforma de gestão de vulnerabilidades e auditoria de configurações de ativos de rede, baseia-se na quantidade de endereços IP's escaneados.

4.10. Como visto, a análise de vulnerabilidade objetiva detectar falhas em diversos componentes como: aplicações, softwares, equipamentos, sistemas operacionais, dentre outros. Deve-se fazer continuamente o processo de verificação e análise da rede, para que a mesma fique sempre atualizada e livre de acessos não permitidos e indesejáveis. Essa análise pode ser feita local e/ou remota.

4.11. Após tal análise são oferecidos relatórios com as respectivas soluções propostas. Nesses relatórios podem constar também itens dos quais objetiva-se melhorar a segurança do ambiente, não necessariamente relacionados às falhas encontradas. Divide-se em dois tipos: Ativa - Encontra-se e corrige-se as falhas, emitindo relatórios apenas do que foi feito. Passiva - Encontra-se as falhas e emite-se relatórios para que o cliente se encarregue de corrigir.

4.12. O relatório de análise de vulnerabilidades é constituído de informações essenciais que indicam a melhor estratégia para manter o ambiente da Organização protegido de falhas, ataques e invasões, através de uma avaliação completa, auxiliando de uma forma mais fácil e assertiva a tomada de decisão em relação à segurança da informação.

4.13. Conforme relatório técnico (Doc Sei nº 13742631) da Central IT, empresa contratada para prestação de serviço de *service desk* e sustentação de infraestrutura de tecnologia para organização, desenvolvimento, implantação e execução continuada de tarefas de suporte, rotina e demanda, compreendendo atividades de suporte técnico remoto e/ou presencial de 1º, 2º e 3º Níveis, a usuários de soluções de tecnologia da informação do MJSP, abrangendo a execução de rotinas periódicas, orientação e esclarecimento de dúvidas e recebimento, registro, análise, diagnóstico e atendimento de solicitações de usuários, sustentação e projetos de evolução do ambiente de infraestrutura tecnológica e gerenciamento de processos de Tecnologia da Informação e Comunicação - TIC, para o Ministério da Justiça e Segurança Pública e suas unidades regionais, o Ministério possui um total de 6.702 IP's e 8 domínios.

4.14. Segundo a Norma Complementar 04/IN1/DSIC/GSI/PR, ativos de informação são os meios de armazenamento, transmissão e processamento, os sistemas de informação, bem como os locais onde se encontram esses meios e as pessoas que a eles têm acesso.

4.15. Dada a grande quantidade de endereços IP's e de ativos de informação do Ministério da Justiça e Segurança Pública, conforme mencionado neste e em tópicos anteriores, a estratégia de segurança da informação da DTIC, visa priorizar num primeiro momento a proteção dos ativos estratégicos do Ministério. Deve-se ter em mente que os ativos estratégicos de uma organização são os ativos que permitem a sua diferenciação face às demais organizações e a sustentação do negócio no longo prazo.

4.16. Considerando que o modelo de licenciamento atual de mercado para a plataforma de gestão de vulnerabilidades e auditoria de configurações de ativos de rede, baseia-se na quantidade de endereços IP's escaneados e considerando o total 6.702 endereços de IP's atuais, acrescidos de uma **previsão de crescimento de 30%**(trinta) porcento, estima-se a necessidade de uma quantidade de licenças necessárias para **9.000** IP's, número arredondado para fins de cálculo.

4.17. A previsão de crescimento é baseada na quantidade de aquisições de equipamentos previstas no PDTIC 2021-2023 (13743301), sobretudo nas necessidades vinculadas as ações A0002, A0007, A0009, A0010, A0040, A0042, A0053, A0062, como também na implantação de novos sistemas Web, aplicações e soluções que requerem a instalação de novas máquinas virtuais.

4.18. Desta forma, **a aquisição deverá ocorrer por meio de 9 licenças contemplando 1.000 IP's cada uma, por ano**. Com as primeiras licenças adquiridas, serão analisados os Appliance de Segurança(14), os Ativos de rede(274), os Hosts físicos no Datacenter(84), os sistemas operacionais de servidores(917), os dispositivos de armazenamento (21), os servidores de aplicação(187) e as estações de trabalho da alta administração e colaboradores diretos. com as demais licenças adquiridas no período de um ano, será possível cobrir todo o parque computacional do Ministério.

4.19. Com essa estratégia procura-se evitar o que ocorre na maioria das vezes em outras organizações, quando os projetos de análise de vulnerabilidades terminam apenas com a entrega de diversos relatórios, e com poucas ações realizadas, o famoso projeto de relatório de gaveta. Além disso, os períodos entre as aquisições das licenças possibilitará a execução dos planos de ação, ao mesmo tempo em que trará economia de recursos. A Gestão de Vulnerabilidades compreende todo o ciclo de vida necessário para que as vulnerabilidades sejam tratadas, priorizadas, tendo acompanhamentos por períodos através de relatórios gerenciais e planos de ações factíveis.

4.20. **Solução de Análise em Aplicações Web**

4.21. Para compreender a necessidade dessa solução é importante entender como uma

ferramenta de análise funciona e a importância de realizar verificações de segurança em bibliotecas.

4.22. Os testes por análise dinâmica para aplicações web funcionam basicamente em dois passos:

1. 4.23. É executada uma varredura completa na aplicação, identificado as páginas e recursos por meio de navegação nas URLs, processo conhecido pelo termo em inglês *crawling*.
2. 4.24. Baseado no resultado na navegação, é inferido possíveis vulnerabilidades que o recurso possa ter. Então é realizado a tentativa de exploração da falha, desde a manipulação de cookies à injeção de SQL. Baseado na resposta do servidor, é possível identificar se a vulnerabilidade é explorável ou não.

4.25. Hoje a maior parte do código de uma aplicação é originado de bibliotecas de fonte aberto ou código proprietário. As bibliotecas são geralmente módulos de software de terceiros projetados para executar funções frequentemente necessárias. Elas fornecem mecanismos como suporte para acesso a dados, gerenciamento de recursos, comunicações e criação de interface com o usuário. Por isso, muitas vezes, as aplicações contém fragilidades que um atacante sem muito esforço possa explorar, sem necessitar um conhecimento prévio da aplicação.

4.26. Os pesquisadores de segurança periodicamente identificam vulnerabilidades em bibliotecas e disponibilizam os detalhes da descoberta através de um processo de divulgação de sua própria escolha. Algumas dessas divulgações são coordenadas com o CVE - Common Vulnerabilities and Exposures ou com o Open Source Vulnerability Database (OSVDB). Porém uma boa parte simplesmente são publicadas em posts de blogs ou e-mails para listas de discussão.

4.27. As vulnerabilidades que as bibliotecas podem conter colocam em risco a segurança da aplicação como um todo. O Ministério da Justiça e Segurança Pública, possui, pelo menos, 58 (cinquenta e oito) serviços críticos e essenciais, a maioria disponibilizado por meio de aplicações web, conforme relatório(13742757).

4.28. Demonstra-se dessa forma, a importância de identificar e tratar as vulnerabilidades desses sistemas, pois eles contém além de informações de segurança pública, informações de inteligência e dados pessoais que precisam ser protegidos.

4.29. **Consultoria Especializada**

4.30. Segundo dados do Portal de Gestão de Pessoas, disponível na intranet em janeiro de 2021, na Diretoria de Tecnologia da Informação e Comunicação trabalham 70 pessoas, sendo que destas apenas 8 são do quadro de ativo permanente, o que equivale a 11,42% do total. Já a Coordenação de Riscos e Segurança da Informação - CRS, responsável pela gestão e fiscalização da presente contratação, possui apenas 8 pessoas, sendo destas 4 contratos temporário, 1 Exercício Descentralizado e 3 requisitados, ou seja, não possui servidor do próprio quadro.

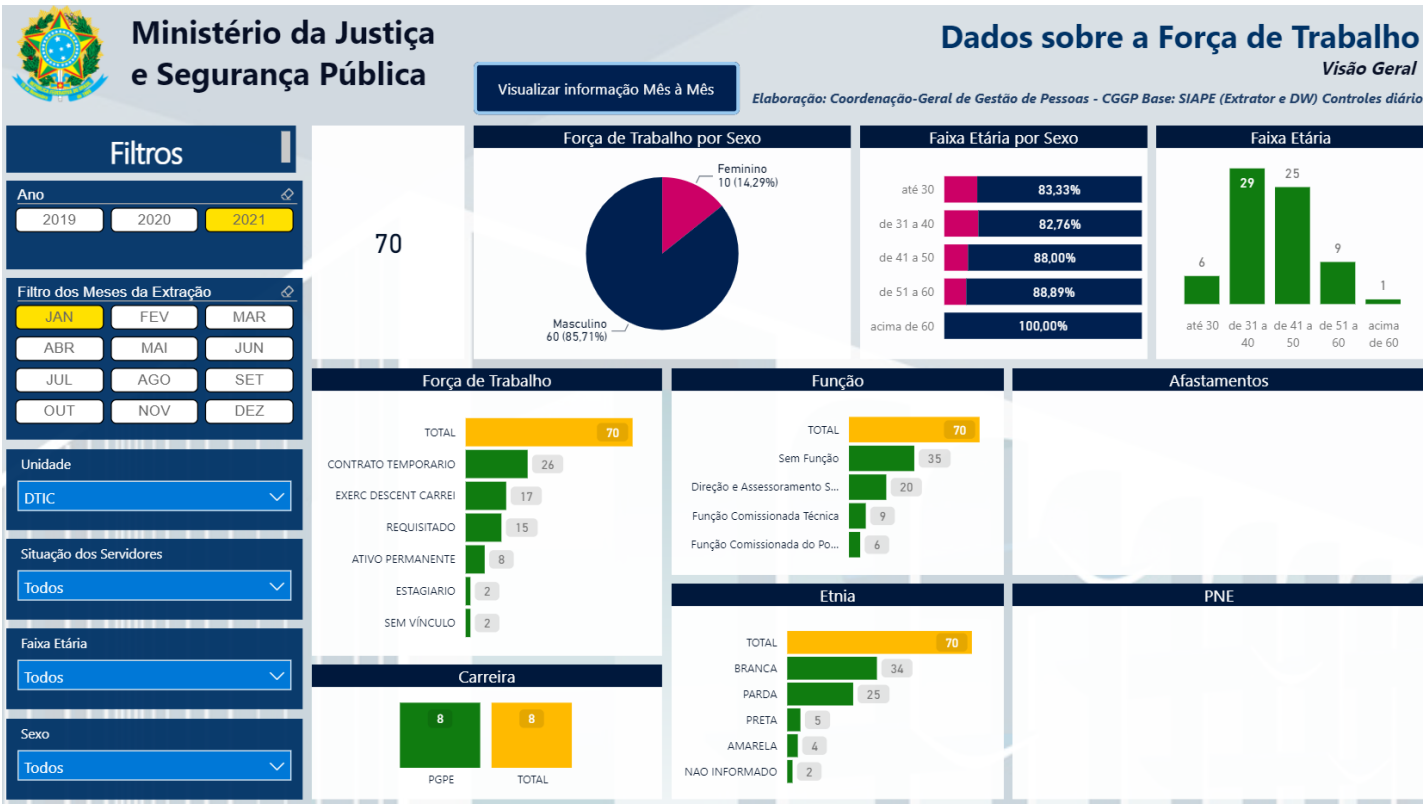


Imagem 6 - Força de trabalho do MJSP, Fonte: Portal Gestão de Pessoas, disponível em https://justicagovbr.sharepoint.com/sites/intra-CGGP/SitePages/For%C3%A7a-de-Trabalho.aspx, acesso em 19/01/2021.

4.31. A consultoria especializada será realizada sob demanda e tem como objetivos realizar as seguintes tarefas:

- 4.31.1. Esclarecer dúvidas de usuários em relação à operação do sistema;
- 4.31.2. Acompanhar, quando solicitado, todas as operações realizadas no sistema;
- 4.31.3. Prestar serviços de suporte técnico para a solução de problemas que impeçam o perfeito funcionamento do sistema;
- 4.31.4. Identificar problemas inerentes ao software e ao ambiente onde este se encontra instalado;
- 4.31.5. Discutir implementações de melhorias, visando possíveis adequações;
- 4.31.6. Produzir relatórios personalizados em diversos formatos;
- 4.31.7. Documentação e transferência de conhecimento das atividades técnicas realizadas;
- 4.31.8. Apoio no desenvolvimento de dashboard´s e solução de problemas internos, relativos às licenças adquiridas; e
- 4.31.9. Integração da solução com a ferramenta de ITSM utilizada pelo órgão.

4.32. Na prestação dos serviços de consultoria especializada, deverão ser utilizados profissionais com qualificação e treinamento adequados para o desenvolvimento das tarefas relacionadas anteriormente. Para a consultoria especializada foi estimado **480 horas por ano**, para cada solução, essa estimativa foi obtida considerando a média do tempo da análise de duas PoC's (*Proof of Concept),* prova de de conceito, de ferramentas de vulnerabilidades, considerando o tempo de varredura e o tempo de análise e também com base na análise de outras contratações de TIC do Ministério.

4.33. Portanto sugere-se que os itens a serem contratados , sejam os itens relacionados na tabela 1 - Relação de itens da contratação.

Objeto	Unidade	Quantidade
Licenciamento de plataforma de gestão de vulnerabilidades e auditoria de configurações de ativos de rede, contemplando no mínimo 1.000 endereços IP, por ano de uso, com garantia e atualização upgrade/update por até 24(vinte e quatro) meses	Licença	9
Consultoria Especializada	horas/ano	480
Licenciamento para solução de análise em aplicações Web, pacote para 8 (oito) domínios (FQDN), por ano de uso, com garantia e atualização upgrade/update por até 24(vinte e quatro) meses	Licença	1
Consultoria Especializada	horas/ano	480

Tabela 3 - Relação de itens da contratação

5. ANÁLISE DE SOLUÇÕES

5.1. Conforme inciso II do art. 11, deve-se verificar para composição da análise comparativa:

5.1.1. – A disponibilidade de solução similar em outro órgão ou entidade da Administração Pública;

5.1.2. – As alternativas do mercado;

5.1.3. – A existência de software público brasileiro;

5.1.4. – As políticas, os modelos e os padrões de governo, a exemplo do ePing, eMag, ePwg, ICP-Brasil e e-ARQ Brasil, quando aplicáveis;

5.1.5. – As necessidades de adequação do ambiente do órgão ou entidade para viabilizar a execução contratual (exemplo: mobiliário, instalação elétrica, espaço adequado para prestação do serviço, etc);

5.1.6. – A possibilidade de aquisição na forma de bens ou contratação como serviço;

5.1.7. – Os diferentes modelos de prestação do serviço;

5.1.8. – Os diferentes tipos de soluções em termos de especificação, composição ou características dos bens e serviços integrantes;

5.1.9. – A ampliação ou substituição da solução implantada.

5.1.10. Com base neste levantamento, cenários ou arranjos poderão ser formados para compor as soluções possíveis para atendimento da necessidade.

6. IDENTIFICAÇÃO DAS SOLUÇÕES

Id	Cenário 1
Solução	Utilização de solução do Portal do Software Público Brasileiro
Descrição	O Software Público Brasileiro é um tipo específico de software livre que atende às necessidades de modernização da administração pública de qualquer dos Poderes da União, dos Estados, do Distrito Federal e dos Municípios e é compartilhado sem ônus no Portal do Software Público Brasileiro, resultando na economia de recursos públicos e constituindo um recurso benéfico para a administração pública e para a sociedade.
Fornecedor	Portal do Software Público Brasileiro
Análise da Solução	O presente cenário tem o objetivo de analisar a adquisição junto ao Portal do Software Público Brasileiro para atender às necessidades do MJSP. O principal objetivo do Portal é promover o desenvolvimento de um "ambiente colaborativo que não só reduz os custos do governo, mas também permite o desenvolvimento de artefatos tecnológicos" (Santanna, 2007). De acordo com Santanna, "o conceito de utilização livre de código fonte - que deve sustentar as sociedades modernas - é central para o Portal do Software Público Brasileiro. A Administração Pública brasileira precisava de um ambiente no qual diversos atores sociais fossem capazes de compartilhar suas soluções já testadas e aprovadas a fim de evitar, entre outros fatores, a sobreposição de custos com outras soluções que são similares às que já existem" (Santanna, 2007). Além disso, o Portal colabora para a geração de emprego e renda, facilitando o contato entre pessoas que pretendem utilizar soluções informatizadas e aqueles que fornecem serviços. A rede estabelecida cria um complexo sistema de garantias econômicas, políticas e relações sociais que envolvem diversas esferas da sociedade. O software, neste contexto, não é apenas um produto, mas também um artefato por meio do qual seus criadores proporcionam novos referenciais de produção. Os atores neste cenário são simultaneamente produtores e consumidores, o que Tapscott & williams definem como os prosumers" (Tapscott & williams, 2007). Sempre que possível são utilizados softwares desenvolvidos na plataforma de Software público no ambiente de processamento central do MJSP, como por exemplo, os Sistema de Informação Eletrônica - SEI. Conforme pesquisa no portal de software público Brasileiro, registrada no documento SEI (13709507), Constam 81 softwares disponíveis no portal na data pesquisada, no entanto **não encontra-se disponível nenhuma solução de gestão de vulnerabilidades**. Conclui-se pelos fatos expostos que não é possível adotar os softwares disponíveis no Portal de Software Público Brasileiro para atender às necessidades do MJSP

Id	Cenário 2
Solução	Utilização de softwares livres
Descrição	Utilização de ferramentas livres ou gratuitas, como os softwares Wireshark, Nmap, Metasploit, OpenVas...
Fornecedor	Comunidades *Open Source* e páginas específicas dos projetos.
Análise da Solução	A solução proposta atende apenas parte da necessidade, pois a utilização desse cenário implica em não contar com suporte técnico especializado, ademais a atualização da base de vulnerabilidades e falhas não possui a mesma frequência de cenários com softwares pagos. Além disso, a adoção da solução proposta, por não possuir uma equipe dedicada de pesquisadores para avaliar e atualizar a ferramenta quando da descoberta de vulnerabilidades de dia zero não provê uma atualização tempestiva, não atendendo às necessidade do Ministério. A vulnerabilidade de dia zero é uma vulnerabilidade encontrada em um sistema, um hardware ou um software e pode ser uma porta para ameaças, como um ataque de malware. Em outras palavras, vulnerabilidade de dia zero é uma falha que precisa ser corrigida o mais rápido possível por causa dos riscos que ela gera para as organizações. Ela pode ocasionar uma exploração de dia zero, um ataque digital que faz uso das vulnerabilidades de dia zero para instalar softwares maliciosos em um dispositivo. Outro ponto desfavorável ao cenário apresentado é que os relatórios fornecidos pelas ferramentas não apresentariam rastreabilidade das atividades já realizadas nos ativos e sistemas, pois seriam utilizadas ferramentas de diferentes fabricantes para realização de diferentes atividades complementares. Seriam utilizadas, por exemplo, ferramentas específicas para detectar dispositivos remotos, como firewalls e roteadores com suas marcas e modelos, além da verificação de conexões e pacotes de rede como é o caso do Nmap e Wireshark. Outras ferramentas como o Metasploit e OpenVas para realizar exames rigorosos contra um conjunto de endereços IP e outras ferramentas de scanners para segurança de rede sem fio como Aircrack. Assim, como se vê a solução proposta não atende grande parte das necessidades tecnológicas e de negócio requeridas pelo Ministério.

Id	Cenário 3
Solução	Contratação de empresa especializada para fornecimento e instalação de solução de gestão de vulnerabilidades em ativos de tecnologia da informação e aplicações web, compreendendo a aquisição de serviços de Consultoria Especializada, suporte 24x7, com garantia (manutenção e suporte técnico)
Descrição	Aquisição de software de gerenciamento de vulnerabilidades em Ativos e web applications, com modelo de licenciamento anual
Fornecedores*	Brinqa, Digital Defense, Expanse, Kenna Security, NopSec, Outpost24, Qualys, Rapid7, RedSeal, RiskIQ, RiskSense, Skybox Security e Tenable
Fornecedores**	Synopsys, CheckMarx, Veracode, MicroFocus, Whitehat Security, Constrast Security, HCL Software, Rapid7, Onapsis, GitLab e CAST
Análise da Solução	Nesse cenário é contemplado a aquisição de solução baseada em nuvem (*cloud computing*). Essa solução apresenta facilidade de gerenciamento, valor de aquisição adequado e atualização automática da plataforma. No modelo de contratação em nuvem, todo o faturamento será na forma de custeio. Todas os requisitos de funcionalidades do projeto são atendidos por esse cenário. As soluções analisadas Qualys (VM e WAS) e Tenable.io conseguem fazer o gerenciamento de vulnerabilidades em ativos de tecnologia da informação além de testes em aplicações Web. Ambas foram testadas com versão de avaliação e os resultados e relatórios se mostraram adequados.

* Fonte: Relatório The Forrester Wave™: Vulnerability Risk Management, Q4 2019. The 13 providers that matter most and How they Stack Up. (Fornecedores de ferramentas de vulnerabilidades em ativos)

** Fonte Gartner (April 2020) (Fornecedores de ferramentas de vulnerabilidades em Aplicações)

7. ANÁLISE COMPARATIVA DE SOLUÇÕES

7.1. Consiste em uma análise crítica entre as diferentes soluções, considerando o aspecto econômico (TCO) entre as Soluções e os aspectos qualitativos em termos de benefícios para o alcance dos objetivos da contratação.

Requisito	Solução	Sim	Não	Não se Aplica
A Solução encontra-se implantada em outro órgão ou entidade da Administração Pública?	Solução 1			X
	Solução 2	X		
	Solução 3	X		
A Solução está disponível no Portal do Software Público Brasileiro? (quando se tratar de software)	Solução 1		X	
	Solução 2		X	
	Solução 3		X	
A Solução é composta por software livre ou software público? (quando se tratar de software)	Solução 1			X
	Solução 2	X		
	Solução 3		X	
A Solução é aderente às políticas, premissas e especificações técnicas definidas pelos Padrões de governo ePing, eMag, ePWG?	Solução 1			X
	Solução 2			X
	Solução 3			X
A Solução é aderente às regulamentações da ICP-Brasil? (quando houver necessidade de certificação digital)	Solução 1			X
	Solução 2			X
	Solução 3			X
A Solução é aderente às orientações, premissas e especificações técnicas e funcionais do e-ARQ Brasil? (quando o objetivo da solução abranger documentos arquivísticos)	Solução 1			X
	Solução 2			X
	Solução 3			X

8. REGISTRO DE SOLUÇÕES CONSIDERADAS INVIÁVEIS

8.1. Conforme § 1º do art. 11, 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.

CENÁRIO 1	
Análise da Solução	Não existe solução disponível no Portal do Software Público Brasileiro.
CENÁRIO 2	
Análise da Solução	A solução proposta atende apenas parte da necessidade, pois a utilização desse cenário implica em não contar com suporte técnico especializado, além disso a atualização da base de vulnerabilidades e falhas não possui a mesma frequência de cenários com softwares pagos.

9. ANÁLISE COMPARATIVA DE CUSTOS (TCO)

9.1. <Conforme inciso III do art. 11, deve-se proceder a comparação de custos totais de propriedade para as soluções técnica e funcionalmente viáveis>.

Cenário	Estimativa (R$)
1.	R$ 0,00
2.	R$ 0,00
3.	R$ 3.982.447,80

10. CÁLCULO DOS CUSTOS TOTAIS DE PROPRIEDADE

Solução Viável 1
Custo Total de Propriedade – Memória de Cálculo
Cálculo do Custo Total de Propriedade da Solução 3, considerando os custos inerentes ao ciclo de vida dos bens e serviços da solução, incluindo custos direitos e indiretos, a exemplo dos valores de aquisição dos ativos, insumos, garantia, manutenção, etc. Será disponibilizado na fase de Pesquisa de Preço.

11. MAPA COMPARATIVO DOS CÁLCULOS TOTAIS DE PROPRIEDADE (TCO)

Descrição da solução	Estimativa de TCO ao longo dos anos					Total
	Ano 2021	Ano 2022	Ano 2023	Ano 2024	Ano 2025	
Contratação de empresa especializada para fornecimento e instalação de solução unificada de gestão de vulnerabilidades em ativos de tecnologia da informação e aplicações web, compreendendo a aquisição de serviços de operação assistida e Consultoria	**R$ 2.532.748,47**	**R$ 1.355.134,53**	**R$ 2.627.313,27**	**R$ 1.355.134,53**	**R$ 1.408.221,43**	**R$ 9.278.552,23**

Especializada, suporte 24x7, com garantia (manutenção e suporte técnico)						

12. **DESCRIÇÃO DA SOLUÇÃO DE TIC A SER CONTRATADA**

12.1. **Contratação de empresa especializada para fornecimento e instalação, por meio de subscrição de licenças de software, de solução de avaliação de vulnerabilidades em ativos de tecnologia da informação e aplicações web, compreendendo a aquisição de serviços de consultoria especializada, suporte 24x7, com garantia (manutenção e suporte técnico) para o Ministério da Justiça e Segurança Pública (MJSP), incluindo a garantia de atualização das versões, pelo período de 24(vinte e quatro) meses, podendo ser prorrogada até o prazo máximo de 48(quarenta e oito) meses.**

12.2. A presente aquisição visa suprir o Ministério da Justiça e Segurança Pública com o aparato tecnológico necessário para o efetivo cumprimento da sua missão de trabalhar para a consolidação do Estado Democrático de Direito e de sua visão em ser reconhecido pela sociedade como protagonista na defesa da cidadania, na proteção de direitos, na integração da política de segurança pública, na cooperação jurídica internacional e no combate à corrupção, ao crime organizado e ao crime violento.

12.3. Nesse sentido, o fortalecimento e ampliação da estrutura e dos serviços de tecnologia da informação e comunicação contribuem, invariavelmente, para o aumento de desempenho dos servidores que atuam diretamente nas áreas finalísticas. Desta forma, a presente aquisição busca o alinhamento estratégico entre a área de Tecnologia da Informação e as áreas de negócio do Ministério da Justiça e Segurança Pública.

12.4. Na sociedade contemporânea, ao mesmo tempo em que as informações são consideradas os principais ativos de uma organização, as mesmas estão também sob o constante risco. por isso, sua perda ou vazamento constitui um enorme prejuízo para as organizações. Principalmente, para um órgão como o Ministério da Justiça e segurança pública que atua, dentre outras, em áreas que envolvem Segurança Pública, combate à corrupção e lavagem de dinheiro, proteção e defesa do consumidor, repressão ao tráfico ilícito de drogas, operações policiais e atividades de inteligência, a ocorrência de tais eventos deve ser salvaguardada.

12.5. A adoção de um processo de gestão de vulnerabilidades com o objetivo de reduzir drasticamente problemas como malwares, contas inativas, senhas ruins ou sistemas desatualizados, bem como a mitigação de riscos e a proteção de dados, é o que se espera com a utilização de uma ferramenta como a solução a ser contratada.

12.6. Tem-se a clareza de que um processo de gestão de vulnerabilidades é muito maior e mais complexo que apenas a execução de uma ferramenta e que de forma básica todo processo de gestão de vulnerabilidades deve apresentar no mínimos as etapas de **Identificação de vulnerabilidades; Verificação da vulnerabilidade; Mitigação de Vulnerabilidades e Remediação de Vulnerabilidades**. No entanto, a escolha de uma ferramenta de avaliação de vulnerabilidades é um pré requisito conforme demonstra a imagem 7, nova estrutura de orientação para gerenciamento de vulnerabilidades (disponível em https://blogs.gartner.com/augusto-barros/2019/10/25/new-vulnerability-management-guidance-framework/ acesso 15/04/2021).

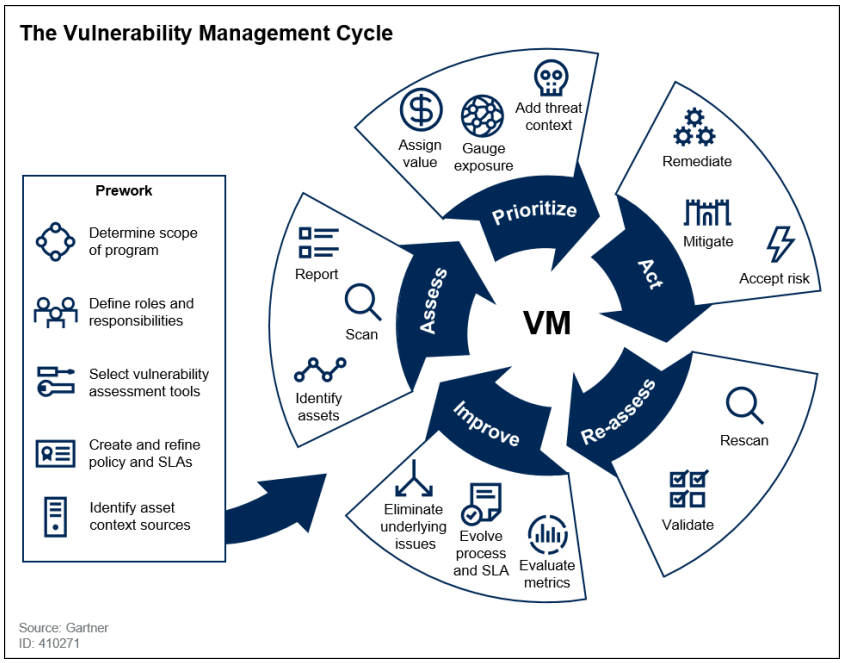


Imagem 7 - Nova estrutura de orientação para gerenciamento de vulnerabilidades (disponível em https://blogs.gartner.com/augusto-barros/2019/10/25/new-vulnerability-management-guidance-framework/ acesso 15/04/2021)

12.7. Ressalta-se que a contratação está alinhada com as boas práticas e aos normativos e padrões de segurança da informação, como por exemplo, a norma ABNT NBR ISO/IEC 27002 que fornece diretrizes para práticas de gestão de segurança da informação e normas de segurança da informação para as organizações, incluindo a seleção, a implementação e o gerenciamento de controles, levando em consideração os ambientes de risco da segurança da informação da organização.

12.8. A gestão de vulnerabilidades técnicas, a qual tem por objetivo prevenir a exploração de vulnerabilidades técnicas, é um dos controles comumente aceitos e necessário dentro do processo de implementação de um sistema de gestão da segurança da informação baseado na ABNT NBR ISO/IEC 27001 descrita no item 12.6.

12.9. A contratação está alinhada, também, a Lei Geral de Proteção de Dados Pessoais (LGPD), a qual no Capítulo VII que trata da segurança e das boas práticas, dispõe no artigo 46 que os agentes de tratamento devem adotar medidas de segurança, técnicas e administrativas aptas a proteger os dados pessoais de acessos não autorizados e de situações acidentais ou ilícitas de destruição, perda, alteração, comunicação ou qualquer forma de tratamento inadequado ou ilícito.

12.10. **Benefícios esperados com a contratação**

12.10.1. **Maior controle de segurança da informação e proteção de dados no âmbito do Ministério da Justiça e Segurança Pública**: através da redução de malwares, sistemas desatualizados, dentre outros problemas;

12.10.2. **Aumento dos esforços de correção e testes de eficácia**: as análises de vulnerabilidades de rede permitem não só a identificação de problemas de rede, mas também ajuda na sua priorização e no desenvolvimento de uma estratégia para lidar com aqueles mais críticos;

12.10.3. **Melhoria na gestão de mudanças e no gerenciamento de patches**: faz parte da gestão de vulnerabilidades centralizar e gerar todos os feedbacks sobre os problemas, as suas correções e as próximas ações;

12.10.4. **Fortalecimento da atuação da Equipes de Tratamento de Incidentes de**

Segurança nas Redes de computadores: A identificação e o tratamento das vulnerabilidades auxiliarão a ETIR na execução de suas responsabilidades de análise e respostas às notificações e atividades relacionadas a incidentes de segurança em redes de computadores além da redução desses incidentes;

12.10.5. **Apoio nas auditorias de Segurança da Informação e Comunicações** a obtenção de relatórios detalhados permitirá a devida diligência durante as auditorias;

12.10.6. **Atualização da Política de Segurança da Informação e Comunicações**: O gerenciamento de vulnerabilidades possibilitará aplicar melhorias na segurança da informação e na revisão da POSIC e suas normas complementares.

12.10.7. **Auxílio nos requisitos regulamentares**: A identificação e o tratamento das vulnerabilidades contribuirá para que o Ministério mantenha-se em conformidade com:

12.10.8. os normativos emanados pelo Departamento de Segurança da Informação e Comunicações do Gabinete de Segurança Institucional da Presidência da República;

12.10.9. os princípios e controles de segurança definidos nos padrões ABNT NBR ISO/IEC 27001, 27002, 27005, 27011 e 27014;

12.10.10. a Lei Nº 13.709, de 14 de agosto de 2018, Lei Geral de Proteção de Dados Pessoais (LGPD);

12.10.11. os frameworks de processos de governança e boas práticas como o ITIL e COBIT.

12.11. Nesta fase de planejamento da contratação, a equipe estimou o valor para a presente contratação para o período de 24 meses em **R$ 3.982.447,80 (três milhões, novecentos e oitenta e dois mil quatrocentos e quarenta e sete reais e oitenta centavos)**, valor este oriundo de levantamento prévio com várias empresas, entretanto será feito o levantamento da pesquisa de mercado por área competente dentro da Sede do Ministério da Justiça e Segurança Pública junto aos *players* do mercado de Tecnologia da Informação com, posterior, juntada ao Termo de Referência, para posterior análise desta equipe técnica.

13. ESTIMATIVA DE CUSTO TOTAL DA CONTRATAÇÃO PARA O MINISTÉRIO DA JUSTIÇA E SEGURANÇA PÚBLICA

13.1. Estima-se um custo total da contratação, para os cinco anos, o valor de R$ 9.278.552,23 (nove milhões, duzentos e setenta e oito mil quinhentos e cinquenta e dois reais e vinte e três centavos) .

14. DECLARAÇÃO DE VIABILIDADE DA CONTRATAÇÃO

14.1. De acordo com este estudo técnico preliminar da contratação, conclui-se que esta contratação está alinhada com as necessidades estratégicas elencadas no Plano Diretor de Tecnologia da Informação e Comunicação do Ministério da Justiça e Segurança Pública (2021-2023), sendo descritas e tratadas como macro requisitos e necessidades de negócio como serviço para tal finalidade.

14.2. Foram avaliadas as soluções disponíveis no mercado quanto à viabilidade técnica e econômica para o atendimento das necessidades deste órgão.

14.3. Após análise das soluções, suas vantagens, desvantagens, avaliação das necessidades de adequação e demais itens cabíveis, os Integrantes Técnico e Requisitante declaram que a contratação da solução é viável.

15. APROVAÇÃO E ASSINATURA

A Equipe de Planejamento da Contratação foi atualizada pela PORTARIA SAA Nº 64, DE 9 DE JULHO DE 2021 (15257536).

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

Integrante Técnico	
Nome	LUCAS REINEHR DE ANDRADE
Matrícula/SIAPE	3223177
Integrante Requisitante	
Nome	IVANILDO DE OLIVEIRA DA SILVA JR
Matrícula/SIAPE	1535600
Integrante Requisitante Substituto	
Nome	JOÉDES CARDOSO DA SILVA
Matrícula/SIAPE	3730955
Autoridade Máxima da Área de TIC (*OU AUTORIDADE SUPERIOR, SE APLICÁVEL – § 3º do art. 11*)	
Nome	RODRIGO LANGE
Matrícula/SIAPE	1558579

Documento assinado eletronicamente por **ALEXANDRA LACERDA FERREIRA RIOS**, **Pregoeiro(a)**, em 13/09/2021, às 13:44, com fundamento no § 3º do art. 4º do Decreto nº 10.543, de 13 de novembro de 2020.

A autenticidade do documento pode ser conferida no site http://sei.autentica.mj.gov.br informando o código verificador **15516784** e o código CRC **AFFEF861**
O trâmite deste documento pode ser acompanhado pelo site http://www.justica.gov.br/acesso-a-sistemas/protocolo e tem validade de prova de registro de protocolo no Ministério da Justiça e Segurança Pública.

DIÁRIO OFICIAL DA UNIÃO

Publicado em: 16/09/2020 | Edição: 178 | Seção: 1 | Página: 269

Órgão: Ministério da Justiça e Segurança Pública/Gabinete do Ministro

PORTARIA Nº 513, DE 15 DE SETEMBRO DE 2020

Dispõe sobre a implantação de Programa de Integridade em empresas contratadas pelo Ministério da Justiça e Segurança Pública.

O MINISTRO DE ESTADO DA JUSTIÇA E SEGURANÇA PÚBLICA-SUBSTITUTO, no uso das atribuições que lhe confere o inciso II do parágrafo único do art. 87 da CRFB, c/c o inciso III do art. 1º do Decreto nº 8.851, de 20 de setembro de 2016, e tendo em vista o disposto no inciso VIII do art. 7º da Lei nº 12.846, de 1º de agosto de 2013, nos arts. 41 e 42 do Decreto nº 8.420, de 18 de março de 2015, no parágrafo único do art. 7º da Portaria CGU nº 57, de 4 de janeiro de 2019, e no Anexo IX da Portaria MJSP nº 86, de 23 de março de 2020, e o consta no processo administrativo nº 08001.004150/2019-11, resolve:

Art. 1º Dispor sobre a implantação de Programa de Integridade em empresas contratadas pelo Ministério da Justiça e Segurança Pública.

Parágrafo único. Esta Portaria se aplica:

I - no caso de contratações cujos valores sejam iguais ou superiores a R$ 10.000.000,00 (dez milhões de reais); e

II - nos casos de contratações em que sejam celebrados termos aditivos para prorrogação da prestação de serviços continuados ou para efetivar acréscimos legais ao preço, ao ser atingida a alçada prevista no inciso I, pelo somatório dos valores.

Art. 2º São objetivos desta Portaria:

I - inserir as empresas contratadas na política e nas ações de integridade da administração pública;

II - contribuir para a redução dos riscos de práticas ilegais ou irregulares que possam gerar atos lesivos ou potencialmente lesivos aos princípios da administração pública, ao erário e à imagem do Ministério da Justiça e Segurança Pública;

III - prevenir a ocorrência de irregularidades relacionadas a desvios de conduta administrativa ou ética;

IV - orientar o relacionamento entre os agentes públicos e as empresas contratadas e seus dirigentes e funcionários; e

V - propiciar a prestação do serviço público com transparência e previsibilidade.

Art. 3º Deverá haver previsão expressa nos editais de licitação e em documentação prévia às contratações de que as empresas contratadas deverão se comprometer a implantar Programa de Integridade ou adequar seu Programa de Integridade já existente ao previsto nesta Portaria.

Art. 4º Os termos de referência e projetos básicos das contratações deverão conter cláusulas específicas com as obrigações deste Ministério e da empresa contratada relativamente às exigências de integridade, nos seguintes moldes:

I - das obrigações dos órgãos do Ministério da Justiça e Segurança Pública e seus agentes públicos:

a) não praticar atos para ingerência na administração da empresa contratada, especialmente quanto a direcionamento de escolha de possíveis trabalhadores;

b) para contratos de prestação de serviços com regime de dedicação exclusiva de mão de obra, não praticar atos tendentes a gerar vínculo empregatício entre os empregados da empresa contratada e o Ministério, vedando-se qualquer relação entre estes que caracterize pessoalidade e subordinação direta, atentando-se às vedações explícitas no art. 5º da Instrução Normativa SEGES/MPOG nº 5, de 26 de maio de 2017; e

c) notificar a empresa contratada, por escrito, sobre desvios de conduta, irregularidades, fraudes ou atos ilícitos, praticados na execução do contrato; e

II - das obrigações da empresa contratada:

a) estabelecer normas gerais de integridade:

1. em até 6 (seis) meses para contratos de até 12 (doze) meses; e

2. em até 9 (nove) meses para contratos de mais de 12 (doze) meses;

b) orientar seus empregados alocados para a execução do contrato sobre as normas de integridade e a indispensabilidade de seu cumprimento;

c) adotar práticas de governança e gestão capazes de identificar e mitigar desvios de conduta, irregularidades, fraudes e atos ilícitos, de acordo com as normas de integridade previstas na Lei nº 12.846, de 1º de agosto de 2013, e no Decreto nº 8.420, de 18 de março de 2015;

d) relatar ao órgão contratante, por escrito, qualquer descumprimento das normas de integridade praticado por agentes públicos com os quais mantenha contato em decorrência da execução do contrato;

e) substituir com presteza qualquer profissional que tenha cometido desvios de conduta, irregularidades, fraudes e atos ilícitos, conforme observado e notificado pelo agente público competente;

f) apresentar, no momento da celebração do contrato, Declaração de Inexistência de Vínculo Familiar, nos termos do art. 7º do Decreto nº 7.203, de 4 de junho de 2010, em que é assumido o compromisso de não utilizar, na execução do contrato, mão de obra que seja cônjuge, companheiro ou parente em linha reta ou colateral, por consanguinidade ou afinidade, até o terceiro grau, de agente público que exerce cargo em comissão ou função de confiança no âmbito do Ministério da Justiça e Segurança Pública;

g) apresentar à equipe de fiscalização do contrato, juntamente com o rol de documentos obrigatórios do empregado alocado para a execução do contrato, Termo de Ciência e Concordância, devidamente assinado pelo empregado, conforme modelo constante no anexo a esta Portaria; e

h) encaminhar à equipe de fiscalização do contrato, observados os prazos estabelecidos na alínea "a", documentação que evidencie, em alinhamento com os parâmetros do Capítulo IV do Decreto nº 8.420, de 2015, a realização das seguintes ações e atividades:

1. promoção e participação em reuniões, apresentações, palestras e quaisquer outros eventos de natureza semelhante que evidenciam o comprometimento da alta direção da empresa em temas relacionados à integridade;

2. mapeamento dos riscos de integridade e estabelecimento de ações mitigadoras, revisadas periodicamente;

3. canal de denúncia, aberto e amplamente divulgado, com garantia do devido sigilo ao denunciante;

4. código de ética ou de conduta aplicável a todos os dirigentes, administradores e empregados, independente de cargo, emprego, posto ou função exercidos;

5. treinamentos periódicos sobre o Programa de Integridade, que envolvam as vedações incidentes na relação público-privada;

6. promoção de campanhas para divulgar os princípios e valores que regem a empresa contratada e o serviço público, bem como outros temas sobre integridade e combate a desvios de conduta, fraudes, irregularidades e atos ilícitos;

7. adoção de medidas disciplinares, em caso de violação do Programa de Integridade, e de procedimentos e determinações que assegurem a pronta interrupção da tentativa ou da prática de desvios de conduta, fraudes, irregularidades e atos ilícitos;

8. monitoramento contínuo do Programa de Integridade, com objetivo de aperfeiçoar os mecanismos de prevenção de atos lesivos, bem como sua detecção e combate; e

9. encaminhamento semestral de relatório da execução do Programa de Integridade à equipe de fiscalização do contrato; e

i) cumprir e exigir que os empregados alocados para a execução do contrato nas repartições administrativas cumpram, no que couber, as regras estabelecidas pelos órgãos do Ministério da Justiça e Segurança Pública.

Art. 5º A implantação ou a adequação do Programa de Integridade poderá ser comprovada por qualquer documento hábil a ser encaminhado à equipe de fiscalização do contrato, preferencialmente, em meio digital.

Art. 6º Caberá à equipe de fiscalização do contrato acompanhar o cumprimento do prazo para apresentação dos documentos comprobatórios, que, após análise da conformidade das informações, deverá dar ciência à unidade do Ministério da Justiça e Segurança Pública responsável pelo Programa de Integridade e à empresa contratada.

§ 1º Após a implementação ou adequação do Programa de Integridade pela contratada, a equipe de fiscalização deverá realizar acompanhamento da execução do programa, por meio do relatório encaminhado pela empresa contratada, semestralmente.

§ 2º Em caso de descumprimento do envio do relatório semestral, o responsável pelo acompanhamento deverá notificar a empresa contratada e proceder com o registro do ocorrido.

§ 3º Em caso de descumprimento da obrigação de apresentar o Programa de Integridade dentro dos prazos estabelecidos, a equipe de fiscalização deverá tomar as providências cabíveis para a aplicação de penalidade à empresa contratada.

Art. 7º O descumprimento das obrigações previstas nesta Portaria ensejará aplicação das penalidades previstas e acordadas no contrato ou de penalidades de natureza administrativa, no caso dos agentes públicos.

Art. 8º Esta Portaria deverá constar como anexo dos editais referentes às licitações e contratações, inclusive em potencial, de que tratam os incisos do parágrafo único do art. 1º.

Art. 9º Esta Portaria entrará em vigor no dia 30 de novembro de 2020.

TERCIO ISSAMI TOKANO

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

ANEXO II DO EDITAL

VALORES MÁXIMOS ADMISSÍVEIS

Grupo	Item	Código SIASG CATSER	DESCRIÇÃO	Unidade de Medida	Quantidade			Valores Unitários
					MJSP	CADE	TOTAL	
1	1	27502	Licenciamento de plataforma de avaliação de vulnerabilidades e auditoria de configurações de ativos de rede, contemplando no mínimo 1.000 endereços IP, por ano de uso, com suporte técnico (24x7), treinamento e atualização upgrade/update, por 24 (vinte e quatro) meses	Licença	09	03	12	R$ 537.462,56
	2	27340	Serviço Técnico Especializado para avaliação de vulnerabilidades	Horas	960	960	1.920	R$ 556,80
2	3	27502	Licenciamento para solução de análise de segurança em aplicações Web, pacote para 8 (oito) domínios (FQDN), por ano de uso, com suporte técnico (24x7), treinamento e atualização upgrade/update, por 24 (vinte e quatro) meses	Licença	01	01	02	R$ 435.166,67
	4	27340	Serviço Técnico Especializado para avaliação de vulnerabilidades	Horas	960	960	1.920	R$ 482,38

Documento assinado eletronicamente por **ALEXANDRA LACERDA FERREIRA RIOS**, **Pregoeiro(a)**, em 13/09/2021, às 13:44, com fundamento no § 3º do art. 4º do Decreto nº 10.543, de 13 de novembro de 2020.

A autenticidade do documento pode ser conferida no site http://sei.autentica.mj.gov.br informando o código verificador **15516588** e o código CRC **0F128C6C**
O trâmite deste documento pode ser acompanhado pelo site

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

ANEXO III DO EDITAL

MINUTA ATA DE REGISTRO DE PREÇOS

O Ministério da Justiça e da Segurança Pública, com sede na Esplanada dos Ministérios, Bloco "T", Anexo II, sala 621, em Brasília – DF, CEP 70064-900, neste ato representado(a) pelo(a) ..... (*cargo e nome*), nomeado(a) pela Portaria nº ..... de ..... de ..... de 200..., publicada no ..... de ..... de ..... de ....., portador da matrícula funcional nº ....., considerando o julgamento da licitação na modalidade de pregão, na forma eletrônica, para REGISTRO DE PREÇOS nº ...../20..., publicada no ..... de ...../...../20....., processo administrativo nº 08006.001082/2020-13, RESOLVE registrar os preços da(s) empresa(s) indicada(s) e qualificada(s) nesta ATA, de acordo com a classificação por ela(s) alcançada(s) e na(s) quantidade(s) cotada(s), atendendo as condições previstas no edital, sujeitando-se as partes às normas constantes na Lei nº 8.666, de 21 de junho de 1993 e suas alterações, no Decreto nº 7.892, de 23 de janeiro de 2013, e em conformidade com as disposições a seguir:

1. DO OBJETO

1.1. A presente Ata tem por objeto o registro de preços para eventual prestação de serviços de implementação de solução para avaliação de vulnerabilidades em ativos de tecnologia da informação e aplicações web ao Ministério da Justiça e Segura Pública, compreendendo: a subscrição de licenças de software, abarcando a atualização, o treinamento e o suporte técnico (24x7); e o serviço técnico especializado, especificado no item 2.3 do Termo de Referência, anexo I do edital de Pregão nº ...../20..., que é parte integrante desta Ata, assim como a proposta vencedora, independentemente de transcrição.

2. DOS PREÇOS, ESPECIFICAÇÕES E QUANTITATIVOS

2.1. O preço registrado, as especificações do objeto e as demais condições ofertadas na(s) proposta(s) são as que seguem:

Prestador do serviço *(razão social, CNPJ/MF, endereço, contatos, representante)*							
Grupo	Item	Código SIASG CATSER	DESCRIÇÃO	Quantidade			Unidade de Medida
				MJSP	CADE	TOTAL	
1	1	27502	Licenciamento de plataforma de avaliação de vulnerabilidades e auditoria de configurações de ativos de rede, contemplando no mínimo 1.000 endereços IP, por ano de uso, com suporte técnico	09	03	12	Licença

1			(24x7), treinamento e atualização upgrade/update, por 24 (vinte e quatro) meses				
	2	27340	Serviço Técnico Especializado para avaliação de vulnerabilidades	960	960	1.920	Horas
2	3	27502	Licenciamento para solução de análise de segurança em aplicações Web, pacote para 8 (oito) domínios (FQDN), por ano de uso, com suporte técnico (24x7), treinamento e atualização upgrade/update, por 24 (vinte e quatro) meses	01	01	02	Licença
	4	27340	Serviço Técnico Especializado para avaliação de vulnerabilidades	960	960	1.920	Horas

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

3. ÓRGÃO (S) GERENCIADOR E PARTICIPANTE (S)

3.1. O órgão gerenciador será o Ministério da Justiça e Segurança Pública.

3.2. São órgãos e entidades públicas participantes do registro de preços:

Item nº	*Órgãos Participantes*
1	CADE
2	CADE
3	CADE
4	CADE

4. DA ADESÃO À ATA DE REGISTRO DE PREÇOS

4.1. Não será admitida a adesão à ata de registro de preços decorrente desta licitação.

5. VALIDADE DA ATA

5.1. A validade da Ata de Registro de Preços será de 12 meses, a partir da sua assinatura, não podendo ser prorrogada.

6. REVISÃO E CANCELAMENTO

6.1. A Administração realizará pesquisa de mercado periodicamente, em intervalos não superiores a 180 (cento e oitenta) dias, a fim de verificar a vantajosidade dos preços registrados nesta Ata

6.2. Os preços registrados poderão ser revistos em decorrência de eventual redução dos preços praticados no mercado ou de fato que eleve o custo do objeto registrado, cabendo à Administração promover as negociações junto ao(s) fornecedor(es)

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

6.4. O fornecedor que não aceitar reduzir seu preço ao valor praticado pelo mercado será liberado do compromisso assumido, sem aplicação de penalidade

6.4.1. A ordem de classificação dos fornecedores que aceitarem reduzir seus preços aos valores de mercado observará a classificação original *(Suprimir o item quando inexistirem outros fornecedores classificados registrados na ata.)*

6.5. Quando o preço de mercado tornar-se superior aos preços registrados e o fornecedor não puder cumprir o compromisso, o órgão gerenciador poderá:

6.5.1. liberar o fornecedor do compromisso assumido, caso a comunicação ocorra antes do pedido de fornecimento, e sem aplicação da penalidade se confirmada a veracidade dos motivos e

comprovantes apresentados; e

6.5.2. convocar os demais fornecedores para assegurar igual oportunidade de negociação.

6.6. Não havendo êxito nas negociações, o órgão gerenciador deverá proceder à revogação desta ata de registro de preços, adotando as medidas cabíveis para obtenção da contratação mais vantajosa.

6.7. O registro do fornecedor será cancelado quando:

6.7.1. descumprir as condições da ata de registro de preços;

6.7.2. não retirar a nota de empenho ou instrumento equivalente no prazo estabelecido pela Administração, sem justificativa aceitável;

6.7.3. não aceitar reduzir o seu preço registrado, na hipótese deste se tornar superior àqueles praticados no mercado; ou

6.7.4. sofrer sanção administrativa cujo efeito torne-o proibido de celebrar contrato administrativo, alcançando o órgão gerenciador e órgão(s) participante(s).

6.8. O cancelamento de registros nas hipóteses previstas nos itens 6.7.1, 6.7.2 e 6.7.4 será formalizado por despacho do órgão gerenciador, assegurado o contraditório e a ampla defesa.

6.9. O cancelamento do registro de preços poderá ocorrer por fato superveniente, decorrente de caso fortuito ou força maior, que prejudique o cumprimento da ata, devidamente comprovados e justificados:

6.9.1. por razão de interesse público; ou

6.9.2. a pedido do fornecedor

7. DAS PENALIDADES

7.1. O descumprimento da Ata de Registro de Preços ensejará aplicação das penalidades estabelecidas no Edital.

7.1.1. As sanções do item acima também se aplicam aos integrantes do cadastro de reserva, em pregão para registro de preços que, convocados, não honrarem o compromisso assumido injustificadamente, nos termos do art. 49, §1º do Decreto nº 10.024/19.

7.2. É da competência do órgão gerenciador a aplicação das penalidades decorrentes do descumprimento do pactuado nesta ata de registro de preço (art. 5º, inciso X, do Decreto nº 7.892/2013), exceto nas hipóteses em que o descumprimento disser respeito às contratações dos órgãos participantes, caso no qual caberá ao respectivo órgão participante a aplicação da penalidade (art. 6º, Parágrafo único, do Decreto nº 7.892/2013).

7.3. O órgão participante deverá comunicar ao órgão gerenciador qualquer das ocorrências previstas no art. 20 do Decreto nº 7.892/2013, dada a necessidade de instauração de procedimento para cancelamento do registro do fornecedor

8. CONDIÇÕES GERAIS

8.1. As condições gerais do fornecimento, tais como os prazos para entrega e recebimento do objeto, as obrigações da Administração e do fornecedor registrado, penalidades e demais condições do ajuste, encontram-se definidos no Termo de Referência, ANEXO AO EDITAL.

8.2. É vedado efetuar acréscimos nos quantitativos fixados nesta ata de registro de preços, inclusive o acréscimo de que trata o § 1º do art. 65 da Lei nº 8.666/93, nos termos do art. 12, §1º do Decreto nº 7.892/13.

8.3. No caso de adjudicação por preço global de grupo de itens, só será admitida a contratação dos itens nas seguintes hipóteses.

8.3.1. contratação da totalidade dos itens de grupo, respeitadas as proporções de quantitativos definidos no certame; ou

8.3.2. contratação de item isolado para o qual o preço unitário adjudicado ao vencedor seja o menor preço válido ofertado para o mesmo item na fase de lances

8.4. A ata de realização da sessão pública do pregão, contendo a relação dos licitantes que aceitarem cotar os bens ou serviços com preços iguais ao do licitante vencedor do certame, será anexada a esta Ata de Registro de Preços, nos termos do art. 11, §4º do Decreto n. 7.892, de 2013.

Para firmeza e validade do pactuado, a presente Ata foi lavrada que, depois de lida e achada em ordem, vai assinada pelas partes e encaminhada cópia aos demais órgãos participantes.

Local e data

Assinaturas

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

Documento assinado eletronicamente por **ALEXANDRA LACERDA FERREIRA RIOS**, **Pregoeiro(a)**, em 13/09/2021, às 13:44, com fundamento no § 3º do art. 4º do Decreto nº 10.543, de 13 de novembro de 2020.

A autenticidade do documento pode ser conferida no site http://sei.autentica.mj.gov.br informando o código verificador **15516620** e o código CRC **A988BF82**
O trâmite deste documento pode ser acompanhado pelo site http://www.justica.gov.br/acesso-a-sistemas/protocolo e tem validade de prova de registro de protocolo no Ministério da Justiça e Segurança Pública.

Referência: Processo nº 08006.001082/2020-13 SEI nº 15516620

Ministério da Justiça e Segurança Pública
Secretaria-Executiva

Esplanada dos Ministérios, Bloco T, Anexo II, - Bairro Zona Cívico Administrativa, Brasília/DF, CEP 70064-900
Telefone: (61) 2025-7645 - - www.justica.gov.br

ANEXO IV DO EDITAL

MINUTA DE CONTRATO

Minuta de Contrato Nº 9048696/2019-DICON/CCONT/CGL/SAA/SE

MINUTA DE TERMO DE CONTRATO Nº ...../2021

TERMO DE CONTRATO DE PRESTAÇÃO DE SERVIÇOS Nº ___/2021 QUE FAZEM ENTRE SI A UNIÃO, REPRESENTADA PELO MINISTÉRIO DA JUSTIÇA SEGURANÇA PÚBLICA, POR INTERMÉDIO DA DIRETORIA DE TECNOLOGIA INFORMAÇÃO E COMUNICAÇÃOE DA COORDENAÇÃO-GERAL DE LICITAÇÕES CONTRATOS, E A EMPRESA xxxxxxxxxxxxxxxxxx.

PROCESSO Nº 08006.001082/2020-13

A União, representada pelo **MINISTÉRIO DA JUSTIÇA E SEGURANÇA PÚBLICA**, com sede à Esplanada dos Ministérios, CEP 70064-900, Brasília/DF, inscrito no CNPJ n° 00.394.494/0013-70, neste ato representado por intermédio do xxxxxxxxxxxxxxxxxxxxxxxxxx, Senhor **xxxxxxxxxxxxxx**, xxxxxxxxxxxxxxx, xxxxxxxxxxxxxxxxx, portador do RG nº xxxxxxxxxxxxxxxxx - e CPF nº xxxxxxxxxxxxxxxxxxxxxxx, nomeado por meio da Portaria n° xxxxxx de xx de xxxxxxxxxxxx de 20xx, publicada no D.O.U. de xx de xxxxxx de 20xx, e da **Sra. DÉBORA DE SOUZA JANUÁRIO**, brasileira, solteira, portadora do RG nº 3.558.79980–SSP/SP e do CPF nº 712.315.791-53, nomeada por meio da Portaria n° 1.087, de 06 de novembro de 2015, publicada no D.O.U. de 09 de novembro de 2015 e com delegação de competência fixada pela Portaria nº 49, de 22 de agosto de 2018, publicada no D.O.U. de 23 de agosto de 2018, doravante denominado **CONTRATANTE**, e a Empresa **XXXXXXXXXXXXXXXXX.**, inscrita no CNPJ n° XXXXXXXXXX e inscrição estadual n° XXXXXXXX, estabelecida XXXXXXXXXXX - CEP XXXXXXX, neste ato representada pelo **xxxxxxx**, CPF n° xxxxxxx, RG n° xxxxxx, doravante denominada **CONTRATADA**, tendo em vista o que consta no Processo nº 08006.001082/2020-13, e em observância às disposições da Lei nº 8.666, de 21 de junho de 1993, da Lei nº 10.520, de 17 de julho de 2002, da Lei nº 8.248, de 22 de outubro de 1991, *do Decreto nº 7.892, de 23 de janeiro de 2013*, do Decreto nº 9.507, de 21 de setembro de 2018, do Decreto nº 7.174, de 12 de maio de 2010, da Instrução Normativa SGD/ME nº 1, de 4 de Abril de 2019 e da Instrução Normativa SEGES/MPDG nº 5, de 26 de maio de 2017 e suas alterações, resolvem celebrar o presente Termo de Contrato, decorrente do Pregão *por Sistema de Registro de Preços* nº ...../20...., mediante

as cláusulas e condições a seguir enunciadas.

1. CLÁUSULA PRIMEIRA – OBJETO

1.1. O objeto do presente instrumento é a contratação de empresa especializada, mediante Sistema de Registro de Preços, para prestação de serviços de implementação de solução para avaliação de vulnerabilidades em ativos de tecnologia da informação e aplicações web ao Ministério da Justiça e Segura Pública, compreendendo: a subscrição de licenças de software, abarcando a atualização, o treinamento e o suporte técnico (24x7); e o serviço técnico especializado, conforme as especificações e demais condições de execução contidas 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. Objeto da contratação:

Item	DESCRIÇÃO	Quantidade	Unidade de Medida	Valor Unitário	Valor Total
1	Licenciamento de plataforma de avaliação de vulnerabilidades e auditoria de configurações de ativos de rede, contemplando no mínimo 1.000 endereços IP, por ano de uso, com suporte técnico (24x7), treinamento e atualização upgrade/update, por 24 (vinte e quatro) meses		Licença		
2	Serviço Técnico Especializado para avaliação de vulnerabilidades		Horas		
3	Licenciamento para solução de análise de segurança em aplicações Web, pacote para 8 (oito) domínios (FQDN), por ano de uso, com suporte técnico (24x7), treinamento e atualização upgrade/update, por 24 (vinte e quatro) meses		Licença		
4	Serviço Técnico Especializado para avaliação de vulnerabilidades		Horas		

2. CLÁUSULA SEGUNDA - VIGÊNCIA

2.1. O prazo de vigência deste Termo de Contrato é aquele fixado no Edital, com início na data de ...../...../..... e encerramento em ...../...../....., podendo ser prorrogado por interesse das partes limite de 48 (quarenta e oito) meses, com base no artigo 57, IV, da Lei 8.666, de 1993, atentando, em especial para o cumprimento dos seguintes requisitos:

2.1.1. Esteja formalmente demonstrado que a forma de prestação dos serviços tem natureza continuada;

2.1.2. Seja juntado relatório que discorra sobre a execução do contrato, com informações de que os serviços tenham sido prestados regularmente;

2.1.3. Seja juntada justificativa e motivo, por escrito, de que a Administração mantém interesse na realização do serviço;

2.1.4. Seja comprovado que o valor do contrato permanece economicamente vantajoso para a Administração;

2.1.5. Haja manifestação expressa da contratada informando o interesse na prorrogação;

2.1.6. Seja comprovado que a contratada mantém as condições iniciais de habilitação.

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

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

3. CLÁUSULA TERCEIRA – PREÇO

3.1. O valor total da contratação é de R$..... (.....).

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

3.3. O valor acima é meramente estimativo, de forma que os pagamentos devidos à CONTRATADA dependerão dos quantitativos de serviços efetivamente prestados.

4. CLÁUSULA QUARTA– DOTAÇÃO ORÇAMENTÁRIA

4.1. As despesas decorrentes desta contratação estão programadas em dotação orçamentária própria, prevista no orçamento da União, para o exercício de 2021, na classificação abaixo:

4.2. Programa de Trabalho:

4.3. Natureza da Despesa:

4.4. Plano Interno:

4.5. Ptres:

4.6. Fonte:

4.7. Ação:

4.8. PO:

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

5. CLÁUSULA QUINTA – PAGAMENTO

5.1. O prazo para pagamento à CONTRATADA e demais condições a ele referentes encontram-se definidos no Termo de Referência e no Anexo XI da IN SEGES/MP n. 5/2017.

6. CLÁUSULA SEXTA – REAJUSTAMENTO DE PREÇOS EM SENTIDO AMPLO

6.1. 1.1. As regras acerca do reajustamento de preços em sentido amplo do valor contratual (reajuste em sentido estrito e/ou repactuação) são as estabelecidas no Termo de Referência, anexo do Edital.

7. CLÁUSULA SÉTIMA – GARANTIA DE EXECUÇÃO

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

8. CLÁUSULA OITAVA – MODELO DE EXECUÇÃO DOS SERVIÇOS E FISCALIZAÇÃO

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

9. CLÁUSULA NONA – OBRIGAÇÕES DA CONTRATANTE E DA CONTRATADA

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

10. CLÁUSULA DÉCIMA - SANÇÕES ADMINISTRATIVAS.

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

11. CLÁUSULA DÉCIMA PRIMEIRA - RESCISÃO

11.1. O presente Termo de Contrato poderá ser rescindido:

11.1.1. por ato unilateral e escrito da Administração, nas situações previstas nos incisos I a XII e XVII do art. 78 da Lei nº 8.666, de 1993, e com as consequências indicadas no art. 80 da mesma Lei, sem prejuízo da aplicação das sanções previstas no Termo de Referência, anexo ao Edital;

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

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

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

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

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

11.4.2. Relação dos pagamentos já efetuados e ainda devidos;

11.4.3. Indenizações e multas.

12. CLÁUSULA DÉCIMA SEGUNDA – VEDAÇÕES E PERMISSÕES

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

12.2. É permitido à CONTRATADA caucionar ou utilizar este Termo de Contrato para qualquer operação financeira, nos termos e de acordo com os procedimentos previstos na Instrução Normativa SEGES/ME nº 53, de 8 de Julho de 2020.

12.2.1. A cessão de crédito, a ser feita mediante celebração de termo aditivo, dependerá de comprovação da regularidade fiscal e trabalhista da cessionária, bem como da certificação de que a cessionária não se encontra impedida de licitar e contratar com o Poder Público, conforme a legislação em vigor, nos termos do Parecer JL-01, de 18 de maio de 2020.

12.2.2. A crédito a ser pago à cessionária é exatamente aquele que seria destinado à cedente (contratada) pela execução do objeto contratual, com o desconto de eventuais multas, glosas e prejuízos causados à Administração, sem prejuízo da utilização de institutos tais como os da conta vinculada e do pagamento direto previstos na IN SEGES/ME nº 5, de 2017, caso aplicáveis.

13. CLÁUSULA DÉCIMA TERCEIRA – ALTERAÇÕES

13.1. Eventuais alterações contratuais reger-se-ão pela disciplina do art. 65 da Lei nº 8.666, de 1993, bem como do ANEXO X da IN/SEGES/MPDG nº 05, de 2017.

13.2. A CONTRATADA é obrigada a aceitar, nas mesmas condições contratuais, os acréscimos ou supressões que se fizerem necessários, até o limite de 25% (vinte e cinco por cento) do valor inicial atualizado do contrato.

13.3. As supressões resultantes de acordo celebrado entre as partes contratantes poderão exceder o limite de 25% (vinte e cinco por cento) do valor inicial atualizado do contrato.

14. CLÁUSULA DÉCIMA QUARTA – DOS CASOS OMISSOS

14.1. Os casos omissos serão decididos pela CONTRATANTE, segundo as disposições

contidas na Lei nº 8.666, de 1993, na Lei nº 10.520, de 2002 e demais normas federais aplicáveis e, subsidiariamente, segundo as disposições contidas na Lei nº 8.078, de 1990 – Código de Defesa do Consumidor – e normas e princípios gerais dos contratos.

15. CLÁUSULA DÉCIMA QUINTA – PUBLICAÇÃO

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

16. CLÁUSULA DÉCIMA SEXTA - FORO

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

17. CLÁUSULA DÉCIMA SÉTIMA – DA ASSINATURA ELETRÔNICA E/OU DIGITAL

17.1. O presente instrumento será firmado através de assinatura eletrônica e/ou digital, certificada pelo Sistema Eletrônico de Informações - SEI do Ministério da Justiça e Segurança Pública - MJSP, garantida a eficácia das Cláusulas.

17.2. Em conformidade com o disposto no § 2º, art. 10, da MPV 2.200/01, a assinatura deste termo pelo representante oficial da CONTRATADA, pressupõe declarada, de forma inequívoca, a sua concordância, bem como o reconhecimento da validade e do aceite ao presente documento.

17.3. A respectiva autenticidade poderá ser atestada a qualquer tempo, seguindo os procedimentos impressos na nota de rodapé, não podendo, desta forma, as partes se oporem a sua utilização.

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

DÉBORA DE SOUZA JANUÁRIO
xxxxxxxxxxxxxxxxxxxxxx
Coordenadora-Geral de Licitações e Contratos
xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx
Ministério da Justiça e Segurança Pública

Ministério da Justiça e Segurança Pública

xxxxxxxxxxxxxxxxxxxxxxx

Representante da Contratada

TESTEMUNHAS:

1. NOME:

CPF:

2. NOME:

CPF:

em 13/09/2021, às 13:44, com fundamento no § 3º do art. 4º do Decreto nº 10.543, de 13 de novembro de 2020.

A autenticidade do documento pode ser conferida no site http://sei.autentica.mj.gov.br informando o código verificador **15798489** e o código CRC **CAD0E2AA**
O trâmite deste documento pode ser acompanhado pelo site http://www.justica.gov.br/acesso-a-sistemas/protocolo e tem validade de prova de registro de protocolo no Ministério da Justiça e Segurança Pública.

Referência: Processo nº 08006.001082/2020-13 SEI nº 15798489

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

ANEXO V DO EDITAL

DECLARAÇÃO DE CIÊNCIA SOBRE A IMPLANTAÇÃO DO PROGRAMA DE INTEGRIDADE

Nos termos do item 5.7 do Edital do Pregão Eletrônico nº ___/2021, a empresa _____, portadora do CNPJ nº _____, declara ciência que deverá implantar o Programa de Integridade estabelecido pela Portaria MJSP nº 513, de 15 de setembro de 2020, em conformidade com as orientações previstas no Termo de Referência.

Data

Assinatura

Documento assinado eletronicamente por **ALEXANDRA LACERDA FERREIRA RIOS**, **Pregoeiro(a)**, em 13/09/2021, às 13:44, com fundamento no § 3º do art. 4º do Decreto nº 10.543, de 13 de novembro de 2020.

A autenticidade do documento pode ser conferida no site http://sei.autentica.mj.gov.br informando o código verificador **15798182** e o código CRC **E31E5165**
O trâmite deste documento pode ser acompanhado pelo site http://www.justica.gov.br/acesso-a-sistemas/protocolo e tem validade de prova de registro de protocolo no Ministério da Justiça e Segurança Pública.