16832818 08006.000003/2021-38

MINISTÉRIO DA JUSTIÇA E SEGURANÇA PÚBLICA

EDITAL DE LICITAÇÃO
PREGÃO ELETRÔNICO Nº 21/2021
(08006.000003/2021-38)

Torna-se público que a União, por intermédio do Ministério da Justiça e Segurança Pública, por meio do Pregoeiro designado pela Portaria nº 251, de 02 de dezembro de 2021, da Coordenação-Geral de Licitações e Contratos da Subsecretaria de Administração, publicada no D.O.U. de 06 de dezembro de 2021, da Coordenação-Geral de Licitações e Contratos da Subsecretaria de Administração (UASG 200005), realizará licitação, na modalidade PREGÃO, na forma ELETRÔNICA, **com o critério de julgamento menor preço por grupo**, sob a forma de execução indireta, no regime de **empreitada por preço global para o grupo 1 e regime de empreitada unitário para o grupo 2**, nos termos da Lei nº 10.520, de 17 de julho de 2002, da Lei nº 8.248, de 22 de outubro de 1991, do Decreto nº 10.024, de 20 de setembro de 2019, do Decreto 9.507, de 21 de setembro de 2018, do Decreto nº 7.746, de 05 de junho de 2012, do Decreto nº 7.174, de 12 de maio de 2010, da Instrução Normativa SGD/ME nº 1, de 4 de abril de 2019, das Instruções Normativas SEGES/MP nº 05, de 26 de maio de 2017 e nº 03, de 26 de abril de 2018 e da Instrução Normativa SLTI/MPOG nº 01, de 19 de janeiro de 2010, da Lei Complementar n° 123, de 14 de dezembro de 2006, da Lei nº 11.488, de 15 de junho de 2007, do Decreto n° 8.538, de 06 de outubro de 2015, aplicando-se, subsidiariamente, a Lei nº 8.666, de 21 de junho de 1993 e as exigências estabelecidas neste Edital.

Data da sessão: 17/01/2022

Horário: 09:00

Local: Portal de Compras do Governo Federal – *https://www.gov.br/compras/pt-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, através da seleção de empresa especializada, para o fornecimento de Serviço de Centro de Operações de Segurança (Security Operations Center - SOC) com funcionamento e suporte 24h por dia e 7 dias por semana, Serviço de tratamento e resposta aos incidentes cibernéticos - CSIRT - Blue Team e Serviço de teste de invasão - Red Team e garantia dos serviços pelo período de 24(vinte e quatro) meses, renováveis até o limite de 60 (sessenta) meses, para o atendimento das necessidades da Diretoria de Tecnologia da Informação e Comunicação - DTIC do Ministério da Justiça e Segurança Pública - MJSP, conforme condições, quantidades e exigências estabelecidas neste Edital e seus anexos.

1.2. A licitação será dividida em 2 (dois) grupos, formados por 2 (dois) itens cada um, conforme Tabela 1 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 menor preço GLOBAL do grupo, observadas as exigências contidas neste Edital e seus Anexos quanto às especificações do objeto.

1.4. Cada serviço 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 2021, e será incluído proporcionalmente na LOA 2022 e 2023, mediante orçamento a ser disponibilizado pelas áreas demandantes em momento oportuno, para custear despesas com a contratação de empresa especializada, na classificação abaixo:

2.1.1. Gestão/Unidade: 200005

2.1.2. Fonte: 0100000000

2.1.3. Programa de Trabalho: 172184 (PTRES)

2.1.4. Elemento de Despesa: 339040

2.1.5. PI: GL67OTCGLTI

3. DO CREDENCIAMENTO

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

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

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

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

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

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

4. DA PARTICIPAÇÃO NO PREGÃO

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

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

4.2. Não poderão participar desta licitação os interessados:

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

4.2.2. que não atendam às condições deste Edital e seus anexos;

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

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

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

4.2.6. entidades empresariais que estejam reunidas em consórcio;

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

5. DA APRESENTAÇÃO DA PROPOSTA E DOS DOCUMENTOS DE HABILITAÇÃO

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

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

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

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

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

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

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

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

6. DO PREENCHIMENTO DA PROPOSTA

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

6.1.1. valor **unitário e total** do item;

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

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

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

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

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

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

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

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

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

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

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

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

6.9. O prazo de validade da proposta não será inferior a 180 (cento e oitenta) dias**,** a contar da data de sua apresentação.

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

7.26.1. prestados por empresas brasileiras;

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

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

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

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

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

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

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

7.28.4. O caso de o licitante ofertante do melhor lance não atender à convocação para o envio da proposta ajustada no prazo estabelecido, o pregoeiro convocará o próximo licitante detentor de proposta válida, obedecida a classificação na etapa de lances e garantidos os mesmos prazos concedidos ao licitante anteriormente convocado, inclusive em relação às prorrogações.

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

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

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

8. **DA ACEITABILIDADE DA PROPOSTA VENCEDORA.**

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

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

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

8.2.2. contenha vício insanável ou ilegalidade;

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

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

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

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

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

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

8.5. 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.

8.5.1. 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.

8.6. 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.

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

8.7. 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.

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

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

8.10. 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.

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

9. DA HABILITAÇÃO

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

a) SICAF;

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

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

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

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

9.1.2. A consulta aos cadastros será realizada em nome da empresa licitante e, no caso do Cadastro Nacional de Condenações Cíveis por Atos de Improbidade Administrativa, também de seu sócio majoritário, por força do artigo 12 da Lei n° 8.429, de 1992, que prevê, dentre as sanções impostas ao responsável pela prática de ato de improbidade administrativa, a proibição de contratar com o Poder Público, inclusive por intermédio de pessoa jurídica da qual seja sócio majoritário.

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

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

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

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

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

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

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

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

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

9.3. Havendo a necessidade de envio de documentos de habilitação complementares, necessários à confirmação daqueles exigidos neste Edital e já apresentados, o licitante será convocado a encaminhá-los, em formato digital, via sistema, no prazo de 2 (duas) horas, sob pena de inabilitação.

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

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

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

9.6. Se o licitante for a matriz, todos os documentos deverão estar em nome da matriz, e se o licitante for a filial, todos os documentos deverão estar em nome da filial, exceto aqueles documentos que, pela própria natureza, comprovadamente, forem emitidos somente em nome da matriz.

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

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

9.8. **Habilitação jurídica:**

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

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

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

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

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

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

9.9. **Regularidade fiscal e trabalhista:**

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

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

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

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

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

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

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

9.10. **Qualificação Econômico-Financeira:**

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

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

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

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

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

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

9.10.4. As empresas, cadastradas ou não no SICAF, que apresentarem resultado inferior ou igual a 1(um) em qualquer dos índices de Liquidez Geral (LG), Solvência Geral (SG) e Liquidez

Corrente (LC), deverão comprovar patrimônio líquido de 10 % (dez por cento) do valor estimado da contratação ou do item pertinente.

9.11. **Qualificação Técnica:**

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

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

9.11.1.1.1. Grupo 1 - Experiência na prestação de serviços de administração de solução(ões) de automação (Orquestração, Automação e Resposta de Segurança (Security Orchestration, Automation, and Response - SOAR), de análise e correlacionamento (Monitoramento de estação de trabalho (Endpoint Detection and Response - EDR), Análise de Tráfego de Rede (Network Traffic Analysis - NTA), Análise de Comportamento de Usuário (User Entity and Behavior Analytics - UEBA), Análise de Inteligência de Ameaças Cibernéticas (Cyber Threat Intelligence - CTI) e de coleta (Informações de segurança e gestão de eventos (Security Informati on and Event Management - SIEM) para um total de, no mínimo de;

9.11.1.1.2. 10 (dez) sistemas e serviços de TI;

9.11.1.1.3. 200 (duzentos) maquinas virtuais;

9.11.1.1.4. 100 (cem) ativos de infraestrutura TI;

9.11.1.1.5. 1200 (mil e duzentos) estações de trabalho, incluindo desktops e notebooks, e;

9.11.1.1.6. 1200 (mil e duzentos) usuários de rede.

9.11.1.1.7. Grupo 2 - Experiência na prestação de **serviços de testes de invasão** em empresa ou órgão da Administração Pública para exploração de vulnerabilidades de segurança da informação, que contenham pelo menos 1.000 usuários de sistema cadastrados e ativos, em conformidade com boas práticas internacionais;

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

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

9.11.4. Será permitido o somatório de atestado(s) de capacidade técnica para efeito de comprovação de experiência na prestação dos serviços de características técnicas semelhantes ao objeto desta contratação, não se exigindo que todos tenham sido prestados a uma única pessoa jurídica de direito público ou privado.

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

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

9.11.7. As empresas, cadastradas ou não no SICAF, deverão apresentar atestado de vistoria assinado pelo servidor responsável, nos termos do item 4.16.1 do Termo de Referência.

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

9.12. O licitante enquadrado como microempreendedor individual que pretenda auferir os benefícios do tratamento diferenciado previstos na Lei Complementar n. 123, de 2006, estará dispensado (a) da prova de inscrição nos cadastros de contribuintes estadual e municipal e (b) da apresentação do balanço patrimonial e das demonstrações contábeis do último exercício.

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

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

9.14. Caso a proposta mais vantajosa seja ofertada por microempresa, empresa de pequeno porte ou sociedade cooperativa equiparada, e uma vez constatada a existência de alguma restrição no que tange à regularidade fiscal e trabalhista, a mesma será convocada para, no prazo de 5 (cinco) dias úteis, após a declaração do vencedor, comprovar a regularização.

9.14.1. O prazo poderá ser prorrogado por igual período, a critério da administração pública, quando requerida pelo licitante, mediante apresentação de justificativa.

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

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

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

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

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

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

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

10. DO ENCAMINHAMENTO DA PROPOSTA VENCEDORA

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

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

rubricadas pelo licitante ou seu representante legal.

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

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

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

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

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

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

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

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

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

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

11. DOS RECURSOS

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

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

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

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

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

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

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

12. DA REABERTURA DA SESSÃO PÚBLICA

12.1. A sessão pública poderá ser reaberta:

12.1.1. Nas hipóteses de provimento de recurso que leve à anulação de atos anteriores à realização da sessão pública precedente ou em que seja anulada a própria sessão pública, situação

em que serão repetidos os atos anulados e os que dele dependam.

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

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

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

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

13. DA ADJUDICAÇÃO E HOMOLOGAÇÃO

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

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

14. DA GARANTIA DE EXECUÇÃO

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

15. DO TERMO DE CONTRATO

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

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

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

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

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

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

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

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

15.4. O prazo de vigência da contratação é de 24 (vinte e quatro) meses prorrogável conforme previsão no termo de referência.

15.5. Previamente à contratação a Administração realizará consulta ao SICAF para identificar possível suspensão temporária de participação em licitação, no âmbito do órgão ou entidade, proibição de contratar com o Poder Público, bem como ocorrências impeditivas indiretas, observado o disposto no

art. 29, da Instrução Normativa nº 3, de 26 de abril de 2018, e nos termos do art. 6º, III, da Lei nº 10.522, de 19 de julho de 2002, consulta prévia ao CADIN.

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

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

15.6. Na assinatura do contrato 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.

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

16. DO REAJUSTAMENTO EM SENTIDO GERAL

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

17. DO RECEBIMENTO DO OBJETO E DA FISCALIZAÇÃO

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

18. DAS OBRIGAÇÕES DA CONTRATANTE E DA CONTRATADA

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

19. DO PAGAMENTO

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

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

20. DAS SANÇÕES ADMINISTRATIVAS.

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

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

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

20.1.3. apresentar documentação falsa;

20.1.4. deixar de entregar os documentos exigidos no certame;

20.1.5. ensejar o retardamento da execução do objeto;

20.1.6. não mantiver a proposta;

20.1.7. cometer fraude fiscal;

20.1.8. comportar-se de modo inidôneo;

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

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

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

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

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

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

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

20.4.4.1. 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.

20.4.5. 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;

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

20.6. 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.

20.7. 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.

20.8. 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.

20.9. 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.

20.10. 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.

20.11. 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.

20.12. As penalidades serão obrigatoriamente registradas no SICAF.

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

21. DA IMPUGNAÇÃO AO EDITAL E DO PEDIDO DE ESCLARECIMENTO

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

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

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

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

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

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

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

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

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

22. DAS DISPOSIÇÕES GERAIS

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

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

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

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

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

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

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

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

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

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

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

22.12. A empresa contratada deverá se comprometer a implantar o Programa de Integridade ou adequar seu Programa de Integridade já existente ao previsto na Portaria N° 513, de 15 de Setembro de 2020.

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

22.13.1. ANEXO I - Termo de Referência (SEI nº 16676496)

22.13.1.1. ANEXO I - A - PROPOSTA DE PREÇOS (SEI nº 15854396)

22.13.1.2. ANEXO I - B - MODELO DE ORDEM DE SERVIÇO – O.S. (SEI nº 15854396)

22.13.1.3. ANEXO I - C - RELATÓRIO DE CHAMADO TÉCNICO – RCTA (SEI nº 15854396)

22.13.1.4. ANEXO I - D - MODELO DE DECLARAÇÃO DE VISTORIA (SEI nº 15854396)

22.13.1.5. ANEXO I - E - TERMO DE CIÊNCIA (SEI nº 15854396)

22.13.1.6. ANEXO I - F - TERMO DE COMPROMISSO (SEI nº 15854396)

22.13.1.7. ANEXO I - G - MODELO DE DECLARAÇÃO DE RENÚNCIA À VISTORIA (SEI nº 15854396)

22.13.1.8. ANEXO I - H - MODELO DE PLANO DE INSERÇÃO (SEI nº 15854396)

22.13.1.9. ANEXO I - I - MODELO DE PLANO DE FISCALIZAÇÃO (SEI nº 15854396)

22.13.1.10. ANEXO I - J - MODELO DE DECLARAÇÃO DE SUSTENTABILIDADE AMBIENTAL (SEI nº 15854396)

22.13.1.11. ANEXO I - K - PLANILHA DE AVALIAÇÃO DE TREINAMENTO (SEI nº 15854396)

22.13.1.12. ANEXO I - L - TERMO DE RECEBIMENTO PROVISÓRIO (SEI nº 15854396)

22.13.1.13. ANEXO I - M - TERMO DE RECEBIMENTO DEFINITIVO (SEI nº 15854396)

22.13.1.14. ANEXO I - N - ESTUDO TÉCNICO PRELIMINAR (SEI nº 15854445)

22.13.1.15. ANEXO I - O - PORTARIA 513 MJSP (SEI nº 15854486)

22.13.2. ANEXO II – MINUTA DE TERMO DE CONTRATO (SEI nº 16765671)

22.13.3. ANEXO III - MODELO DE DECLARAÇÃO DE INEXISTÊNCIA DE VÍNCULO FAMILIAR (SEI nº 16486913)

ARIEL CRAVEIRO NOLETO
Pregoeiro

Documento assinado eletronicamente por **Ariel Craveiro Noleto**, **Pregoeiro(a)**, em 30/12/2021, às 09:53, 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 **16832818** e o código CRC **F2C59A22**
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.

16676496 08006.000003/2021-38

MINISTÉRIO DA JUSTIÇA E SEGURANÇA PÚBLICA
Secretaria-Executiva
Coordenação de Riscos e Segurança de TIC

MINUTA DE TERMO DE REFERÊNCIA
PROCESSO Nº 08006.000003/2021-38

1. **OBJETO DA CONTRATAÇÃO**

1.1. Contratação de empresa especializada, para o fornecimento de **Serviço de Centro de Operações de Segurança (Security Operations Center - SOC) com funcionamento e suporte 24h por dia e 7 dias por semana, Serviço de tratamento e resposta aos incidentes cibernéticos - CSIRT - Blue Team e Serviço de teste de invasão - Red Team** e garantia dos serviços pelo período de 24(vinte e quatro) meses, renováveis até o limite de 60 (sessenta) meses, para o atendimento das necessidades da Diretoria de Tecnologia da Informação e Comunicação - DTIC do Ministério da Justiça e Segurança Pública - MJSP, de acordo com as especificações técnicas contidas neste Termo de Referência – TR e seus anexos.

2. **DESCRIÇÃO DA SOLUÇÃO DE TIC**

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

2.1.1. A tabela 1 apresenta a descrição dos itens a serem contratados (bens e serviços que compõem a solução), detalhados neste Termo de Referência.

Tabela 1 - Bens e serviços que compõem a solução.

Grupo	Item	Código SIASG CATSER	Descrição do Bem ou Serviço	Quantidade	Métrica ou Unidade	Regime de operação	Forma
1	1	26000	Serviço de Security Operations Center - SOC	24	Unidade (Mensal)	24x7	contínuo
	2	26000	Serviço de Tratamento e Resposta aos Incidentes Cibernéticos - CSIRT - Blue Team	24	Unidade (Mensal)	24x7	contínuo
2	3	26000	Serviço de Teste de Invasão - Red Team: Sistemas Web	217	Unidade (Alvo)	N/A	sob demanda
	4	26000	Serviço de Teste de Invasão - Red Team: Infraestrutura	610	Unidade (Alvo)	N/A	sob demanda

2.2. **Da classificação dos serviços**

2.2.1. 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.

2.2.2. 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.

2.2.3. 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.

2.2.4. Os serviços a serem contratados enquadram-se nos pressupostos do inciso XXIII, Art. 1º, 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.

2.2.5. 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 PARA A CONTRATAÇÃO**

3.1. ***Contextualização e Justificativa da Contratação***

3.1.1. A Informação se tornou uma ferramenta de fácil acesso e essencial para o desenvolvimento pessoal e coletivo. Porém, essa informação deixou de ser unicamente um recurso de desenvolvimento passando a ser o item mais valioso em uma organização, sendo considerado muitas vezes como patrimônio do órgão no qual ela foi gerada. Diante dessa valorização da informação, ela passou atrair a atenção de pessoas ou entidades na busca de auferir lucro, se posicionar melhor no mercado, obter vantagens ou mesmo destruir imagens e reputações. Na sociedade atual, não basta apenas armazenar a informação para futura recuperação, uma vez que estão sob constante risco e necessitam ser adequadamente protegidas. É nesse contexto que a segurança da informação se tornou um elemento essencial para a manutenção da idoneidade das instituições e de sua manutenção no mercado.

3.1.2. A Segurança da Informação, por sua vez, se relaciona com a proteção de um conjunto de informações, estas entendidas como qualquer conhecimento armazenado ou codificado em um meio de armazenamento ou de transporte, com a finalidade de preservar o seu valor, seja para um indivíduo ou organização, possuindo como atributos básicos a confidencialidade, integridade e a disponibilidade. Ou seja, a segurança da informação busca, de forma resumida, garantir seus atributos básicos nos ativos das organizações sejam eles físicos, lógicos ou humanos, que possuam valor, sustente processos do negócio ou até mesmo possam causar dano caso sejam comprometidos.

3.1.3. Segundo a norma ABNT ISO/IEC 27001:2006 a confidencialidade é a "propriedade de que a informação não esteja disponível ou revelada a indivíduos, entidades ou processos não autorizados". Integridade, por sua vez, é a "propriedade de salvaguarda da exatidão e completeza de ativos". Já a disponibilidade é a "propriedade de estar acessível e utilizável sob demanda por uma entidade autorizada". Existem outro atributos que derivam dessa tríade, sendo a CID - Confidencialidade, Integridade e Disponibilidade as fontes dos demais.

3.1.4. Diante dessa sociedade da informação, a segurança da informação tem se tornado essencial para a proteção de uma organização, necessitando de uma grande estrutura de operação de segurança dentro dos órgãos e sendo inviável contar somente com o corpo técnico interno das entidades, passando a ser executados por Centros de Operações de Segurança ou, na denominação mais conhecida e difundida em inglês, Security Operations Center - SOC.

3.1.5. Um Security Operations Center - SOC, sigla que será utilizada a partir desse momento, é um ente centralizado que possui funções de monitoramento contínuo de ameaças, análise dessas ameaças, bem como, para prevenção e mitigação de incidentes de cibersegurança. Esse entendimento pode ser extraído da brochura do Kaspersky for Security Operations Center, conforme a seguir:

"As businesses learn to better protect themselves, criminals are simultaneously devising increasingly sophisticated techniques to penetrate their security barriers. Attracted by the unprecedented financial rewards that cyberattacks can deliver, growing numbers of threat actors are actively seeking and targeting undiscovered security flaws. In this environment, many organizations are establishing Security Operations Centers (SOCs) to combat security issues as they arise, providing a swift response and a decisive resolution." (https://media.kaspersky.com/en/business-security/enterprise/brochure-soc-powered-by-kl-eng.pdf)

"À medida que as empresas aprendem a se proteger melhor, os criminosos estão simultaneamente planejando cada vez mais técnicas sofisticadas para penetrar em suas barreiras de segurança. Atraídos pelas recompensas financeiras sem precedentes que os ciberataques podem oferecer, um número crescente de atores de ameaças está ativamente buscando e direcionando falhas de segurança não descobertas. Nesse ambiente, muitas organizações estão estabelecendo Centrais de Operações de Segurança SOCs para combater os problemas de segurança à medida que surgem, fornecendo uma resposta rápida e uma resolução decisiva." (tradução livre)

3.1.6. É por meio dos SOCs que as organizações buscam, diante da velocidade desenfreada de evolução das técnicas de invasão ou obtenção da informação, proteger suas informações, ativos, recursos ou imagem. Em teoria os SOCs seriam a fronteira final entre a informação e o seu vazamento, alteração ou destruição.

3.1.7. Um SOC funciona de forma contínua, atuando 24 horas por dia e 7 dias por semana, com a responsabilidade de garantir a tríade CID de segurança da informação, sendo composto por profissionais com conhecimentos específicos e de difícil obtenção seja pelo nível de dinamicidade que a área de segurança possui no que diz respeito a atualizações ou elevado custo para obtenção do conhecimento por meio de cursos e certificação. Diferentemente de uma área como redes de computadores nos quais um modelo ou protocolos existem por anos sem modificação, os vetores de ataques atualizam-se a cada novo *patch* implantado, a cada ativo inserido, a cada profissional contratado em qualquer área, ou seja, a informação sempre está em risco e sem uma estrutura de monitoramento voltada somente para área da segurança da informação, como um SOC, esse risco aumenta consideravelmente.

3.1.8. Levando-se em consideração o modelo de arquitetura de segurança adaptativa proposto pelo Gartner, uma organização somente obterá sucesso na luta contra os crimes cibernéticos se seu SOC for capaz de predizer, prever, detectar e responder efetivamente as ameaças, conforme podemos visualizar na figura 1:

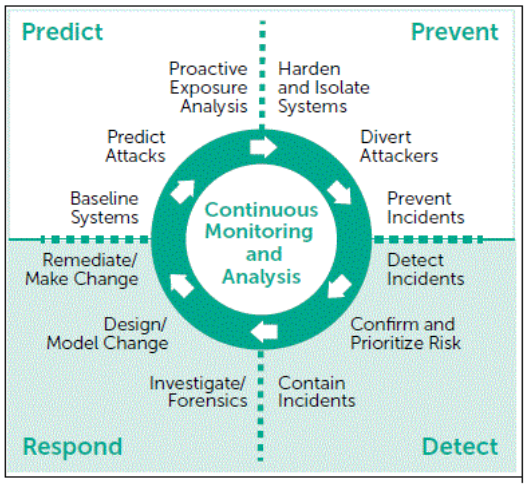

Figura 1 - Gartner, Designing an Adaptive Security Architecture for Protection From Advanced Attacks, February 2014. (retirado da brochura do Kaspersky for Security Operations Center)

3.1.9. Percebe-se mais uma vez que sem uma estrutura dedicada à área de segurança da informação é improvável que um organização consiga garantir esses quatro eixos: predição, prevenção, detecção e resposta efetiva. É possível que uma organização possa até responder, mas, muitas vezes, não no momento adequado.

3.1.10. Outras estruturas ou modelos de segurança são utilizados visando complementar o trabalho realizado por um SOC como equipes de Blue Team e Red Team, bem como o modelo de Purple Team. De acordo com a SANS, uma autoridade mundial na área de segurança da informação, temos as seguintes definições:

- Blue Team:

"[...] focus is to defend the organization from digital/cyber attacks. In truth, while everything that improves the defensive security posture could be construed as Blue Team, there is an overt emphasis on discovering and defending against attacks". (https://wiki.sans.blue/#!index.md)

"[...] focado em defender a organização de digital/cyber ataques. Na verdade, enquanto tudo que promova a postura defensiva de segurança possa ser entendida como Blue Team, há uma ênfase na descoberta e defesa contra esses ataques. " (Tradução Livre)

- Red Team:

"[...] would be those playing the role of the adversary. [...] So Red Team acts as Offense and Blue Team as Defense." (https://wiki.sans.blue/#!index.md)

"[...] seriam aqueles que atuam o papel de adversários. [...] Então o Red Team atua como ofensiva e Blue Team como defensiva." (Tradução Livre)

- Purple Team:

"[...] They typically report to a as a "third" team; think of it as a concept aimed at bringing the red and blue teams together to create purple team exercises. Red teams and blue teams should be encouraged to work as a joint team, to share insights beyond just reporting, to create a strong feedback loop, and to look for detection and prevention controls that can realistically be implemented for immediate improvement. " (https://www.sans.org/purple-team?msc=ptcourse-faq-lp)

"[...] Eles se denominam como o 'terceiro' time; pense nisso como um conceito que visa reunir as equipes vermelhas e azuis para criar exercícios de Purple Team. Equipes vermelhas e azuis devem ser incentivadas a trabalhar como uma equipe conjunta, para compartilhar ideias além somente gerar relatórios, a criar um forte ciclo de feedback, e a procurar controles de detecção e prevenção que possam ser implementados realisticamente para melhoria imediata."(Tradução Livre)

3.1.11. Considerando as definições da SANS para Blue Team, Red Team e Purple Team, podemos afirmar, simplificadamente que o Blue Team é o elo de defesa e sua operação, o Red Team seria o ente de ataque o qual checa as defesas implementadas pelo Blue Team e o Purple Team seria o esforço coordenado envolvendo os outros dois grupos visando garantir a real implementação dos bloqueios a partir das vulnerabilidades apontadas no ataque, assim como, promover a melhoria contínua das equipes.

3.1.12. Sendo esses conceitos mais abrangentes do que verdadeiramente uma equipe propriamente dita, pode-se afirmar que o Blue Team está inserido em todos os eixos do modelo de arquitetura do Gartner exibido na Figura 1, assim como, nas diversas responsabilidades do SOC. Porém, o foco das equipes é mais preventivo e proativo, enquanto o SOC encarrega-se mais efetivamente da operação de monitoração e resposta, ou seja, reativo.

3.1.13. Em contrapartida um *Network Operations Center* - NOC, Centro de Operações de Rede em tradução direta, é uma estrutura que funciona também de forma ininterrupta como um SOC, porém com foco somente na disponibilidade. Um SOC e um NOC não se confundem em suas atribuições, apesar de algumas vezes terem que operar em paralelo. Enquanto um SOC é responsável pela garantia da tríade de segurança: confidencialidade, integridade e disponibilidade, um NOC concentra-se apenas na disponibilidade sem considerar os aspectos de segurança, não sendo sua responsabilidade em teoria. Um exemplo pode esclarecer melhor como num cenário onde se deseja disponibilizar um sistema na Internet. Nesse cenário um NOC e um SOC concentrariam seus focos em responder perguntas conforme a tabela 2:

Tabela 2 - Exemplo de perguntas NOC vs. SOC

Atributo a garantir	NOC	SOC	Atributo a garantir
Disponibilidade da Infraestrutura	Qual a demanda de usuários esse sistema irá possuir?	O sistema será autenticado? Quais usuários podem acessá-lo? Quais perfis existirão? Há algum acesso fora do horário normal?	Disponibilidade de Segurança, Integridade e Confidencialidade
Disponibilidade da Infraestrutura	É um sistema estático ou dinâmico?	Que tipo de tecnologia está sendo utilizada? Existem áreas de acesso restrito? Existem vulnerabilidades conhecidas nessa tecnologia? Está atualizado? É utilizado criptografia ou alguma forma de tornar anônimo?	Disponibilidade de Segurança, Integridade e Confidencialidade
Disponibilidade da Infraestrutura	Qual tipo de banco de dados deverá ser usado?	O banco está hospedado localmente ou na nuvem? Qual versão do banco de dados e quais vulnerabilidades existem? O banco é acessado diretamente ou somente por meio da aplicação? Quem pode acessá-lo diretamente? Quais usuários podem ter acesso ao banco? A partir de quais máquinas ou redes?	Disponibilidade de Segurança, Integridade e Confidencialidade
Disponibilidade da Infraestrutura	Quanto de *Downtime* o sistema pode dispor?	Qual o fluxo de informação para manutenções programadas? Quando foi um erro da aplicação ou um ataque? Quais outros sistemas podem ser comprometidos a partir do sistema atacado?	Disponibilidade de Segurança, Integridade e Confidencialidade
Disponibilidade da Infraestrutura	Qual tipo de hardware vou alocar para hospedar o sistema?	O hardware é virtual ou físico? Quais barreiras existem entre a internet e esse hardware? Que tipo de firewall o protege? Qual dano potencial pode acontecer no comprometimento desse hardware? Quais redes são alcançadas a partir da rede na qual esse hardware está instalado?	Disponibilidade de Segurança, Integridade e Confidencialidade
Disponibilidade da Infraestrutura	Quanto de memória, CPU e disco?	Houve algum aumento anormal na utilização? Por qual motivo? Quais processos estão comprometendo a performance os quais não são comuns ao sistema? Os arquivos possuem hash para verificação de modificação? Quais usuários tem acesso direto ao hardware?	Disponibilidade de Segurança, Integridade e Confidencialidade
Disponibilidade da Infraestrutura	Haverá redundância nesse servidor?	A redundância foi analisada quanto a segurança? Houve algum teste sobre o funcionamento da redundância? Essa redundância fica ativa ou somente é ativada quando da indisponibilidade da principal?	Disponibilidade de Segurança, Integridade e Confidencialidade

3.1.14. Esses seriam alguns questionamentos os quais um SOC e um NOC seriam responsáveis por responder. Percebe-se claramente que o NOC concentra-se na disponibilidade do sistema em termos utilização usual dos usuários enquanto o SOC, concentra-se na disponibilidade em termos de segurança, assim como, na integridade e na confidencialidade.

3.1.15. É a partir desse cenário no qual se insere o Ministério da Justiça e Segurança Pública - MJSP. O Ministério da Justiça e Segurança Pública possui um ambiente composto por uma diversidade de tecnologias, pessoas que as acessam, sistemas, locais e informações que juntas elevam a complexidade da gestão de segurança da informação.

3.1.16. No que diz respeito a diversidade de Tecnologias a tabela 3 apresenta um panorama dos ativos que o MJSP tem sob sua gestão.

Tabela 3 - Panorama de Tecnologias utilizadas no Ministério da Justiça e Segurança Pública.

Itens	Descrição	Totais
1.	Equipamentos e tecnologias utilizadas no MJSP	728
2.	Total de estações de trabalho (14868691)	3.125
3.	Total de usuários cadastrados no AD	5.460
4.	Sistemas	217
6.	Tecnologias de nuvem contratada Oracle e Microsoft	2
7.	Total de chamados para janeiro e fevereiro 2021 - N3 - Segurança(14656980)	219

**Fonte: Planilha Sistemas e Recursos de TI 2021 (Doc. Sei nº 14628507)

3.1.17. Para à obtenção de informações e condições necessárias à correta elaboração da proposta e execução dos serviços. A licitante poderá realizar vistoria técnica conforme item 4.16.1 deste termo e tomar conhecimento dos principais softwares, aplicativos, sistemas e ferramentas auxiliares em utilização no Ministério.

3.1.18. No que diz respeito ao público interno do Ministério da Justiça e Segurança Pública, tem-se atualmente cerca de 5460 usuários, considerando os de sistema e usuários reais, utilizando recursos de TIC.

3.1.19. Associado a esse ambiente misto há uma escassez de pessoal dedicado a área de segurança da informação. Isso sujeita o Ministério da Justiça e Segurança Pública a riscos que podem comprometer as informações, pessoas, sistemas e até mesmo, os locais onde o ministério atua uma vez que a infraestrutura tecnológica do Departamento Penitenciário Nacional - DEPEN, por exemplo, está sob a gestão direta do Ministério da Justiça e Segurança Pública. Maiores detalhes sobre a infraestrutura do Ministério podem estão agrupadas no Relatório de informações sobre infraestrutura, documento Sei nº (14628328).

3.1.20. O Ministério da Justiça, diante do cenário estratégico que ocupa junto ao Governo Federal apresenta um significativo volume de ataques virtuais sofridos em suas redes corporativas. Isso é associado, conforme podemos encontrar na Lei nº 13.844/2019, às competências as quais o Ministério da Justiça e Segurança Pública possui como, citando apenas algumas:

a) política judiciária;

b) políticas sobre drogas;

c) defesa da ordem econômica nacional e dos direitos do consumidor;

d) nacionalidade, imigração e estrangeiros;

e) ouvidoria-geral do consumidor e das polícias federais;

f) prevenção e combate à corrupção, à lavagem de dinheiro e ao financiamento do terrorismo e cooperação jurídica internacional;

g) coordenação de ações para combate a infrações penais em geral, com ênfase em corrupção, crime organizado e crimes violentos;

h) política nacional de arquivos;

i) coordenação e promoção da integração da segurança pública no território nacional, em cooperação com os entes federativos;

j) coordenação do Sistema Único de Segurança Pública;

k) planejamento, coordenação e administração da política penitenciária nacional;

l) promoção da integração e da cooperação entre os órgãos federais, estaduais, distritais e municipais e articulação com os órgãos e as entidades de coordenação e supervisão das atividades de segurança pública;

m) assistência ao Presidente da República em matérias não afetas a outro Ministério;

n) política de organização e manutenção da polícia civil, da polícia militar e do corpo de bombeiros militar do Distrito Federal.

3.1.21. Percebe-se pelo exposto na Lei nº 13.844/2019 que uma significativa quantidade de informações sensíveis trafegam na rede corporativa do Ministério da Justiça e Segurança Pública e, dessa forma, é muito importante possuir uma equipe dedicada ao acompanhamento ininterrupto da "saúde" de sua infraestrutura no que diz respeito à Segurança da Informação e Comunicação submete o Ministério e o Governo Brasileiro, mitigando os riscos de perda de informações e danos à imagem institucional."

3.1.22. Ainda no que diz respeito a sensibilidade dos dados trafegados temos a proximidade da vigência plena da Lei Geral de Proteção de Dados, que determina a utilização de mecanismos para proteção dos dados pessoais tratados no Ministério da Justiça e Segurança Pública.

3.1.23. De acordo com a figura 3, temos os tipos de violações de dados por método de ataque e segmento da indústria:

# OF DATA BREACHES PER METHOD PER INDUSTRY						
Method	Banking	Business	Education	Government	Medical	Totals
Hacking/Intrusion (includes Phishing, Ransomware/Malware and Skimming)	31	291	29	35	191	577
Unauthorized Access	45	223	59	15	196	538
Employee Error/Negligence/ Improper Disposal/Lost	12	42	15	19	73	161
Accidental Web/Internet Exposure	12	44	7	8	17	88
Physical Theft	2	17	0	2	32	53
Insider Theft	6	12	2	3	10	33
Data on the Move	0	15	1	1	6	23

Figura 3 - End of Year Data Breach Report 2019 - Identity Theft Resource Center

3.1.24. No segmento governo, o método de ataque mais utilizado foi Hacking/Intrusion com cerca de 42,2%, assim como, em todos os outros segmentos. Não se deve considerar o número de violações de dados de forma absoluta, mas se deve levar em consideração a sensibilidade do dado violado, não somente, o prejuízo financeiro imediato associado.

3.1.25. Diante do que foi exposto, é imprescindível para que o Ministério da Justiça e Segurança Pública possa prover a segurança dos dados e ativos presentes em todo seu parque tecnológico que essa contração seja realizada com a maior brevidade possível.

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

3.2.1. A presente contratação está alinhada ao PDTI 2021-2023, conforme consta na página 29 do Plano Diretor de Tecnologia da Informação, documento SEI (14424141) e Declaração de Adequação ao planejamento estratégico do órgão (13312423).

3.3. ***Estimativa da demanda***

3.3.1. Foram realizados estudos acerca do cenário atual da necessidade no âmbito do Ministério da Justiça e Segurança Pública, considerando os requisitos das suas unidades e os ativos atualmente instalados no parque computacional do órgão, conforme Estudo Técnico Preliminar, documento SEI

(14628351).Os itens e os respectivos quantitativos referem-se às necessidades do MJSP, apresentado na tabela 4.

Tabela 4 - Estimativa da demanda

Grupo	Item	Código SIASG CATSER	Descrição do Bem ou Serviço	Quantidade	Métrica ou Unidade	Regime de operação
1	1	26000	Serviço de Security Operations Center - SOC	24	Unidade (Mensal)	24x7
	2	26000	Serviço de Tratamento e Resposta aos Incidentes Cibernéticos - CSIRT - Blue Team	24	Unidade (Mensal)	24x7
2	3	26000	Serviço de Teste de Invasão - Red Team: Sistemas Web	217	Unidade (Alvo)	N/A
	4	26000	Serviço de Teste de Invasão - Red Team: Infraestrutura	610	Unidade (Alvo)	N/A

3.4. ***Parcelamento da Solução de TIC***

3.4.1. **Justificativa para o agrupamento para itens 1 e 2**

3.4.1.1. Um Security Operations Center - SOC, não é uma unidade isolada, mas uma estrutura responsável por lidar com as questões relacionadas a Segurança da Informação. Tipicamente um SOC possui as funções de Monitoramento e Gestão de Vulnerabilidades, Monitoramento Contínuo de Eventos de Segurança, Gestão da Resposta a Incidentes de Segurança, Gestão das Ameaças de Segurança, entre outras. Todas essas funções de monitoramento e gestão necessitam de ferramentas e pessoal para configuração, análise e aplicação de inteligência para o que foi detectado ou descoberto. Nesse sentido, caso a tarefa de configuração, análise e aplicação de inteligência seja dedicada ao SOC, é possível que a tarefa de monitorar e gerir fique comprometida uma vez que a quantidade de informação que deve ser monitorada não é pequena.

3.4.1.2. Noutro giro, um Blue Team pode ser definido, em linhas gerais, como tudo que promova uma postura defensiva de segurança. Considerando isso, atividades como a análise de vulnerabilidades detectadas, análise de eventos de segurança detectados, sugestões sobre a melhor resposta a incidentes de segurança ficam melhor alocadas a uma equipe dedicada a execução dessa inteligência. Exemplos de atividades típicas de uma equipe de Blue Team seriam análises de log, auditorias de segurança, análises de risco, desenvolvimento de cenários de risco, avaliação de vulnerabilidades em ativos, entre outros.

3.4.1.3. As ferramentas que automatizam um SOC necessitam de ajustes em seus algoritmos e modelos de inteligência e, essas atividades, ficam melhor alocadas em um equipe dedicada a essas tarefas. Dessa forma, um SOC e um Blue Team possuem correlação em suas atividades e devem funcionar em sinergia, porém, cada um com suas atividades específicas e complementares, sendo aquela dedicada ao monitoramento e gestão dos serviços relacionados à Segurança da Informação e esta a serviços de análise e inteligência de segurança da informação.

3.4.1.4. O monitoramento e gestão seria ineficiente sem a análise e inteligência e, por isso, uma comunicação rápida, eficaz e sem entraves administrativos ou burocráticos que prejudicariam o atendimento preciso e tempestivo é essencial. Afinal, o tempo de resposta aos incidentes de segurança da informação diante dos eventos registrados no monitoramento deve ser o mais breve possível.

3.4.1.5. Devido a essa necessidade de funcionamento preciso, tempestivo, de comunicação rápida e eficaz é que os itens um e dois foram agrupados em um mesmo grupo, sendo providos por uma mesma empresa. Não é mera coincidência também que o regime de execução para os itens um e dois foi definido como 24h por dia, 7 dias por semana durante todo o ano.

3.4.1.6. Esse agrupamento promoverá uma maior eficiência não só no âmbito da funcionalidade da solução, como também naquele relacionado à prevenção de contratações conflituosas e, por conseguinte, a resolução de conflitos entre fornecedores distintos. O modelo de contratação ora pretendido permite a preservação do funcionamento integrado dos itens, não comprometendo a funcionalidade da solução, tendo em vista que os serviços de monitoramento, gestão, instalação, configuração, treinamento e inteligência serão executados por um único fornecedor proporcionando a equipe de segurança do Ministério da Justiça concentrar-se na Gestão da Solução de Segurança total proporcionada pelo serviço, assim como, um visão global da solução. Assim, há uma redução do risco de perda, interrupção do funcionamento da solução e consequente indisponibilidade do serviço de TIC, por conta de uma possível divisão de responsabilidades entre diferentes fornecedores.

3.4.1.7. A adjudicação dos itens 1 e 2 desta contratação a empresas distintas, além de aumentar seu custo administrativo, abre margem para que as empresas deixem de prestar o serviço contratado, alegando que a falha de um componente sob sua responsabilidade foi causada por falha de componente sob responsabilidade de outra CONTRATADA. De modo a impedir que esse cenário se torne realidade, comprometendo a disponibilidade de todos os serviços de TIC deste Ministério devido a uma falha em Segurança da Informação, é fundamental que os itens objeto desta contratação sejam adjudicados a um único licitante.

3.4.1.8. Assim, entende-se que é essencial para a pretensa contratação, e necessário para o alcance dos objetivos técnicos e estratégicos para os quais este projeto foi desenvolvido, que os itens um e dois ora propostos sejam adquiridos/contratados de forma agrupada.

3.4.1.9. Na situação em apreço, é imperativo destacar o que dispõe o Princípio da Padronização, insculpido no inciso I do art. 15 da Lei nº 8.666/1993, pelo qual se estabelece que a Administração, sempre que possível, tem o objetivo de compatibilizar especificações técnicas e de desempenho, observadas, quando for o caso, as condições de manutenção, assistência técnica e garantia, segundo transcrição a seguir, *in verbis*:

> "Lei nº 8.666/1993
>
> Art. 15. As compras, sempre que possível, deverão:
>
> I - atender ao princípio da padronização, que imponha compatibilidade de especificações técnicas e de desempenho, observadas, quando for o caso, as condições de manutenção, assistência técnica e garantia oferecidas;
>
> (...);
>
> III - submeter-se às condições de aquisição e pagamento semelhantes às do setor privado;"

3.4.1.10. Tal princípio, disposto no art. 15, Inciso I, da Lei 8666/1993, visa a propiciar à Administração uma consecução mais econômica e vantajosa de seus fins; e serve, pois, como instrumento de racionalização da atividade administrativa, por meio da redução de custos financeiros, tecnológicos, operacionais, gerenciais, técnico-administrativos e da otimização da aplicação de recursos. Isto é, fatores que se coadunam e se verificam na contratação ora pretendida. Significa, portanto, que, nesse caso, a padronização elimina variações tanto no tocante à seleção de softwares e componentes no momento da contratação, como também na sua utilização, conservação, segurança e manutenção.

3.4.1.11. Desagrupar os itens 1 e 2 (Serviço de Security Operations Center - SOC e Serviço de Tratamento e Resposta aos Incidentes Cibernéticos - CSIRT - Blue Team), nessa situação, ocasionará prejuízos técnicos e operacionais, uma vez que se realizados por vários fornecedores, exigiriam um tempo excessivo em dirimir divergências entre possíveis incompatibilidades ou entendimentos e, causariam um potencial risco de operacionalização e funcionamento, pela adoção de procedimentos variados, divergentes ou incompatíveis.

3.4.1.12. Conforme Acórdão nº 861/2013 - TCU - Plenário -, é lícito os agrupamentos em lotes de itens a serem adquiridos por meio de pregão, desde que possuam mesma natureza e que guardem relação entre si.

3.4.1.13. Segundo o Acórdão nº 5.260/2011 – TCU – 1ª câmara, de 06/07/2011, "Inexiste ilegalidade na realização de pregão com previsão de adjudicação por lotes, e não por itens, desde que os lotes sejam integrados por itens de uma mesma natureza e que guardem correlação entre si". O lote

proposto nesse documento agrupa solução e serviços de uma mesma natureza, que guardam correlação entre si, seja por similaridade técnica ou de tecnologia, bem como de aplicabilidade em busca de uma única solução, sem causar qualquer prejuízo à competitividade.

3.4.1.14. Em suma, a opção pelo fornecimento e consequente adjudicação por grupo para os itens 1 e 2 leva em conta a modalidade de contratação pretendida e os benefícios associados. O agrupamento de vários itens num mesmo lote ou grupo não compromete a competitividade do certame, uma vez que várias empresas, que atuam no mercado, apresentam condições para cotar todos os itens.

3.4.2. **Justificativa para divisão em grupos**

3.4.2.1. O serviço de Red Team tem como objetivo principal identificar, mapear e documentar possíveis vulnerabilidades nos sistemas, processos e ativos de infraestrutura tecnológica. Esses testes envolvem, necessariamente, o uso de técnicas e ferramentas específicas para tentar obter acesso não autorizado e privilegiado aos ativos e informações, bem como a indicação de soluções para a correção das vulnerabilidades encontradas.

3.4.2.2. Como responsável pelos ataques a empresa deve valer-se de sua expertise para tentar atingir um objetivo, realizando sofisticados testes de penetração e buscando pontos de falha nos processos, pessoas e tecnologias que compõem as defesas atualmente em uso na empresa para o cumprimento da missão.

3.4.2.3. A empresa estaria agindo como uma ameaça externa, que buscaria localizar quaisquer vulnerabilidades possíveis de serem exploradas, objetivando, por exemplo, extrair dados da localidade predeterminada. O foco em realmente “quebrar” a segurança implantada deve dirigir a vontade do Red Team na busca por brechas de segurança, o que pode envolver as mais diversas táticas, desde a utilização de ataques spear phishing, ou até mesmo a simples tática da utilização de pendrives infectados, deixados nos arredores da empresa.

3.4.2.4. Já a equipe do Blue Team, como mencionada anteriormente, também avalia a segurança de rede e identifica possíveis vulnerabilidades. Entretanto, o que o diferencia do Red Team é o seu foco em detecção de ameaças e resposta de incidentes, ou seja, seu principal objetivo é aplicar estratégias de defesa e manter a segurança dos sistemas e aplicações.

3.4.2.5. Eles também são os responsáveis por fortalecer toda a infraestrutura de segurança digital, usando softwares como o IDS, que fornece uma análise contínua de atividades comuns e suspeitas. Assim, a principal função do Blue Team é detectar e prevenir controles de segurança.

3.4.2.6. Vale ressaltar que uma infraestrutura de segurança completa e eficaz, preparada para qualquer ataque, só é possível com os dois grupos trabalhando juntos — um time complementa o outro.

3.4.2.7. Idealmente estes times devem ser composto por profissionais de empresas diferentes, para que a equipe que venha a realizar os ataques, não tenha contribuído para a estratégia de defesa atualmente aplicada pela outra equipe, pois isto poderia gerar um conflito de interesses em relação aos testes, a partir da atitude de não querer buscar realmente, ou mesmo expor, as fraquezas disponíveis na infraestrutura da corporação, e que não tenham sido cobertas pelas defesas que ajudaram a implantar. Dificultando até possíveis futuras auditorias. **Nesse sentido, a empresa licitante vencedora do grupo 1 está automaticamente impedida de ser tornar vencedora do grupo 2 e a vencedora do grupo 2 não poderá ser a vencedora do grupo 1.**

3.4.2.8. Segregação de funções refere-se a práticas onde o conhecimento e/ou privilégios necessários para se completar um processo são quebrados e divididos entre múltiplos usuários de forma que apenas um seja capaz de executá-lo ou controla-lo sozinho. A principal razão de se aplicar a segregação de funções é prevenir a realização e ocultação de fraude e erro no curso normal das atividades, uma vez que havendo mais de uma pessoa ou empresa para realizar uma atividade se minimiza a oportunidade de transgressões e aumenta as chances de se detectá-la, assim como de se detectar erros não intencionais.

3.4.2.9. A ISO 27001 considera a segregação de funções um dos potenciais controles a serem aplicados para controlar a implementação e operação da segurança da informação dentro da organização. O controle da norma requer que atividades e áreas de reponsabilidade conflitantes sejam segregadas de forma a reduzir o risco de um acesso não autorizado a um ativo ou uma modificação ou mau uso não intencional.

3.4.2.10. Ademais, 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.

3.4.2.11. Neste sentido, a Súmula TCU nº 247 dispõe que é obrigatória a admissão da adjudicação por item e não por preço global, nos editais das licitações para a contratação de obras, serviços, compras e alienações, cujo objeto seja divisível, desde que não haja prejuízo para o conjunto ou complexo ou perda de economia de escala, tendo em vista o objetivo de propiciar a ampla participação de licitantes que, embora não dispondo de capacidade para a execução, fornecimento ou aquisição da totalidade do objeto, possam fazê-lo com relação a itens ou unidades autônomas, devendo as exigências de habilitação adequar-se a essa divisibilidade.

3.4.3. **Justificativa para o agrupamento para itens 3 e 4**

3.4.3.1. Conforme explicado no item **Justificativa para divisão em grupos**, o serviço de Red Team tem como objetivo principal identificar, mapear e documentar possíveis vulnerabilidades nos sistemas, processos e ativos de infraestrutura tecnológica. Nesse sentido, percebe-se que o Red Team pode executar vários tipos de testes de invasão e, inclusive, vários deles podem ser utilizados em um mesmo procedimento como:

3.4.3.1.1. Web: realiza testes de vulnerabilidades e exploração em ambientes e aplicações WEB;

3.4.3.1.2. Mobile: testa vulnerabilidades e exploração em aplicativos e sistemas operacionais para dispositivos moveis;

3.4.3.1.3. Rede: focado em explorar a infraestrutura de rede;

3.4.3.1.4. Wireless: nesse tipo de teste é examinada a rede sem fio utilizada no ambiente, focando em pontos de acessos, protocolos e credenciais administrativas;

3.4.3.1.5. Físico: os controles de acessos ao ambiente são testados, mapeando fraquezas aos recursos físicos da empresa;

3.4.3.1.6. Engenharia Social: o foco é testar os próprios colaboradores, utilizando técnicas psicológicas para tentar induzi-los a passar informações importantes;

3.4.3.1.7. Estresse (DDos): verifica a disponibilidade de uma aplicação suportar uma alta demanda de requisições;

3.4.3.1.8. Externo: realizado a partir da Internet;

3.4.3.1.9. Interno: normalmente alocado no cliente.

3.4.3.2. A Tabela 10, do Estudo Técnico Preliminar, Anexo I-N, demonstra que um alvo é um ativo, o qual pode ser um sistema, appliance de segurança, ativo de rede, dentre outros. Nesse contexto, considera-se que um sistema possui em média dez ativos. Dessa forma, nota-se similaridade e complementariedade entre os itens 3 e 4 do grupo 2, uma vez que, para efeitos desta contratação, ambos são considerados alvos. Sendo que o item 4 (Serviço de Teste de Invasão - Red Team: Infraestrutura) constitui um serviço a ser realizado em um único alvo, enquanto que o item 3 (Serviço de Teste de Invasão - Red Team: Sistemas Web) constitui um serviço que pode contemplar múltiplos alvos.

3.4.3.3. Assim, resta caracterizado que os serviços de teste de invasão em ativos de infraestrutura e em sistemas web são similarmente idênticos e diferenciam-se apenas pela complexidade e tempo necessários para em sua execução, razão pela qual foram separados em itens diferentes, o que possibilitará ao Ministério avaliar suas defesas cibernéticas a um custo compatível com o esforço para a respectiva execução.

3.4.3.4. Além disso, a equipe de planejamento avalia que o não agrupamento dos itens 3 e 4 levaria um parcelamento inadequado do objeto porque tais itens constituem-se, em essência, o mesmo objeto sendo requeridas empresas segmentadas na mesma especialização para a execução desses serviços. Desse

modo, o parcelamento poderia ocasionar uma licitação com poucos fornecedores interessados pelo item 4, com consequente aumento dos valores contratados em comparação à compra agrupada dos itens, considerando que o item 4 por ser um serviço de baixa complexidade tende a ter um valor menor para sua execução.

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

3.4.4.1. 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. Com vistas a subsidiar o entendimento a respeito da participação de consórcios em licitações públicas, transcrevemos, abaixo, comentário do Professor Marçal Justen Filho sobre o assunto:

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

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

3.4.4.3. Não obstante, o objeto a ser contratado é amplamente comercializado por diversas empresas no mercado. Tal permissibilidade poderia causar dano à administração por frustrar o próprio caráter competitivo da disputa pelo menor preço.

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

3.5.1. Com a contratação de um Security Operations Center - SOC - com suporte 24h por dia e 7 dias, Blue Team, Red Team irá possibilitar ao Ministério da Justiça e Segurança Pública perseguir os seguintes resultados:

3.5.1.1. Redução de riscos associados a perda de dados, comprometimento dos sistemas, imagem institucional do ministério e do governo brasileiro.

3.5.1.2. Maior assertividade nos investimentos em soluções de segurança da informação efetivamente necessárias.

3.5.1.3. Redução dos riscos associados aos ativos críticos.

3.5.1.4. Aumento da maturidade de segurança da informação.

3.5.1.5. Economia de tempo e redução da complexidade, identificando e saneando a segurança da informação antes da implantação dos sistemas.

3.5.1.6. Aumentar a segurança dos seus ativos eliminando os pontos cegos.

3.5.1.7. Desenvolvimento de relatórios e apurações especiais; e painéis gerenciais para apoio à tomada de decisão dos gestores, quanto ao risco da instituição.

3.5.1.8. Garantir a segurança da informação e comunicação no âmbito do Ministério da Justiça e o sigilo das informações dos cidadãos.

3.5.1.9. Implantar e fortalecer as equipes de tratamento de incidentes cibernéticos nas redes de computadores.

3.5.1.10. Implantar ações que promovam o envolvimento da alta administração do órgão em relação às diretrizes e ações de Segurança da Informação e Comunicação.

3.5.1.11. Definir e implantar mecanismos mais efetivos de responsabilização de colaboradores por eventos relacionados à Segurança da Informação e Comunicação.

3.5.1.12. Contribuir para o aumento da capacidade de resiliência dos ativos de informação e das infraestruturas críticas.

3.5.1.13. Instituir práticas de auditoria de Segurança da Informação e Comunicações.

3.5.1.14. Atualizar a Política de Segurança da Informação e Comunicações.

3.5.1.15. Manter uma equipe ininterrupta de resposta rápida e efetiva a ataques e incidentes cibernético .

3.5.1.16. Implantar o estado da arte em termos de segurança da informação.

3.5.1.17. Multiplicar o efetivo na área de segurança da informação.

3.5.1.18. Elevar o conhecimento técnico e a capacidade de gestão do corpo técnico próprio do Ministério da Justiça.

3.5.1.19. Obter uma melhor compreensão da real situação em termos de segurança da informação do Ministério da Justiça de forma periódica por meio de um Red Team.

4. **ESPECIFICAÇÃO DOS REQUISITOS DA CONTRATAÇÃO**

4.1. ***Requisitos de Negócio***

4.1.1. Garantir a continuidade dos negócios do Ministério da Justiça e Segurança Pública e manter a capacidade de atendimento às áreas de negócio do Ministério, que dependem das soluções de tecnologia da informação.

4.1.2. Garantir o gerenciamento contínuo de controles de segurança da informação no ambiente do Ministério da Justiça e Segurança Pública.

4.1.3. Fornecer às unidades de negócio do Ministério da Justiça e Segurança Pública e à sociedade soluções tecnológicas que agreguem valor ao negócio e atendam às necessidades do cidadão no fornecimento de informações e serviços disponibilizados com qualidade e eficiência.

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

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

4.1.6. Aprimorar e integrar a gestão da segurança da informação no âmbito do Ministério da Justiça e Segurança Pública.

4.1.7. Para um melhor entendimento foi definido um diagrama de relacionamento dos serviços e seus respectivos componentes, objeto da presente contratação, com os demais serviços da DTIC adaptado de acordo com o *Framework* para implementar um SOC de Schinagl, S., Schoon, K., & Paans, R. (2015). O *framework* for designing a security operations centre (SOC). *Proceedings of the Annual Hawaii International Conference on System Sciences*, 2015-March, 2253–2262. https://doi.org/10.1109/HICSS.2015.270.

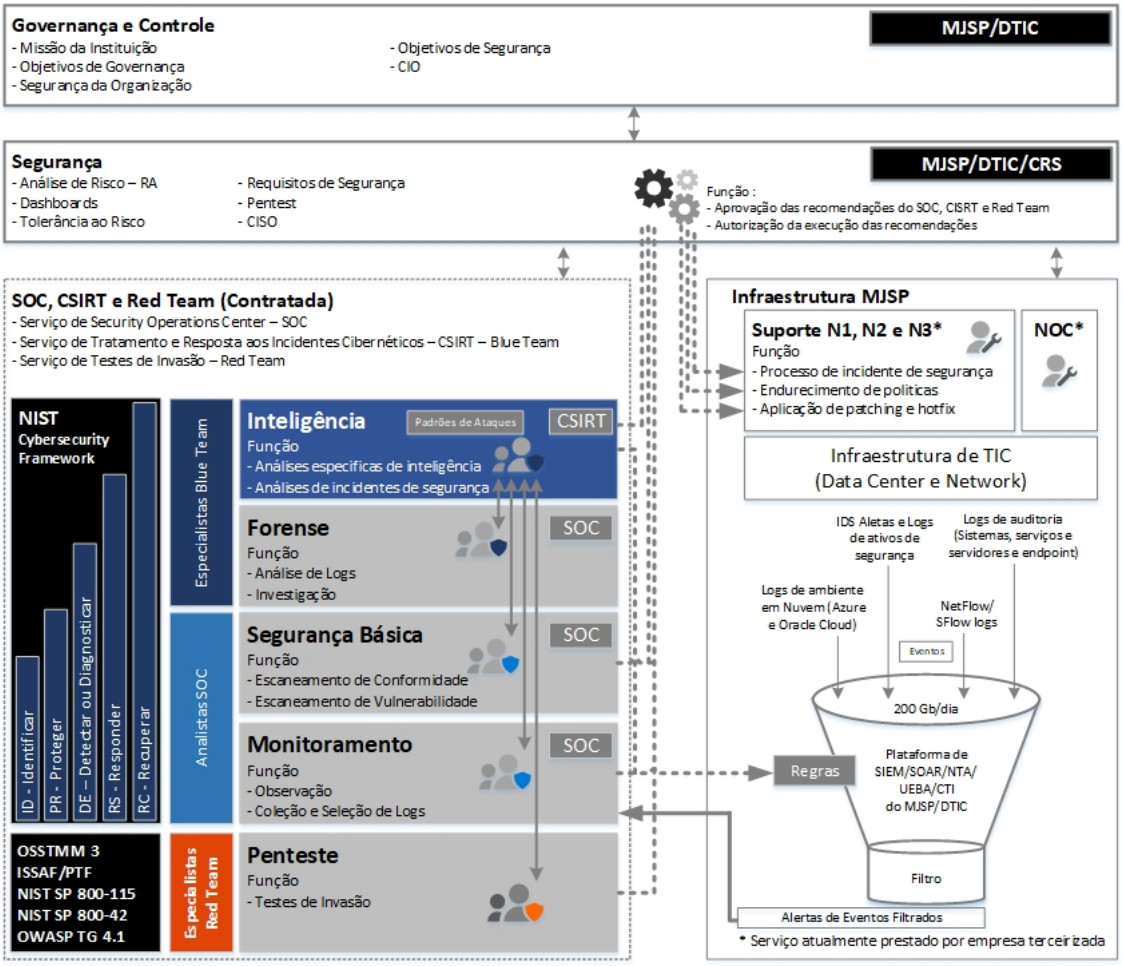

Figura 4 - Diagrama de relacionamento dos serviços e seus respectivos componentes com os demais serviços da DTIC.

4.1.8. Na Figura 4 é apresentado o diagrama de interação, para a presente contração, entre o MJSP representado pela Diretoria de Tecnologia da Informação e Comunicação - DTIC e a Coordenação de Riscos e Segurança da Informação - CRS com o papel de gestores estratégicos, táticos e operacionais com a Infraestrutura de TIC do MJSP e os serviços de SOC, de Tratamento e Resposta a Incidentes Cibernéticos e de Red Team.

4.1.8.1. A DTIC com o papel de Governança e Controle atuando na gestão estratégica realizando a conformidade e função:

4.1.8.1.1. Missão da Instituição;

4.1.8.1.2. Objetivos de Governança;

4.1.8.1.3. Segurança da Organização;

4.1.8.1.4. Objetivos de Segurança;

4.1.8.1.5. CIO (*Chief Information Officer*);

4.1.8.2. A CRS com o papel de Segurança atuando na gestão tática e operacional e realizando conformidade e funções:

4.1.8.2.1. Análise de Risco;

4.1.8.2.2. Dashboards;

4.1.8.2.3. Tolerância ao Risco;

4.1.8.2.4. Requisitos de Segurança;

4.1.8.2.5. Pentest;

4.1.8.2.6. CISO (*Chief Information Security Officer*);

4.1.8.2.7. Intermediando as ações de aprovação e autorizações das requisições entre o CSIRT e SOC com a Infraestrutura de TIC do MJSP;

4.1.8.3. Os **Serviços de Security Operations Center - SOC, Serviço de Tratamento e Resposta a Incidentes Cibernéticos - CSIRT - Blue Team e Serviço de Testes de Invasão - Red Team** executando de forma colaborativa e integrada e conforme o framework de segurança cibernética (CSF) do NIST para SOC e CSIRT, Computer Security Incident Response Team (CSIRT) Services Framework para o CSIRT, bem como OSSTMM 3, ISSAF/PTF, NIST SP 800-115 e 800-42 e OWASP TB 4.1 para o Red Team, com os papeis:

4.1.8.3.1. Inteligência - através da equipe de especialistas Blue Team do CSIRT com as funções de Análise especificas de inteligência e de incidentes cibernéticos de acordo com os Padrões de Ataques;

4.1.8.3.2. Forense - através da equipe de especialistas Blue Team com as funções de Análise de Logs e Investigação;

4.1.8.3.3. Segurança Básica - através da equipe de analistas do SOC com as funções de Escaneamento de conformidade e vulnerabilidade;

4.1.8.3.4. Monitoramento - através da equipe de analistas do SOC com as funções de Observação e Coleção e Seleção de Logs dos alertas de eventos e realizando a ajustes devidos de regras da Plataforma de SIEM/SOAR/NTA/UEBA/CTI do MJSP.

4.1.8.3.5. "Pentest" - através da equipe de especialistas Red Team com a função de Testes de invasão.

4.1.8.4. Infraestrutura de TIC do MJSP executando a sustentação do parque computacional com os papeis e componentes:

4.1.8.4.1. Suporte N1, N2 e N3 - através de equipe técnica terceirizada.

4.1.8.4.2. Aplicação de políticas, patching e hotfix de sugestões emanadas do CSIRT, SOC e Red Team, aprovadas pela área de segurança.

4.1.8.4.3. NOC - através de equipe técnica com a monitoramento da infraestrutura de TIC.

4.1.8.4.4. Plataforma de SIEM/SOAR/NTA/UEBA/CTI do MJSP com um consumo aproximado de 200 GB/dia de eventos sendo:

4.1.8.4.4.1. Logs de ambientes em Nuvem (Azure e Oracle Cloud);

4.1.8.4.4.2. IDS Alertas e Logs de ativos de segurança;

4.1.8.4.4.3. NetFlow/ SFlow Logs;

4.1.8.4.4.4. Logs de auditoria (Sistemas, serviços, servidores e endpoint);

4.1.9. A solução será composta por 3 (três) itens de serviço integrados, sendo todos executados no ambiente tecnológico das CONTRATADAS ou presencialmente quando necessário;

4.1.9.1. **Serviço de Security Operations Center - SOC**

4.1.9.1.1. **Serviço de Security Operations Center - SOC em regime operação de 24 horas por 7 dias por semana ininterruptos;**

4.1.9.2. **Serviço de Tratamento e Resposta aos Incidentes Cibernéticos - CSIRT - Blue Team em regime operação de 24 horas por 7 dias por semana ininterruptos;**

4.1.9.3. **Serviço de Testes de Invasão - Red Team, atendimento sob demanda;**

4.1.9.4. **O Serviço de Security Operations Center - SOC** e o **Serviço de Tratamento e Resposta aos Incidentes Cibernéticos - CSIRT - Blue Team** atuarão em conjunto e envolve os seguintes serviços, conforme *Information Technology Infraestructure Library* – ITIL e as atividades dos processos do volume de **Transição de Serviços e Operação de Serviços**;

4.1.9.4.1. Gerenciamento de Configurações e de Ativo de Serviços;

4.1.9.4.2. Gerenciamento de Mudanças;

4.1.9.4.3. Gerenciamento de Liberações e Implantação;

4.1.9.4.4. Gerenciamento do Conhecimento;

4.1.9.4.5. Gerenciamento de Evento;

4.1.9.4.6. Gerenciamento de Incidente;

4.1.9.4.7. Gerenciamento de Problema;

4.1.9.4.8. Gerenciamento de Requisição;

4.1.9.4.9. Gerenciamento de Acesso;

4.1.9.4.10. Desempenhar atividades de 3º nível de **Operação de Serviços** das funções:

4.1.9.4.10.1. Central de Serviços;

4.1.9.4.10.2. Gerenciamento de Operações de TI (Controle de Operações de Segurança da Informação);

4.1.9.4.10.3. Gerenciamento Técnico;

4.1.9.4.10.4. Gerenciamento de Aplicação;

4.1.9.4.11. Ambos os serviços desempenharão os seguintes objetivos e propósitos:

4.1.9.4.11.1. Gerenciar a capacidade e recursos requeridos para empacotar, construir, testar e implementar as liberações no ambiente de produção.

4.1.9.4.11.2. Estabelecer e manter a integridade dos ativos de serviços e suas configurações.

4.1.9.4.11.3. Prover conhecimento de qualidade para a organização.

4.1.9.4.11.4. Prover mecanismos de implementação eficientes e padronizados.

4.1.9.4.11.5. Garantir que os serviços possam ser gerenciados, operados e suportados conforme os requisitos definidos.

4.1.9.4.11.6. Realizar as atividades e processos necessários para garantir o gerenciamento e a entrega dos serviços conforme níveis de serviços aqui definidos.

4.1.9.4.11.7. Gerenciar continuamente a tecnologia em uso para entregar e suportar os serviços.

4.1.9.4.11.8. Melhorar a percepção de qualidade e a satisfação de usuários e clientes quanto ao uso dos serviços do MJSP.

4.1.9.4.11.9. Prover mecanismos eficientes para tratamento das questões relativas ao dia-a-dia dos serviços.

4.1.9.5. O **Serviço de Teste de Invasão - Red Team** envolve os seguintes serviços, conforme *Information Technology Infraestructure Library* – ITIL e as atividades dos processos do volume de **Transição de Serviços e Operação de Serviços**;

4.1.9.5.1. Gerenciamento do Conhecimento;

4.1.9.5.2. Gerenciamento de Incidente;

4.1.9.5.3. Gerenciamento de Problema;

4.1.9.5.4. Gerenciamento de Requisição;

4.1.9.5.5. Desempenhar atividades de 2º e 3º nível de **Operação de Serviços** das funções:

4.1.9.5.5.1. Central de Serviços;

4.1.9.5.6. Serviços de Red Team desempenharão os seguintes objetivos e propósitos:

4.1.9.5.6.1. Estabelecer e manter a integridade dos ativos de serviços e suas configurações.

4.1.9.5.6.2. Prover conhecimento de qualidade para a organização.

4.1.9.5.6.3. Garantir que os serviços possam ser gerenciados, operados e suportados conforme os requisitos definidos.

4.1.9.5.6.4. Realizar as atividades e processos necessários para garantir o gerenciamento e a entrega dos serviços conforme níveis de serviços aqui definidos.

4.1.9.5.6.5. Gerenciar continuamente a tecnologia em uso para entregar e suportar os serviços.

4.1.9.5.6.6. Prover mecanismos eficientes para tratamento das questões relativas ao dia-a-dia dos serviços.

4.1.9.5.7. A Ordem de Serviço estabelecerá o prazo para execução por ativo de serviços de teste de invasão - Red Team: sistemas web, o qual não será inferior a 1 semana nem ultrapassará 4 semanas.

4.1.9.5.8. A Ordem de Serviço estabelecerá o prazo para execução por ativo de serviços de teste de invasão - Red Team: infraestrutura, o qual não será inferior a 1 dia nem ultrapassará 1 semana.

4.1.9.6. A(s) CONTRATADA(s) deverá(ão) disponibilizar ferramenta de ITSM (Information Technology Service Management) para registro, acompanhamento e controle dos Incidentes e Requisições de Segurança e gerir todo o ciclo de vida dos chamados de SOC e BLUE TEAM, como também para os chamados de RED TEAM. Ao final do contrato, as bases de dados das ferramentas utilizadas, com todos os dados, inclusive históricos das demandas, solicitações, atendimentos e demais informações relativas à prestação de serviços deverão ser entregues e permanecerão sob custódia exclusiva do Ministério.

4.1.9.7. Prestação de informações e realização de demandas através de chamados técnicos do ministério, sob autorização e controle da CRS.

4.1.9.8. Apoiar a CRS na elaboração de minuta de comunicação à Autoridade Nacional de Proteção de Dados (ANPD) quanto ao registro de incidentes junto ao Ministério, de acordo com o Art. 48 da LGPD .

4.1.9.9. Apoiar a CRS na elaboração de minuta de comunicação à Autoridade Policial quanto ao registro de incidentes com classificação de crimes cibernético junto ao Ministério.

4.1.9.10. Configurar, com a supervisão da CRS, a Plataforma de SIEM/SOAR/NTA/UEBA/CTI do Ministério de acordo com os mecanismos de retenção e guarda de registros de conexão, nos termos da Lei 12.965/2014 que estabeleceu os princípios, garantias, direitos e deveres para o uso da Internet no Brasil.

4.1.9.11. Apoiar a CRS na realização de ações para registro e cadastramento para a inclusão do CSIRT do MJ no Grupos de Segurança e Resposta a Incidentes (CSIRTs) Brasileiros, junto ao Centro de Estudos, Resposta e Tratamento de Incidentes de Segurança - CERT.BR e junto à Rede Federal de Gestão de Incidentes Cibernéticos.

4.1.9.12. Apoiar a CRS na divulgação de ações de segurança da informação (Alertas, Conscientização e Recomendações) aos usuários finais, equipes de TIC e aos gestores com o objetivo de fortalecer uma estrutura para projetar, implementar, monitorar, manter e melhorar a segurança da informação consistente com a cultura organizacional, conforme preceitua a ABNT NBR ISO/IEC 27000, bem como para acompanhamento e avaliação dos indicadores de performance e serviços de SOC e CSIRT pelos gestores de TIC do Ministério a CONTRATADA deverá desenvolver e manter um **Portal WEB de CSIRT do Ministério** para a disponibilização de tais informações, como também informações para registro de notificações por usuários externos ao Ministério com uso de tecnologias seguras, definidas pela CRS com apoio da Contratada, para comunicações através de canal seguro**.**

4.1.9.13. A CONTRATADA ficará, durante a vigência contratual do presente objeto, incumbida de realizar parametrizações, customizações e manutenções na **Plataforma de SIEM/SOAR/NTA/UEBA/CTI do Ministério.** Atualmente, a ferramenta implantada e em utilização, é a **Azure Sentinel** do fabricante **Microsoft**. Caso o Ministério opte por outra solução a mesma deverá ser absorvida pela CONTRATADA sem ônus para a CONTRATANTE.

4.1.9.14. A CONTRATANTE poderá incluir novas atividades correlatas (atualização ou novas tecnologias da infraestrutura) que englobem as atividades de evolução da infraestrutura, para atendimento de ajustes, implantação de novas tecnologias, melhorias ou necessidades específicas no ambiente tecnológico do Ministério. As atualizações de atividades serão feitas através de solicitações específicas formalizadas pela CONTRATANTE. As novas atividades devem atender aos mesmos indicadores de níveis de serviço mínimos e requisitos obrigatórios previstos neste termo.

4.1.9.15. Para um melhor entendimento das responsabilidades a serem executadas pelos serviços objeto da presente contratação, foi definido uma Matriz de Responsabilidade R.A.C.I apresentado a seguir, a qual esta alinhada com a Figura 04 - Diagrama de relacionamento dos serviços e seus respectivos componentes com os demais serviços da DTIC e envolve todos os atores com participação no SOC e na Área de Segurança Cibernética;

Tabela 5 - Matriz de Responsabilidade R.A.C.I - Plataforma de SIEM/SOAR/NTA/UEBA/CTI do Ministério e Área de Segurança da Cibernética

Matriz de Responsabilidade R.A.C.I - Plataforma de SIEM/SOAR/NTA/UEBA/CTI do Ministério e Área de Segurança da Cibernética													
Serviços		**Transição de Serviços**				**Operação de Serviços**							
		Processos				**Processos**						**Funç**	
Situação	**Descrição**	**Ger. de Configurações e de Ativo de Serviços**	**Ger. de Mudanças**	**Ger. de Liberações e Implantação**	**Ger. do Conhecimento**	**Ger. de Evento**	**Ger. de Incidente**	**Ger. de Problema**	**Ger. de Requisição**	**Ger. de Acesso**	**Central de Serviços**	**Ger. de Operações de TI**
Nova contratação	Solução de SOC	C/I	C/I	C/I	C/I	R/C/I	R/C/I	R/C/I	R/C/I	C/I	C/I	C/I
	Serviços de CSIRT Blue Team	R/C/I	R/C/I	R/C/I	R/C/I	R/C/I	R/C/I	R/C/I	R/C/I	R/C/I	R/C/I	R/C/I
	Serviços de Red Team	-	-	-	R/C	-	R/C	R/C	R/C/I	-	R/C/I	-
Contratação existente	Serviço de NOC	C/I	C/I	C/I	C/I	C/I	C/I	C/I	C/I	C/I	C/I	C/I
	Serviços de Infraestrutura	R/C/I	R/C/I	R/C/I	R/C/I	R/C/I	R/C/I	R/C/I	R/C/I	R/C/I	R/C/I	R/C/I
Contratante	**MJSP\DTIC\CRS**	**A/C/I**	**A/C/I**	**A/C/I**	**A/C/I**	**A/C/I**	**A/C/I**	**A/C/I**	**A/C/I**	**A/C/I**	**A/C/I**	**A/C/I**

Legenda:
R: Responsável por executar uma atividade;
A: Autoridade, quem responde pela atividade, o dono
C: Consultado, quem deve ser consultado e participar da decisão ou atividade no momento que for executada;
I: Informado, quem deve receber a informação de que uma atividade foi executada;
Obs.: As atividades da nova contratação são junto a Plataforma de SIEM/SOAR/NTA/UEBA/CTI do Ministério (item 4.1.8.3.4) e não conflitará com as atividades da contratação existente, pois a mesma, atuará de forma subsidiária ao contrato existente quando da necessidade de ações junto a Área de Segurança Cibernética, conforme definido no item 4.1.8.4.1.

4.1.10. A matriz RACI referente a tabela 5 poderá ser modificada sempre que a CONTRATANTE avaliar como necessária, respeitando os limites definidos neste termo de referência.

4.1.11. **Indicadores de performance do Serviço de Security Operation Center - SOC**

4.1.11.1. A frequência de aferição dos indicadores de performance será mensal, porém com registros diários quando aplicável, devendo a contratada elaborar Relatório Mensal de Atividades, apresentando-o ao Ministério até o quinto dia útil do mês subsequente ao da prestação do serviço.

4.1.11.2. Devem constar desse relatório, entre outras informações, as vulnerabilidades encontradas com as respectivas correções/mitigações sugeridas, riscos, ameaças, alertas, incidentes, indicadores de performance, metas de níveis de serviço alcançados, recomendações técnicas, administrativas e gerenciais para o próximo período e demais informações relevantes para a gestão contratual. O conteúdo detalhado e a forma do relatório gerencial serão definidos pelas partes.

4.1.11.3. Caberá à Comissão de Fiscalização do contrato analisar mensalmente o Relatório Mensal de Atividades executados pela Contratada, observando os indicadores e os níveis de serviço alcançados.

4.1.11.4. Os indicadores de performance são flexíveis em quantidade e qualidade e abrangem, mas não se limitam, os que estão descritos na tabela a seguir:

Tabela 6 - Indicadores de Performance do Serviço SOC

Categoria	**Subcategoria**	**Métrica**	**Unidade de medida**
Governança	Conformidade	Quantidade de violações de políticas	número
		Porcentagem de sistemas com controles de segurança testados	percentual
	Privacidade	Quantidades de incidentes notificados a ANPD	número
	CSIRT	Avaliação da Maturidade do CSIRT de acordo com o "ENISA CSIRT maturity assessment model versão 2.0 - 30 de abril de 2019"	Nível e percentual de evolução
	Orquestração	Automação/Orquestração dos processos continuidade de negocio e resposta a incidentes cibernéticos	Nível e percentual de evolução
Técnico	Ameaças	Nível de segurança	Classificação de cores
		Atribuição de ameaças a atores (usando inteligência de ameaças)	a definir
	Vulnerabilidade	Tempo para remediação da vulnerabilidade	tempo
		Gravidade da vulnerabilidade	escala
		Incidentes de vulnerabilidade conhecida vs. desconhecida	número/escala
		Exposição à vulnerabilidade	escala

	Risco	Posição de risco	escala
		Risco por sistema/serviço	escala
		Principais riscos	texto
		Tipos de casos (MITRE ATT&CK)	número
	Alerta	Tempo por investigação de alerta	tempo
		Índice de geração de alerta	número/escala
		Número de alertas que permanecem por analisar (em aberto)	número
		Criticidade de um alerta	escala
	Incidente	Prioridade de incidentes	texto
		Total de incidentes por mês	número
		Número de ataques bem sucedidos	número/percentual
		Tempo médio de detecção (MTTD)	tempo
		Tempo médio para resolução/recuperação (MTTR)	tempo
		Custo por incidente	valor/texto
		Sucesso na mitigação	número/percentual
	Resiliência	Tempo médio gasto por ataque (MTTA)	tempo
		Eficiência defensiva	escala
		Repercussão do ataque	texto
		Quantidade de interrupções	número e percentual
		Tempo de interrupções	tempo
Pessoas	Performance	Número de incidentes encerrados em um turno	número
		Análise de escalação de caso	número
Gerais	Performance	Taxa de falso positivo	percentual
		Tempo médio de analise	tempo
		Nível de disponibilidade da infraestrutura de SOC	percentual
	Cobertura	Quantidade de ativos monitorados	número
		Quantidade de ativos monitorados vs. Quantidade total de ativos	número e percentual

4.1.12. Para fins de execução do contrato, a(s) CONTRATADA(s) deverá(ão) atender aos requisitos técnicos especificados neste Termo de Referência e todos os processos poderão ser amadurecidos conforme a evolução da prestação dos serviços durante a execução do contrato.

4.1.13. ***Requisitos Técnicos***

4.1.14. **Grupo 1: Item 1 - Serviço de Security Operations Center - SOC**

4.1.14.1. O **SOC** funcionará 24 horas por dia e 7 dias por semana, tendo por **objetivo sustentar e operar a Plataforma de SIEM/SOAR/NTA/UEBA/CTI do Ministério da Justiça e Segurança pública**, bem como a realização permanente de ações proativas voltadas para a segurança do parque computacional do Ministério da Justiça e Segurança Pública, sem prejuízo aos níveis de serviços definido neste Termo de Referência, bem como realizando as seguintes atividades, não se restringindo somente a elas:

4.1.14.1.1. Monitoramento contínuo e análise, predizendo, prevendo, prevenindo, detectando e respondendo efetivamente as ameaças de todos incidentes cibernéticos.

4.1.14.1.2. Gerar painéis dinâmicos e em tempo real da situação atual de segurança do Ministério informando através de um score o nível de segurança.

4.1.14.1.3. Atuar como suporte de primeiro nível aos incidentes cibernéticos identificando, classificando, interrompendo, catalogando todas as tentativas de ataque aos sistemas e à infraestrutura do ministério.

4.1.14.1.4. Demandar ao NOC ou ao Suporte N1, N2 e N3 da infraestrutura de TIC do Ministério, medidas a serem tomadas para evitar ou conter incidente.

4.1.14.1.5. Atuar no sentido de interromper um incidente quando da inoperância do NOC ou suporte N1, N2 e N3. Para incidentes que requeiram atuação imediata e em circunstâncias onde a equipe do NOC não esteja disponível ou não possa atuar, serão definidos protocolos para atuação da equipe de SOC e Blue Team.

4.1.14.1.6. Outros serviços os quais o SOC atuará em substituição ao NOC, poderão ser definidos durante a vigência do contrato, por meio de reuniões entre a CONTRATANTE e a CONTRATADA

4.1.14.1.7. Atuar em harmonia com o NOC do ministério.

4.1.14.1.8. Prestar o serviço de SOC realizando a **detecção, triagem, investigação e resposta a incidente** de eventos utilizando Plataforma de SIEM/SOAR/NTA/UEBA/CTI do Ministério de acordo com as seguintes funções:

4.1.14.1.8.1. Camada de Automação:

4.1.14.1.8.1.1. Orquestração, Automação e Resposta de Segurança (Security Orchestration, Automation, and Response - SOAR);

4.1.14.1.8.2. Camada de Análise e Correlacionamento:

4.1.14.1.8.2.1. Monitoramento de estação de trabalho (Endpoint Detection and Response - EDR);

4.1.14.1.8.2.2. Análise de Tráfego de Rede (Network Traffic Analysis - NTA);

4.1.14.1.8.2.3. Análise de Comportamento de Usuário (User Entity and Behavior Analytics - UEBA);

4.1.14.1.8.2.4. Análise de Inteligência de Ameaças Cibernéticas (Cyber Threat Intelligence - CTI);

4.1.14.1.8.3. Camada de coleta:

4.1.14.1.8.3.1. Informações de segurança e gestão de eventos (Security Information and Event Management - SIEM).

4.1.14.1.9. Configuração, manutenção, monitoramento e operação da Plataforma de SIEM/SOAR/NTA/UEBA/CTI do Ministério.

4.1.14.1.10. Monitoramento e Análise de toda a infraestrutura do Ministério, utilizando-se de análise dos logs disponibilizados em tempo real através da Plataforma de SIEM/SOAR/NTA/UEBA/CTI do Ministério. Para o devido dimensionamento do esforço de trabalho necessário, atualmente, a Plataforma de SIEM/SOAR/NTA/UEBA/CTI coleta eventos que representam aproximadamente 200 GB/dia e 5000 EPS.

4.1.14.1.11. Realização de atividades de preparação do processo de coleta de logs, incluindo a normalização, filtragem, redução, agregação e priorização, bem como atividades que envolve o processamento, normalização, armazenamento, e demais atividades de correlacionamento de logs que serão realizadas nas ferramentas da Plataforma de SIEM/SOAR/NTA/UEBA/CTI do Ministério, a partir dos dados disponibilizados pelo Ministério quando ocorrer a contratação.

4.1.14.1.12. Caso as ferramentas de propriedade do Ministério não atendam a completa execução dos serviços objeto da presente contratação a contratada poderá adotar solução tecnológica complementar em termos de hardware e software.

4.1.14.1.13. A CONTRATADA poderá utilizar soluções de hardware e software proprietárias desde que previamente autorizadas pelo CONTRATANTE, arcando a CONTRATADA com todos os custos diretos e indiretos inerentes a utilização de solução tecnológica e seus licenciamentos necessários.

4.1.14.1.14. Prevê-se que o SOC funcionará como o centralizador de todas as informações de segurança da informação e suporte de primeiro nível para os processos previstos no item 4.1.9.4, por isso, a necessidade de seu funcionamento ser ininterrupto. O dimensionamento da equipe do SOC será a cargo da contratada em quantitativo mínimo que garanta o monitoramento ininterrupto de seu funcionamento, a qualidade das informações

prestadas e estar apta a atuar no estado da arte em termos de segurança da informação, assim como cumprir os Níveis Mínimos de Serviço Exigidos determinados.

4.1.14.2. Principais atividades a serem executadas de forma contínua pela CONTRATADA:

4.1.14.2.1. Acompanhar a execução dos serviços para o cumprimento dos níveis de serviço estabelecidos;

4.1.14.2.2. Priorizar os atendimentos críticos, conforme definição do CONTRATANTE;

4.1.14.2.3. Monitorar de forma permanente e avaliar criticamente os produtos e serviços de segurança do CONTRATANTE;

4.1.14.2.4. Prover os fiscais do contrato com os relatórios técnicos e gerenciais suficientes para a comprovação dos serviços realizados;

4.1.14.2.5. Supervisionar sua equipe na execução dos serviços de Security Operations Center e Serviço de Tratamento e Resposta aos Incidentes Cibernéticos - CSIRT - Blue Team;

4.1.14.2.6. Elaborar e propor plano de execução dos serviços;

4.1.14.2.7. Definir plano de treinamento inicial e contínuo dos profissionais que executam os serviços;

4.1.14.2.8. Executar outros serviços correlatos à supervisão dos profissionais na execução dos serviços;

4.1.14.2.9. Orientar a atuação da equipe técnica em situações críticas de trabalho, bem como interagir com os usuários quando a situação requerer;

4.1.14.2.10. Fornecer sugestões e auxiliar na construção e manutenção contínua, com o apoio e aprovação do Ministério da Justiça e Segurança pública, de procedimentos sistematizados e da base de conhecimento, contemplando todas as soluções de problemas resolvidos com respostas padronizadas;

4.1.14.2.11. Consolidar os relatórios de atividades mensais (mês calendário), referente aos serviços, provendo informações gerenciais ao CONTRATANTE;

4.1.14.2.12. Supervisionar sua equipe de profissionais na execução das ações conjuntas com a área de infraestrutura, cumprindo a política de segurança da informação do Ministério e aplicando as melhores práticas de segurança;

4.1.14.2.13. Consolidar todas as soluções adotadas na execução das atividades em manuais de procedimentos e em base de conhecimento;

4.1.14.2.14. Elaborar mensalmente relatórios de desempenho, auditoria e operação dos ativos sob sua administração. O processo de auditoria do CONTRATANTE é contínuo;

4.1.14.2.15. Implantar as melhorias solicitadas pelos servidores do CONTRATANTE através das aberturas de chamados no sistema de gestão de serviços de TI;

4.1.14.2.16. Sugerir novas tecnologias para modernizar o ambiente tecnológico, buscando subsidiar a equipe do CONTRATANTE na gestão de segurança da informação;

4.1.14.2.17. Aplicar as práticas do ITIL 3 ou superior.

4.1.14.2.18. Manter atualizado o *Configuration Management Database* (CMDB) na ferramenta de Gerenciamento de Serviços de TI utilizada pelo CONTRATANTE ou fornecida pela CONTRATADA sem custo adicional, quanto aos recursos administrado;

4.1.14.2.19. Consolidar as sugestões de melhoria;

4.1.14.2.20. Elaborar relatório detalhado das funcionalidades necessárias de equipamentos e softwares a serem adquiridos, destinados à Segurança da Informação do CONTRATANTE;

4.1.14.2.21. Subsidiar tecnicamente, quando demandado, os processos de aquisição;

4.1.14.2.22. Subsidiar os servidores do CONTRATANTE quanto ao dimensionamento da capacidade de hardware e configuração dos ativos de segurança;

4.1.14.2.23. Abrir chamados técnicos, na língua inglesa ou outro idioma quando necessário, para os serviços de suporte técnico remoto das soluções de hardware e software de TI do CONTRATANTE, quanto aos recursos administrados;

4.1.14.2.24. Avaliação do ambiente, serviços e sistemas, monitoramento contínuo, apoiar o CONTRATANTE na homologação de soluções de segurança e na execução de atividades de controle de acessos e demais serviços relacionados à Segurança da Informação no ambiente tecnológico do CONTRATANTE.

4.1.14.2.25. Instalar ou customizar softwares aplicativos e equipamentos relacionados aos serviços, objeto desse TR, homologados para uso no Ministério da Justiça, por solicitação do CONTRATANTE;

4.1.14.2.26. Receber as diretrizes relacionadas à área de Segurança da Informação e providenciar a execução e alocação de recursos de trabalho;

4.1.14.2.27. Apoiar e participar na implementação dos processos bem como na mensuração dos indicadores de objetivos instituídos pelo CONTRATANTE;

4.1.14.2.28. Realizar as atividades em estrita observância na Política de Segurança da Informação (PSI) e demais normas estipuladas pelo CONTRATANTE;

4.1.14.2.29. Consolidar em manuais e *scripts* todos os serviços e soluções adotadas sejam eles novos ou já implantados no CONTRATANTE;

4.1.14.2.30. Auxiliar na elaboração dos procedimentos e metodologias, e verificar e reportar o cumprimento dos mesmos pelas demais áreas de TI;

4.1.14.2.31. Apoiar o CONTRATANTE na análise e definição das regras de uso dos recursos computacionais do CONTRATANTE;

4.1.14.2.32. Implantar as melhorias solicitadas pelos servidores do CONTRATANTE através das ordens de serviço;

4.1.14.2.33. Monitorar e propor soluções aos projetos/atividades em andamento otimizando-os quanto aos requisitos de Segurança da Informação;

4.1.14.2.34. Monitorar o ambiente lógico da CONTRATANTE identificando de forma proativa possíveis tentativas ou ataques aos ativos da CONTRATANTE;

4.1.14.2.35. Participar, quando solicitado, de reunião com os gerentes e participantes dos projetos de desenvolvimento e manutenção de sistemas e administração de dados, a fim de prover soluções para projetos/atividades em andamento;

4.1.14.2.36. Participar da implantação de projetos/soluções, substituição e atualização de soluções destinadas à Segurança da Infraestrutura de rede;

4.1.14.2.37. Implantar e configurar regras na **Plataforma de SIEM/SOAR/NTA/UEBA/CTI do Ministério**;

4.1.14.2.38. Realizar análise de tentativas de invasão a sistemas e equipamentos;

4.1.14.2.39. Auxiliar o CONTRATANTE nos projetos de Segurança da Informação;

4.1.14.2.40. Propor procedimentos de Segurança da Informação;

4.1.14.2.41. Apoiar o CONTRATANTE na revisão e atualização da política de segurança da informação;

4.1.14.2.42. Executar periodicamente testes de alta disponibilidade na infraestrutura do CONTRATANTE com o objetivo de validar o seu funcionamento;

4.1.14.2.43. Elaborar um plano de teste do ambiente de infraestrutura de segurança do CONTRATANTE, que deverá ser mantido atualizado continuamente. Este plano servirá de referência para elaboração de um Plano de Continuidade dos Serviços de Segurança da Informação;

4.1.14.2.44. Sugerir a atualização de versão de todos os softwares e hardwares do parque tecnológico que sustenta a **Plataforma de SIEM/SOAR/NTA/UEBA/CTI do Ministério**;

4.1.14.2.45. Execução de mudanças de configuração nos ativos sob sua administração;

4.1.14.2.46. Executar medidas preventivas com objetivo de identificar e conter possíveis ataques e invasões aos ativos da CONTRATANTE;

4.1.14.2.47. Execução das atividades relativas aos normativos e governança do CONTRATANTE naquilo que for relativo à sua área de atuação.

4.1.14.3. Os produtos listados abaixo devem ser criados e atualizados em conformidade com os padrões e necessidade do Ministério da Justiça:

4.1.14.3.1. Documento contendo a volumetria média de acessos, listando os limites a partir do qual serão considerados um incidente cibernético;

4.1.14.3.2. Guia de procedimentos de sustentação do serviço de proteção de e-mail;

4.1.14.3.3. Guia de procedimentos de sustentação do serviço de antivírus;

4.1.14.3.4. Guia de procedimentos de sustentação do serviço de proteção unificada;

4.1.14.3.5. Guia de procedimentos de sustentação do serviço de gestão unificado de ameaças;

4.1.14.3.6. Guia de procedimentos de sustentação do serviço de firewall de aplicação;

4.1.14.3.7. Guia de procedimentos de sustentação do serviço de gerenciamento de vulnerabilidades;

4.1.14.3.8. Relatórios de Continuidade de Negócios contendo indicadores de capacidade e disponibilidade dos ativos, além de projeções de elevação do uso dos recursos computacionais;

4.1.14.3.9. Documento contendo os requisitos de segurança da informação para a homologação e liberação de serviços, aplicações, servidores de rede;

4.1.14.3.10. Catálogo de Serviços e Base de Itens de Configuração;

4.1.14.3.11. Base de Conhecimento.

4.1.14.4. Deve permitir ajustar os critérios e pontuações de riscos já existentes na ferramenta como também criar novas regras de negócio que contribuam para a análise e pontuação de risco para atividades consideradas suspeitas ou precisam ser monitoradas;

4.1.14.5. A CONTRATADA deverá apoiar o CONTRATANTE em caso de mudanças requeridas por conta de atualizações ou remanejamentos de infraestrutura;

4.1.14.6. A CONTRATADA deverá realizar a configuração das ferramentas que compõem as soluções sob sua administração, a fim de garantir o uso eficiente delas;

4.1.14.7. Sempre que houver atendimento, a CONTRATADA deverá enviar relatório de atividades por e-mail para o CONTRATANTE;

4.1.14.8. A CONTRATADA deverá acionar o fabricante das ferramentas, sob sua administração, sempre que necessário, sem nenhum custo adicional para o CONTRATANTE.

4.1.14.9. Monitoramento e Visibilidade

4.1.14.9.1. Visa o monitoramento contínuo e ininterrupto de ataques cibernéticos direcionados ao Ministério da Justiça, através de correlacionamento de logs e/ou comportamento anômalo de aplicações, serviços e infraestrutura que possam gerar eventos de segurança da informação, aos quais devem ser analisados, podendo estes serem transformados em um incidente cibernético, conforme definido em processo de gestão de incidentes.

4.1.14.10. **O SOC pode ser executado no ambiente da CONTRATANTE ou da CONTRATADA.**

4.1.14.10.1. **Quando no ambiente da CONTRATADA, deve estar ativo e deve atender aos seguintes requisitos mínimos**:

4.1.14.10.1.1. Estar localizado fisicamente em **território nacional**;

4.1.14.10.1.2. Utilizar sistema de gerenciamento de CFTV, que viabilizem o monitoramento de pessoas, equipamentos e sistemas relacionadas ao contrato do MJSP e cujas imagens possam ser recuperadas por no mínimo 90 (noventa) dias;

4.1.14.10.1.3. Efetuar registro de entrada e saída dos visitantes, com identificação individual, em todos os acessos ao SOC por no mínimo 90 dias;

4.1.14.10.1.4. Possuir solução de monitoramento de disponibilidade e desempenho de seus ativos de TIC e de subsistemas;

4.1.14.10.1.5. O perímetro deve ser protegido contra intrusão e acesso indevido;

4.1.14.10.1.6. Ser vigiado fisicamente de forma ininterrupta por segurança especializada em regime de 24x7x365;

4.1.14.10.1.7. Ter controle de acesso físico com pelo menos 2 (dois) fatores de autenticação;

4.1.14.10.1.8. Ser configurado de forma que a falha de um dos equipamentos isoladamente NÃO interrompa a prestação dos serviços;

4.1.14.10.1.9. Ter sistema de provimento ininterrupto de energia elétrica, composto por grupo gerador e UPSs (unidades de alimentação elétrica contínua) para garantir a transição entre o fornecimento normal de energia e o grupo gerador;

4.1.14.10.1.10. Ter componentes de segurança necessários para garantir a preservação dos dados em casos de incêndio e execução de plano de recuperação de catástrofes;

4.1.14.10.1.11. Deverá possuir processos implementados que garantam a segurança das informações do CONTRATANTE, em conformidade com a norma ABNT NBR ISO/IEC 27001.

4.1.14.10.1.12. A Contratada deverá disponibilizar à Contratante acesso aos sistemas que utilize na prestação do serviço e que não sejam do MJSP.

4.1.14.10.2. **Quando no ambiente da CONTRATANTE, deve estar ativo e deve atender aos seguintes requisitos mínimos**:

4.1.14.10.2.1. Possuir solução de monitoramento de disponibilidade e desempenho de seus ativos de TIC e de subsistemas;

4.1.14.10.2.2. O perímetro lógico deve ser protegido contra intrusão e acesso indevido;

4.1.14.10.2.3. Ser configurado de forma que a falha de um dos equipamentos isoladamente NÃO interrompa a prestação dos serviços;

4.1.14.10.2.4. Deverá possuir processos implementados que garantam a segurança das informações do CONTRATANTE, em conformidade com a norma ABNT NBR ISO/IEC 27001.

4.1.14.10.2.5. A Contratada deverá disponibilizar à Contratante acesso aos sistemas que utilize na prestação do serviço e que não sejam do MJSP.

4.1.15. **Grupo 1: Item 2 - Serviço de Tratamento e Resposta aos Incidentes Cibernéticos - CSIRT - Blue Team**

4.1.15.1. O **CISRT - Blue Team** funcionará de forma ininterrupta 24 horas por dia e 7 dias por semana, associado ao SOC para atividades de apoio ao suporte de primeiro nível e contenção de ataques, bem como, para atividades e suporte de segundo nível em diante e tendo por **objetivos proativos prevenir, tratar, responder**, além de **objetivos reativos de analisar, documentar e indicar** como conter e remediar os eventos de segurança da informação e de dados que foram transformados em um incidente cibernético, sem prejuízo aos níveis de serviços definido neste Termo de Referência.

4.1.15.2. A CONTRATADA deverá realizar avaliação completa do ambiente do CONTRATANTE com o objetivo de identificar lacunas ou oportunidades de melhoria (Gap Analysis) com o objetivo de avaliar a maturidade dos controles de segurança do CONTRATANTE.

4.1.15.2.1. A análise dos controles de segurança deverá ser realizada obedecendo o framework de segurança cibernética (CSF) do NIST.

4.1.15.2.2. A análise deverá ser conduzida por profissional com certificação CISSP – Certified Information Systems Security, que será responsável pela apresentação dos resultados da análise ao gestor, fiscais do contrato e gestores de TI do Ministério da Justiça e Segurança pública.

4.1.15.3. Deverão ser observadas as orientações e técnicas emanadas pelos padrões internacionais e pela Rede Federal de Gestão de Incidentes Cibernéticos, além de outros apresentados pela contratada, caso haja em seu portfólio normativos que comprovadamente complementem os demonstrados abaixo:

4.1.15.3.1. NIST Cybersecurity Framework, Version 1.1 ou mais recente;

4.1.15.3.2. NIST Privacy Framework, Version 1.0 ou mais recente;

4.1.15.3.3. NIST Special Publication 800-61 Revision 2 (Computer Security Incident Handling Guide);

4.1.15.3.4. NIST Special Publication 800-115 (Technical Guide to Information Security Testing and Assessment);

4.1.15.3.5. NIST Special Publication 800-53 (Security and Privacy Controlsfor Information Systems and Organizations);

4.1.15.3.6. SANS Incident Handler's Handbook;

4.1.15.3.7. CIS Control, Version 7.1 ou mais recente;

4.1.15.3.8. ISO/IEC 27035-1:2016 - Information technology — Security techniques — Information security incident management — Part 1: Principles of incident management;

4.1.15.3.9. ISO/IEC 27035-2:2016 - Information technology — Security techniques — Information security incident management — Part 2: Guidelines to plan and prepare for incident response;

4.1.15.3.10. ISO/IEC 27035-3:2020 - Information technology — Information security incident management — Part 3: Guidelines for ICT incident response operations;

4.1.15.4. Incidente cibernético - ocorrência que comprometa, real ou potencialmente, a disponibilidade, a integridade, a confidencialidade ou a autenticidade de sistema de informação ou das informações processadas, armazenadas ou transmitidas por esse sistema, que poderá também ser caracterizada pela tentativa de exploração de vulnerabilidade de sistema de informação que constitua violação de norma, política de segurança, procedimento de segurança ou política de uso (Decreto Nº10.748, de 16 de julho de 2021 - Cap. I, Art.3º - V).

4.1.15.5. Para divulgação de ações de segurança da informação (Alertas, Conscientização e Recomendações) aos usuários finais, equipes de TIC e aos gestores com o objetivo de fortalecer uma estrutura para projetar, implementar, monitorar, manter e melhorar a segurança da informação consistente com a cultura organizacional, conforme preceitua a ABNT NBR ISO/IEC 27000, bem como para acompanhamento e avaliação dos indicadores de performance e serviços de SOC e CSIRT pelos gestores de TIC do Ministério a CONTRATADA deverá desenvolver e manter um **Portal WEB de CSIRT do Ministério** hospedado na infraestrutura da CONTRATANTE, para a disponibilização de tais informações, como também informações para registro de notificações por usuários externos ao Ministério com uso de tecnologias seguras, definidas pela CRS, para comunicações através de canal seguro.

4.1.15.6. A seguir é apresentado a Tabela 7 com as categorias quanto a natureza, impacto ao negócio, impacto quanto as informações e esforço de recuperação de incidentes com o objetivo de definir o escopo dos serviços prestados pela CONTRATADA;

Tabela 7 - Categorias quanto natureza do impacto

Natureza	Descrição da Natureza	Impacto ao Negócio	Descrição do Impacto ao negócio	Impacto quanto as informações	Descrição do Impacto quanto as informações	Esforço de Recuperação	Descrição do esforço necessário para a recuperação
Evento	Algo que ocorreu nos sistemas de informação, infraestrutura ou dados mas não necessariamente malicioso ou que requer uma ação.	**Nenhum**	Nenhum efeito na capacidade da organização de fornecer todos os serviços a todos os usuários	**Nenhum**	Nenhuma informação foi exfiltrada, alterada, apagada ou de outra forma comprometida	**N/A**	Não se aplica
Alerta	Algo potencialmente acionável. Uma indicação de um evento acionável.	**Baixo**	Efeito mínimo; a organização ainda pode fornecer todos os serviços críticos a todos os usuários, mas perdeu eficiência			**Regular**	O tempo para a recuperação é previsível com os recursos existentes
Incidente	Qualquer evento com a violação da confidencialidade, integridade, disponibilidade e privacidade, mas sem impacto à missão ou ao negócio.	**Médio**	A organização perdeu a capacidade de fornecer um serviço essencial e crítico para um subconjunto de usuários do sistema	**Quebra de privacidade**	Informações sensíveis pessoalmente identificáveis (PII) de contribuintes, funcionários, beneficiários, etc., foram acessadas ou exfiltradas	**Complementado**	O tempo para a recuperação é previsível com recursos adicionais
				Quebra de propriedade	Informações proprietárias não classificadas, tais como informações de infraestrutura crítica protegida (PCII), foram acessadas ou exfiltradas		
				Perda de integridade	As informações sensíveis ou proprietárias foram alteradas ou excluídas		
Incidente grave	Qualquer evento com a violação da confidencialidade, integridade, disponibilidade e privacidade, com impacto à missão ou ao negócio.	**Alto**	A organização não é mais capaz de fornecer alguns serviços essencial e críticos a nenhum usuário e ou o comprometimento de dados institucionais e ou pessoais.	**Quebra de privacidade**	Informações sensíveis pessoalmente identificáveis (PII) de contribuintes, funcionários, beneficiários, etc., foram acessadas ou exfiltradas	**Estendido**	O tempo para a recuperação é imprevisível; são necessários recursos adicionais e ajuda externa
				Quebra de propriedade	Informações proprietárias não classificadas, tais como informações de infraestrutura crítica protegida (PCII), foram acessadas ou exfiltradas		
				Perda de integridade	As informações sensíveis ou proprietárias foram alteradas ou excluídas		
Invasão e/ou Vazamento	Perda ou comprometimento de sistemas, dados regulados, propriedade empresarial que dispara uma ação ou resposta legal que vai além dos serviços de monitoramento e respostas a incidentes.			**Quebra de privacidade**	Informações sensíveis pessoalmente identificáveis (PII) de contribuintes, funcionários, beneficiários, etc., foram acessadas ou exfiltradas	**Não Recuperável**	A recuperação do incidente não é possível (por exemplo, os dados sensíveis exfiltrados e postados público); lançar investigação
				Quebra de propriedade	Informações proprietárias não classificadas, tais como informações de infraestrutura crítica protegida (PCII), foram acessadas ou exfiltradas		
				Perda de integridade	As informações sensíveis ou proprietárias foram alteradas ou excluídas		

4.1.15.7. O início do processo de resposta a incidente cibernético se dará, sempre que um evento adverso for detectado e descrito no presente termo de referência, porém não se limitando a este. Poderá o corpo técnico de segurança do CONTRATANTE também e a qualquer tempo, abrir um incidente de segurança, o qual deve seguir no mínimo o seguinte fluxo e requisitos:

4.1.15.7.1. Após o incidente aberto, será de responsabilidade do grupo de resposta a incidente de segurança (CSIRT – Blue Team) da CONTRATADA, analisar os logs e artefatos, a fim de no primeiro instante identificar as fontes geradoras de tais logs.

4.1.15.7.2. Uma vez realizado as análises iniciais do incidente gerado, o grupo de resposta a incidente de segurança (CSIRT – Blue Team) da CONTRATADA, deverá trabalhar para identificar quais foram os principais vetores de ataque ao ambiente do CONTRATANTE.

4.1.15.7.3. Juntamente com o CONTRATANTE o grupo de resposta a incidente de segurança (CSIRT – Blue Team) da CONTRATADA, deverá definir a severidade/impacto do incidente . A severidade/impacto do incidente de segurança da informação será definida através da combinação de urgência e impacto, onde impacto é definido como a medida de criticidade do negócio referente ao incidente, e urgência refere-se à velocidade necessária para resolver um incidente.

4.1.15.7.4. Após análises iniciais do incidente, caberá ao grupo de resposta a incidente de segurança (CSIRT – Blue Team), realizar uma análise mais profunda do incidente baseando-se no comportamento do ataque e/ou artefato (malware).

4.1.15.7.5. Todo o processo de análise e resultados obtidos, devem ser documentados a todo tempo na ferramenta de ITSM, para que o CONTRATANTE acompanhe todos os passos para a solução do incidente.

4.1.15.7.6. Uma vez identificado comportamento e os principais vetores de ataque, o grupo de resposta a incidente (Blue Team) da CONTRATADA, deverá definir uma estratégia para a mitigação e contenção do ataque em questão.

4.1.15.7.7. Mitigado o incidente de segurança, o próximo passo exigido é que a CONTRATADA através do grupo de resposta a incidente de segurança (CSIRT – Blue Team), inicie o processo de recolhimento de toda e quaisquer evidências, e identificação dos serviços afetados. Tais evidências serão utilizadas até a finalização do processo, para execução de análise forense do caso.

4.1.15.7.8. Deve-se reunir os dados coletados durante o processo de tratamento de incidente, para iniciar o processo de análise forense do mesmo, ainda pelo grupo de resposta a incidente de segurança (CSIRT – Blue Team). Tal análise deve ser realizada com o objetivo de identificar (pessoas, locais e/ou eventos), correlacionando todas as informações reunidas, e gerando como produto final um laudo sobre o incidente cibernético em questão.

4.1.15.7.9. Caso seja necessário a reconstrução do ataque, este deve ser realizado pela CONTRATADA em ambiente controlado, usando-se por exemplo de sandbox (mecanismo de segurança para separar programas em execução, geralmente utilizado em um esforço para mitigar falhas de sistema ou vulnerabilidades de segurança da informação). Tal ambiente deve ser de propriedade e controle da CONTRATADA.

4.1.15.7.10. O grupo de resposta a incidente de segurança (CSIRT – Blue Team) da CONTRATADA, deve documentar na ferramenta de ITSM, as lições aprendidas do incidente de segurança em questão, formando durante todo o período de vigência do contrato uma grande base de conhecimento sobre ataques adversos.

4.1.15.7.11. A contratada sempre deverá comunicar a área de segurança do Ministério as informações sobre os incidentes e quais as ações foram ou estão sendo tomadas para sua solução.

4.1.15.8. O serviço de tratamento e resposta aos incidentes cibernéticos - CSIRT - Blue Team serão responsáveis por monitorar equipamentos e softwares do CONTRATANTE, envolvendo identificação, classificação e análise de eventos que possam comprometer a disponibilidade, integridade e confidencialidade dos serviços;

4.1.15.9. A contratada deverá prover serviços de resposta aos incidentes de segurança da informação diante dos eventos registrados no monitoramento;

4.1.15.10. Os serviços de monitoramento e reposta a incidentes de segurança poderão ser prestados por meio de Centro de Operações de Segurança da Informação.

4.1.15.11. A CONTRATADA deverá buscar inteligência de proteção contra ataques cibernéticos e sendo responsável por:

4.1.15.11.1. Pesquisar novos tipos de ataques, vírus, malwares, botnets, vulnerabilidades e afins com intuito de melhoria contínua de detecção e mitigação destes males dentro da **Plataforma de SIEM/SOAR/NTA/UEBA/CTI do Ministério.**

4.1.15.11.2. Criar, em colaboração com a CONTRATANTE, casos de uso (regras) que devem ser implementados na **Plataforma de SIEM/SOAR/NTA/UEBA/CTI do Ministério.**

4.1.15.11.3. Revisar periodicamente as regras da **Plataforma de SIEM/SOAR/NTA/UEBA/CTI do Ministério**, realizando as adaptações e evoluções necessárias;

4.1.15.11.4. Produzir e entregar informação de inteligência acionável, na forma de procedimentos para triagem de alertas e procedimentos para resposta a incidentes, correspondentes às regras da **Plataforma de SIEM/SOAR/NTA/UEBA/CTI do Ministério**;

4.1.15.12. Atuar proativamente na antecipação e identificação de incidentes cibernéticos, antes mesmo do impacto nos serviços;

4.1.15.13. Reagir aos eventos de Segurança da Informação que possam afetar a disponibilidade, integridade ou confidencialidade das informações existentes nos sistemas ou serviços de TI do CONTRATANTE;

4.1.15.14. Atuar quando ocorrer a falha dos controles de segurança ou situação previamente desconhecida e que tenha probabilidade de comprometer os sistemas e serviços de TI.

4.1.15.15. Realizar e apresentar relatório de testes de vulnerabilidades de todo o ambiente tecnológico, conforme as práticas de Segurança da Informação;

4.1.15.16. Gerar e consolidar os relatórios analíticos de ataques e ou incidentes contendo dados, informações, indicadores e métricas que permitam avaliar a exposição do parque computacional do CONTRATANTE, contendo: hosts encontrados, topologia de rede, serviços, vulnerabilidade descobertas, nível de risco por plataforma e por vulnerabilidade, atualização de ativos sob sua administração, atualização de softwares (aplicação de patches e fix), sistemas de proteção, para apresentação ao CONTRATANTE, constando as medidas tomadas e sugestões;

4.1.15.17. Apresentar relatório das principais remediações para o tratamento das vulnerabilidades mais comuns, das vulnerabilidades mais críticas e dos exploits conhecidos, emitindo relatórios executivos, operacionais e de conformidade a norma NIST Cybersecurity Framework, Version 1.1 ou mais recente;

4.1.15.18. Monitorar e analisar os logs dos serviços de segurança (equipamentos, sistemas operacionais de servidores e clientes, conexões, programas utilizados etc.), propondo ações corretivas e de melhorias;

4.1.15.19. A CONTRATADA deverá, quando da inexistência de empresa responsável pela infraestrutura do CONTRATANTE ou, quando o risco de exploração for considerado alto e a empresa responsável pela infraestrutura não atuar de forma tempestiva, aplicar correções ou soluções de contorno que minimizem/corrijam as vulnerabilidades apontadas pelo Relatório “Teste de Invasão” a partir do final da “Reunião para apresentação do relatório de recomendações e descrição das atividades executadas durante o teste” de forma subsidiária, após autorização da área de segurança do CONTRATANTE.

4.1.15.20. A CONTRATADA deverá organizar a alocação de turnos e de profissionais de sua equipe.

4.1.15.21. A CONTRATADA será responsável por realizar os testes em todos os sistemas ou ativos informados neste Termo de Referência, assim como, nos que vierem a existir na infraestrutura do CONTRATANTE.

4.1.15.22. Eventos:

4.1.15.22.1. A participação em eventos de Segurança da Informação nacionais ou internacionais deverá ser uma prática adotada pelo prestador visando estar alinhado ao estado da arte em termos de segurança da informação, sendo sugerida a participação da CRS com a indicação do evento, período, local e custos, provendo à CRS todos os meios pelos quais possa pleitear internamente junto a DTIC a participação de sua equipe e, em caso de impossibilidade de participação da equipe da CRS, prover o repasse das informações obtidas no evento tão logo do regresso dos participantes.

4.1.15.22.2. A CONTRATADA deverá divulgar ao menos a cada 6 (seis) meses a listagem de eventos nacionais e internacionais de Segurança da Informação para que o Ministério possa programar a participação dos servidores da área de segurança da informação. Na listagem de eventos deverá constar o nome do evento, período, local e custos relacionados ao evento como material, inscrição e outros.

4.1.15.23. O CONTRATANTE, no curso da execução contratual, poderá demandar a CONTRATADA em temas relacionados a Segurançca da Informação e Comunição, visando auxiliar o CONTRATANTE no desempenho de suas atividades tais como, mas nao se limitando a estas: verificacao de conformidades no ambiente, confecção de relatórios, elaboração de documentos ou pareceres, avaliação de vulnerabilidades em aplicativos a serem instalados, especificação de requisitos de segurança para contratação de ativos ou serviços, auxiliar/avaliar na implantação de frameworks de segurança.

4.1.16. **Grupo 2: Item 3 e Item 4 - Serviço de Teste de Invasão - Red Team**

4.1.16.1. O **Red Team** atenderá sob demanda, tendo como objetivo principal **identificar, mapear e documentar possíveis vulnerabilidades nos sistemas, serviços, processos e ativos de infraestrutura tecnológica do Ministério**. Esses testes envolvem, necessariamente, o uso de técnicas e ferramentas específicas para tentar obter acesso não autorizado e privilegiado aos ativos e informações, bem como a indicação de soluções para a correção das vulnerabilidades encontradas, sem prejuízo aos níveis de serviços definido neste Termo de Referência.

4.1.16.1.1. Para o serviço foram estimados 827 alvos a serem utilizados, segundo interesse e necessidade do MJSP, ao longo dos 24 meses da vigência do contrato a ser estabelecido com a Contratada, conforme tabela 1 e 4. Dos sistemas existentes hoje, estima-se que o Ministério irá demandar, no mínimo, 83 alvos a cada 12 meses, sendo que desses pelo menos 20 serão de sistemas web;

4.1.16.1.2. Cada demanda solicitada poderá ter um ou mais alvos como objetivo de ataque;

4.1.16.1.3. A definição do que estão sendo considerados alvos neste TR encontra-se definido em subitem abaixo - 4.1.16.6;

4.1.16.1.4. Os serviços serão avaliados de acordo com a apresentação do "Relatório de Teste de Invasão" e com os níveis mínimos de serviços estabelecidos na tabela 11, definidos em itens posteriores neste TR.

4.1.16.2. Realizar tentativas de Data Exfiltration, Internal & External Reconnaissance, ShadowMap Scan, Vulnerability Assessment, Social Engineering, Exploitaion, Pivoting / Lateral Movements, entre outros, a rede e aos sistemas do ministério, obedecendo o framework de segurança MITRE ATT&CK que utiliza base global de conhecimento das táticas, técnicas e procedimentos (TTP's) utilizados por atacantes para avaliar a efetividade dos controles de segurança.

4.1.16.3. As equipes de ataque (RED TEAM) e defesa (BLUE TEAM) devem interagir e funcionar de maneira integrada. A equipe de RED TEAM deve compartilhar seu conhecimento no sentido de indicar soluções para vulnerabilidades encontradas e a equipe de BLUE TEAM deve possuir conhecimento das tácticas e técnicas de ataque para que, por meio da coordenação da CRS, aumente-se a efetividade da proteção do ambiente.

4.1.16.4. O Serviço de Testes de Invasão será do tipo externo e interno e terá como objetivo principal identificar, mapear, documentar, controlar e corrigir possíveis vulnerabilidades nos sistemas, processos e ativos de infraestrutura tecnológica. Os componentes da equipe responsável pela execução do serviço devem ter as qualificações que constam nos itens 4.12.13.4.1.1, 4.12.13.4.1.2 e 4.12.13.4.2. Para a realização dos testes de invasão deverão ser observadas as orientações e técnicas emanadas pelos padrões internacionais, além de outros apresentados pela CONTRATADA, caso haja em seu portfólio normativos que comprovadamente complementem os demonstrados abaixo:

4.1.16.4.1. OSSTMM 3 (The Open Source Security Testing Methodology Manual) ;

4.1.16.4.2. ISSAF/PTF (Information Systems Security Assessment Framework);

4.1.16.4.3. NIST Special Publication 800-115 (Technical Guide to Information Security Testing and Assessment);

4.1.16.4.4. NIST Special Publication 800-42 (Guideline on Network Security Testing);

4.1.16.4.5. NIST Special Publication 800-53 (Security and Privacy Controlsfor Information Systems and Organizations);

4.1.16.4.6. OWASP TESTING GUIDE 4.1 ou mais recente (The Open Web Application Security Project).

4.1.16.5. Neste documento os termos "pentest", teste de penetração, teste de intrusão e testes de invasão, são considerados sinônimos;

4.1.16.6. Alvos são todos os ativos de TIC envolvidos na sustentação e operação de um sistema ou serviço de TIC que vão desde a camada física até a camada de aplicação do modelo OSI (Open System Interconnection), bem como um grupo de pessoas/usuários finais e/ou usuários e administradores de TI e processos;

4.1.16.7. Os alvos dos "Testes de Invasão" bem como as premissas e condições para realização destes serão, necessariamente, definidos e aprovados através de demanda por parte do CONTRATANTE;

4.1.16.8. A Contratada deverá observar que os testes de invasão serão executados internamente (qualquer ponto da rede corporativa do CONTRATANTE) e externamente (através da Internet);

4.1.16.9. Todas as fases dos "Testes de Invasão" serão acompanhadas e supervisionadas a critério do CONTRATANTE;

4.1.16.10. Quaisquer atividades que possa comprometer ou prejudicar algum ambiente ou ativo deverá ser imediatamente reportada, antes de sua execução, haja vista a necessidade de manter a disponibilidade dos ambientes e serviços ativos;

4.1.16.11. O teste de invasão deverá obedecer às seguintes fases:

4.1.16.11.1. Planejamento;

4.1.16.11.2. Descoberta;

4.1.16.11.3. Ataque;

4.1.16.11.4. Relatório Teste de Invasão;

4.1.16.11.5. Reunião para apresentação do relatório de recomendações e descrição das atividades executadas durante o teste;

4.1.16.11.6. Realização de reavaliação como parte da demanda solicitada na OS, sem gerar custo adicional não sendo considerada nova demanda;

4.1.16.11.7. Relatório Final do Teste de Invasão.

4.1.16.12. Planejamento:

4.1.16.12.1. Todas as premissas, processos, atividades descritas e aprovadas na demanda, inclusive os cronogramas serão detalhados e apresentados na fase de planejamento;

4.1.16.12.2. Informações sobre o ambiente corporativo, utilizando-se das seguintes técnicas (podendo ser utilizadas ambas, conforme definição do escopo):

4.1.16.12.2.1. Técnica da caixa-preta (nenhum conhecimento sobre o ambiente a ser avaliado. O ambiente deverá ser descoberto pelo especialista) ;

4.1.16.12.2.2. Técnica da caixa branca (o avaliador tem acesso irrestrito a qualquer informação que possa ser relevante ao teste) ;

4.1.16.12.2.3. Técnica da caixa cinza ou híbrida (conhecimento parcial da estrutura interna do alvo).

4.1.16.13. Descoberta:

4.1.16.13.1. Deverá ser utilizada pela CONTRATADA ferramentas para análise de vulnerabilidades e gestão de vulnerabilidades devidamente licenciadas, incluídas ferramentas open source, além de técnicas manuais de análise de vulnerabilidade. As ferramentas deverão ser apresentadas a CONTRATANTE para ciência e aprovação antes de sua efetiva utilização, assim como a metodologia para análise manual de vulnerabilidades;

4.1.16.13.2. Na fase da DESCOBERTA deverão ser atendidos os seguintes quesitos e apresentado juntamente no “RELATÓRIO TESTE DE INVASÃO” (quando necessário):

4.1.16.13.2.1. Coleta passiva, onde deverá ser utilizada, no mínimo, as seguintes técnicas:

4.1.16.13.2.1.1. Whois e nslookup (consultas DNS) ;

4.1.16.13.2.1.2. Sites de busca;

4.1.16.13.2.1.3. Listas de discussão;

4.1.16.13.2.1.4. Blogs de colaboradores;

4.1.16.13.2.1.5. *Dumpster diving* ou *trashing*;

4.1.16.13.2.1.6. Informações livres;

4.1.16.13.2.1.7. Packet sniffing “passive eavesdropping”;

4.1.16.13.2.1.8. Captura de banner.

4.1.16.13.2.2. Coleta ativa, onde deverá ser utilizada, no mínimo, as seguintes técnicas:

4.1.16.13.2.2.1. Port scanning (Mapeamento de rede) ;

4.1.16.13.2.2.2. Varredura de vulnerabilidade.

4.1.16.13.2.3. A varredura de vulnerabilidade deverá verificar/identificar, entre outros:

4.1.16.13.2.3.1. Hosts ativos na rede;

4.1.16.13.2.3.2. Portas e serviços em execução;

4.1.16.13.2.3.3. Serviços ativos e vulneráveis nos hosts;

4.1.16.13.2.3.4. Sistemas operacionais;

4.1.16.13.2.3.5. Vulnerabilidades associadas com sistemas operacionais e aplicações descobertas;

4.1.16.13.2.3.6. Configurações feitas nos hosts sem observância de boas práticas em segurança computacional;

4.1.16.13.2.3.7. Identificação de rotas e estimativa de impacto, caso estas sejam modificadas/desconfiguradas;

4.1.16.13.2.3.8. Identificação de vetores de ataque e cenários para exploração;

4.1.16.13.2.3.9.Vulnerabilidades Detectadas (CVE);

4.1.16.13.2.3.10. Vulnerabilidades de Alto, Médio e Baixo Risco. Conforme o padrão *Common Vulnerability Scoring System* (CVSS) - https://www.first.org/cvss/v3.1/specification-document, item "*Qualitative Severity Rating Scale*";

4.1.16.13.2.3.11. Informações a serem aplicadas na fase de ataques;

4.1.16.13.2.4. Os serviços e aplicações web deverão verificar/identificar, entre outros:

4.1.16.13.2.4.1. Uso indevido de sistema de arquivos e arquivos temporários;

4.1.16.13.2.4.2. Evasão de informação por configurações default de tratamento de erros;

4.1.16.13.2.4.3. Tratamento indevido de entrada;

4.1.16.13.2.4.4. Problemas relacionados à má configuração dos serviços;

4.1.16.13.2.4.5. Gerenciamento inseguro de sessões web.

4.1.16.14. Ataque (exploração):

4.1.16.14.1. Quaisquer suspeita de comprometimento de algum ambiente ou ativo deverá ser imediatamente reportada, antes de sua execução, haja vista a necessidade de manter a disponibilidade dos ambientes e serviços ativos;

4.1.16.14.2. Deverá realizar testes de vulnerabilidades e invasão em endereços IP’s, URL´s, aplicações, ou outro ativo definido do ambiente computacional, composto por servidores, banco de dados, ativos de rede, ativos de segurança e outros equipamentos relacionados ao teste de invasão;

4.1.16.14.3. Deverão ser aplicados, no mínimo, os seguintes tipos de ataques:

4.1.16.14.3.1. Violações do protocolo HTTP;

4.1.16.14.3.2. SQL Injection;

4.1.16.14.3.3. LDAP Injection;

4.1.16.14.3.4. Cookie Tampering;

4.1.16.14.3.5. CrossSite

4.1.16.14.3.6. Scripting (XSS);

4.1.16.14.3.7. Directory Transversal;

4.1.16.14.3.8. Buffer Overflow;

4.1.16.14.3.9. OS Command Execution;

4.1.16.14.3.10. Command Injection;

4.1.16.14.3.11. Remote Code Inclusion;

4.1.16.14.3.12. Server Side Includes (SSI) Injection;

4.1.16.14.3.13. File disclosure;

4.1.16.14.3.14. Information Leak;

4.1.16.14.3.15. Zero day attacks;

4.1.16.14.3.16. Negação de serviço;

4.1.16.14.3.17. Contra protocolo TCP;

4.1.16.14.3.18. Ataques contra a aplicação.

4.1.16.14.4. Os ataques de negação de serviços, contra protocolo TCP e em nível da aplicação deverão, cada qual, explorar/demonstrar/utilizar as seguintes técnicas, entre outras:

4.1.16.14.4.1. Bugs em serviços, aplicativos e sistemas operacionais;

4.1.16.14.4.2. SYN flooding;

4.1.16.14.4.3. Fragmentação de pacotes de IP;

4.1.16.14.4.4. Smurf e fraggle;

4.1.16.14.4.5. Teardrop, nuke e land.

4.1.16.14.4.6. Para ataques contra o protocolo TCP.

4.1.16.14.4.6.1. Sequestro de conexões;

4.1.16.14.4.6.2. Prognóstico de número de sequência do protocolo TCP.

4.1.16.14.4.6.2.1. Ataque de Mitnick;

4.1.16.14.4.6.2.2. Source routing.

4.1.16.14.5. Para ataques em nível da aplicação:

4.1.16.14.5.1. Buffer Overflow;

4.1.16.14.5.2. Problemas com o SNMP;

4.1.16.14.5.3. Vírus, worms e cavalos de Tróia.

4.1.16.14.6. Injeção de Código:

4.1.16.14.6.1. Ataques XSS (Cross site Script) ;

4.1.16.14.6.2. Comprometimento do acesso remoto;

4.1.16.14.6.3. Manutenção de acesso;

4.1.16.14.6.4. Encobrimento de rastros da invasão.

4.1.16.14.7. Para este TR estão sendo considerados os seguintes conceitos em relação a Phishing.

4.1.16.14.7.1. Phishing é uma técnica de fraude online, utilizada por criminosos no mundo da informática para roubar senhas de banco e demais informações pessoais, usando-as de maneira fraudulenta Esta é uma forma de roubo de identidade que ocorre quando um site malicioso se faz passar por um legítimo, para induzi-lo a passar informações confidenciais, como senhas, dados de contas ou números de cartão de crédito. Seja conduzido por e-mail, redes sociais, SMS ou outro vetor, todos os ataques de phishing seguem os mesmos princípios básicos. O golpista envia um texto direcionado, com o objetivo de convencer a vítima a clicar em um link, baixar um anexo, enviar as informações solicitadas ou até mesmo concluir um pagamento real.

4.1.16.14.7.2. Phishing por e-mail: De longe, o método mais comum, o phishing por e-mail usa o e-mail para introduzir a isca de phishing. Esses e-mails geralmente contêm links que levam a sites maliciosos ou anexos que contêm malware.

4.1.16.14.7.3. Phishing nos sites: Os sites de phishing, também conhecidos como sites falsificados, são cópias falsas de sites reais conhecidos e confiáveis. Os hackers criam esses sites falsificados para fazer você inserir suas credenciais de login, que podem ser usadas para fazer login nas suas contas reais. Os pop-ups também são uma fonte comum de phishing nos sites.

4.1.16.14.7.4. Vishing: Abreviação de “phishing de voz”, vishing é a versão em áudio do phishing na internet. O golpista tentará convencer as vítimas por telefone a divulgar informações pessoais que podem ser usadas posteriormente para roubo de identidade. Muitas chamadas automatizadas são tentativas de vishing.

4.1.16.14.7.5. Smishing: Smishing é phishing via SMS. Você recebe uma mensagem de texto que solicita clicar em um link ou baixar um aplicativo. Mas, ao fazer isso, você baixará malware no seu telefone, que poderá roubar suas informações pessoais e enviá-las ao invasor.

4.1.16.14.7.6. Phishing nas redes sociais: Alguns invasores podem acessar contas de redes sociais e forçar as pessoas a enviarem links maliciosos para seus amigos. Outros criam perfis falsos e usam esses perfis para phishing.

4.1.16.14.7.7. Spear phishing: As campanhas de phishing em larga escala são como barcos de pesca industrial que arrastam redes enormes pelo oceano, tentando prender tudo que encontrar pelo caminho. Por outro lado, o spear phishing ocorre quando os phishers personalizam seus ataques para atingir indivíduos específicos. Redes sociais profissionais como o LinkedIn popularizaram o spear phishing para o crime cibernético corporativo, pois os hackers podem encontrar facilmente todas as suas informações de emprego em um só lugar;

4.1.16.14.7.8. Whaling: E para fechar o conjunto de metáforas náuticas, temos whaling (a caça às baleias), um ataque de phishing que visa um determinado indivíduo de alto valor. É o mesmo que spear phishing, mas com metas muito mais ambiciosas. Até os executivos seniores mais importantes estão propensos ao whaling;

4.1.16.14.7.9. Business E-mail Compromise (Fraude de CEO) ou golpe do Man-in-the-E-mail: Tipo de Phishing que envolvem malware e engenharia social ou técnicas de intrusão com o objetivo de extrair informações de pagamento, ou outras informações privilegiadas dos CEO de uma empresa ou outro executivo de alto escalão para a realização de transferências bancárias não autorizadas. As campanhas de fraude de CEO acompanham frequentemente ataques de whaling, pois o criminoso já obteve as credenciais de login do CEO.

4.1.16.14.7.10. Pharming: Explora a base de funcionamento da navegação na Internet realizando o envenenamento do servidor DNS.

4.1.16.14.7.11. Dropbox phishing e Google Docs phishing: Os serviços populares de nuvem são alvos atraentes de phishing. Os invasores ativam versões falsificadas das telas de login, roubam suas credenciais quando você as insere e depois têm acesso a todos os seus arquivos e dados.

4.1.16.14.7.12. Clone phishing: Os invasores podem pegar um e-mail legítimo e depois “cloná-lo”, enviando exatamente o mesmo e-mail para todos os destinatários anteriores com uma alteração crucial: os links foram substituídos pelos links maliciosos.

4.1.16.14.7.13. Manipulação de links: Ataque homográfico, ocorre quando o atacante cria uma página similar a original e envia um link, também semelhante ao original, para a vítima Quando os links são clicados, levam para o site criado pelo atacante. Os truques comuns incluem erros ortográficos propositais (por exemplo, “lado” x “Lado”; o segundo tem um *L* maiúsculo) ou escrever o nome de um site confiável como o texto de exibição do link.

4.1.16.14.7.14. Scripting entre sites: Phishers sofisticados podem explorar pontos fracos nos scripts de um site para sequestrar o site para seus próprios fins. Scripting entre sites é difícil de detectar, porque tudo no site parece ser legítimo, desde o endereço até os certificados de

segurança.

4.1.16.14.8. Com relação a Phishing, a contratada deverá realizar, dentre outros, os seguintes testes:

4.1.16.14.8.1. Phishing por e-mail;

4.1.16.14.8.2. Phishing nos sites;

4.1.16.14.8.3. Vishing;

4.1.16.14.8.4. Smishing;

4.1.16.14.8.5. Phishing nas redes sociais;

4.1.16.14.8.6. Spear phishing;

4.1.16.14.8.7. Dropbox phishing;

4.1.16.14.8.8. Google Docs phishing;

4.1.16.14.8.9. Whaling;

4.1.16.14.8.10. Spear phishing;

4.1.16.14.8.11. Whaling;

4.1.16.14.8.12. Fraude de CEO;

4.1.16.14.8.13. Pharming;

4.1.16.14.8.14. Clone phishing;

4.1.16.14.8.15. Manipulação de links;

4.1.16.14.8.16. Scripting entre sites.

4.1.16.14.9. Para testes de invasão direcionados, especificamente, aos serviços prestados via WEB, tanto Intranet quanto Internet, deverão ser observados e aplicados, os seguintes testes baseados na publicação OWASP TESTING GUIDE (The Open Web Application Security Project) mais recente. Os itens abaixo foram listados a partir do OWASP TESTING GUIDE 4.1:

4.1.16.14.9.1. Para testes de coleta de informações, aplicar padrão: WSTG-INFO-01 ao WSTG-INFO-10;

4.1.16.14.9.2. Para testes de gerenciamento de configuração e deploy, aplicar padrão: WSTG-CONF-01 ao WSTG-CONF-11;

4.1.16.14.9.3. Para testes de gerenciamento de identidades, aplicar padrão: WSTG-IDNT-01 ao WSTG-IDNT-05;

4.1.16.14.9.4. Para testes de autenticação, aplicar padrão: WSTG-ATHN-01 ao WSTG-ATHN-10;

4.1.16.14.9.5. Para testes de autorização, aplicar padrão: WSTG-ATHZ-01 ao WSTG-ATHZ-04;

4.1.16.14.9.6. Para testes de gerenciamento de sessão, aplicar padrão: WSTG-SESS-01 ao WSTG-SESS-08;

4.1.16.14.9.7. Para testes de Teste de validação de entrada, aplicar padrão: WSTG-INPV-01 ao WSTG-INPV-14;

4.1.16.14.9.8. Para testes de Manipulação de Erros, aplicar padrão: WSTG-ERRH-01 ao WSTG-ERRH-02;

4.1.16.14.9.9. Para testes de Criptografia, aplicar padrão: WSTG-CRYP-01 ao WSTG-CRYP-02;

4.1.16.14.9.10. Para testes de lógica de negócio, aplicar padrão: WSTG-BUSL-01 a WSTG-BUSL-09;

4.1.16.14.9.11. Para testes do lado do cliente (Client Side Testing), aplicar padrão: WSTG-CLNT-01 ao WSTG-CLNT-13;

4.1.16.14.9.12. Para testes não previstos no OWASP TESTING GUIDE 4.0 ou 4.1 (The Open Web Application Security Project) poderá ser utilizado o OWASP TESTING GUIDE 3.0 (The Open Web Application Security Project) naquilo que for complementar, visando sempre considerar o melhor resultado de análise.

4.1.16.14.10. Observa-se que o resultado de cada teste deverá vir acompanhado de relatórios contendo, pelo menos:

4.1.16.14.10.1. Referência-base (Whitepaper);

4.1.16.14.10.2. Ameaças encontradas;

4.1.16.14.10.3. Riscos levantados ao ambiente computacional;

4.1.16.14.10.4. Contramedidas para mitigar as ameaças encontradas.

4.1.16.15. Relatório de Teste de Invasão:

4.1.16.15.1. Deverá ser elaborado em língua portuguesa obedecendo a norma culta padrão e entregue ao CONTRATANTE após a fase de ataque, o relatório “RELATÓRIO TESTE DE INVASÃO” para cada teste que será realizado, contemplando no mínimo informações, tais como:

4.1.16.15.1.1. Objetivos, premissas e escopo do teste, datas e horas dos testes, metodologia de análise de vulnerabilidades, descrição das ações realizadas, metodologias, vulnerabilidades encontradas, categorização e severidade das vulnerabilidades, possíveis problemas aplicáveis, recomendações e controles de segurança necessários para correção das vulnerabilidades, apresentação das evidências apuradas, fontes de pesquisa, referências e ferramentas utilizadas, informações acessadas e demais evidências do sucesso da invasão.

4.1.16.15.2. Após a fase de ataque, deverão ser atendidas e apresentadas no Relatório, no mínimo, as seguintes informações detalhadas:

4.1.16.15.2.1. Detalhes da infraestrutura descoberta, alvo dos testes de invasão;

4.1.16.15.2.2. Equipamentos e recursos demandados para este teste;

4.1.16.15.2.3. Tipos de ataque;

4.1.16.15.2.4. Prazos (janelas de tempo para execução dos testes);

4.1.16.15.2.5. Pontos de contato da contratada (responsáveis para tratamento de questões abordadas nos testes);

4.1.16.15.2.6. Tipos de testes realizados pelos especialistas em segurança da informação;

4.1.16.15.2.7. Confirmação ou refutação da existência de vulnerabilidades;

4.1.16.15.2.8. Documentação sobre o caminho utilizado para exploração, avaliação do impacto e prova da existência da vulnerabilidade;

4.1.16.15.2.9. Obtenção de acesso e possível escalada de privilégios;

4.1.16.15.2.10. Detalhamento da metodologia do ataque;

4.1.16.15.2.11. Recomendações para sanar riscos e vulnerabilidades.

4.1.16.15.3. Como critério de conformidade, os subitens dos itens 4.1.16.15.1 e 4.1.16.15.2 do item 4.1.16.15 Relatório de Teste de Invasão serão considerados como parâmetros para aceitação.

4.1.16.16. Reunião para apresentação do relatório de recomendações e descrição das atividades executadas durante o teste;

4.1.16.16.1. Será realizada reunião conduzida pela Contratada, onde será apresentado de forma detalhada todo o conteúdo do "Relatório Teste de Invasão", onde serão sanadas todas as dúvidas do corpo técnico do CONTRATANTE.

4.1.16.17. Relatório Final do Teste de Invasão:

4.1.16.17.1. Após a entrega do "RELATÓRIO DE TESTE DE INVASÃO", o CONTRATANTE analisará o documento para aplicar as recomendações, remediar os riscos ou mesmo assumi-los.

4.1.16.17.2. Após essa análise e aplicadas medidas de remediação, o CONTRATANTE poderá solicitar à CONTRATADA que refaça o teste de invasão para aferição dos resultados com emissão de novo relatório, sem custo adicional para a CONTRATANTE.

4.1.16.17.3. Identificadas inconformidades no relatório, a ordem de serviço será passível de glosa conforme Tabela 11 e a CONTRATADA deverá providenciar as devidas correções no prazo acordado com a CONTRATANTE.

4.1.16.18. Atividades de Apoio, dos testes de invasão:

4.1.16.18.1. Para auxílio das atividades poderão, a critério do CONTRATANTE, serem solicitados à CONTRATADA os seguintes documentos de apoio:

4.1.16.18.1.1. PLANO DE TRABALHO com o detalhamento do escopo dos testes e cronograma de execução;

4.1.16.18.1.2. APRESENTAÇÃO INICIAL das ações a serem aplicadas pela Contratada;

4.1.16.18.1.3. RELATÓRIOS DE ACOMPANHAMENTO SEMANAIS do plano de trabalho.

4.1.16.19. Periodicidade de execução dos testes de invasão:

4.1.16.19.1. A CONTRATADA deverá realizar os Testes de Invasão conforme a quantidade definida em Ordem de Serviço (OS);

4.1.16.19.2. O prazo para conclusão de cada Ordem de Serviço (OS), incluindo, diagnósticos, análises, avaliações e testes com fornecimento de todos os relatórios específicos de avaliação de vulnerabilidades, dos ambientes relacionados neste Termo de Referência, será definido de acordo com cada atividade, sendo divididas em:

4.1.16.19.2.1. Atividades do Pentest;

4.1.16.19.2.2. Entrega do relatório "Teste de Invasão";

4.1.16.19.2.3. Ações corretivas das vulnerabilidades apontadas pela CONTRATADA e aplicadas pelo CONTRATANTE;

4.1.16.19.2.4. Reavaliação do Pentest pós remediação, quando necessário, e a realização dessa atividade não condicionará o atesto do serviço prestado pela Ordem de Serviço que originou, onde a realização ação corretiva não dependa exclusivamente do Ministério;

4.1.16.19.2.5. Entrega do relatório "Relatório Final do Teste de Invasão".

4.1.16.20. A CONTRATADA deverá informar à CONTRATANTE da lista das correções ou soluções de contorno que minimizem/corrijam as vulnerabilidades apontadas pelo Relatório "Teste de Invasão" a partir do final da "Reunião para apresentação do relatório de recomendações e descrição das atividades executadas durante o teste".

4.2. ***Requisitos de Capacitação***

4.2.1. Para os itens 1, 2 e 3 não se aplicam os requisitos de capacitação, uma vez que trata-se de uma contratação para prestação de serviços de TI, destinados à proteção dos equipamentos e estações de trabalho, sistemas e ativos de rede do Ministério da Justiça e Segurança Pública.

4.3. ***Requisitos Legais***

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

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

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

4.3.2.2. Lei Nº 12.682, de 9 de julho de 2012, dispõe sobre a elaboração e o arquivamento de documentos em meios eletromagnéticos;

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

4.3.2.4. Decreto Nº 10.222, de 05 de fevereiro de 2022, que aprova a Estratégia Nacional de Segurança Cibernética.

4.3.2.5. Decreto Nº - 8.789, de 29 de junho de 2016, dispõe sobre o compartilhamento de bases de dados na administração pública federal;

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

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

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

4.3.2.9. Instrução Normativa Nº 4, 12 de abril de 2012, institui a Infraestrutura Nacional de Dados Abertos – INDA;

4.3.2.10. Instrução Normativa Nº 1, da SGD/ME, de 4 de abril de 2019, que dispõe sobre o processo de contratação de soluções de Tecnologia da Informação e Comunicação - TIC pelos órgãos e entidades integrantes do Sistema de Administração dos Recursos de Tecnologia da Informação - SISP do Poder Executivo Federal;

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

4.3.2.12. Decreto Nº 10.748, de 16 de julho de 2021, institui a Rede Federal de Gestão de Incidentes Cibernéticos.

4.3.2.13. Adotar programa de integridade conforme portaria 513 do Ministério da justiça SEI (13669505).

4.4. ***Requisitos de Manutenção***

4.4.1. 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.

4.4.2. 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.

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

4.4.4. Cada novo release, versão de firmware, atualização de produtos que sejam relacionados aos itens do objeto deverá ser disponibilizada pela CONTRATADA sem ônus adicional.

4.4.5. 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. Todos os serviços serão prestados esperando-se a aplicação das melhores práticas e recomendações do mercado e do Fabricante.

4.4.6. 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.

4.4.7. Os chamados técnicos somente deverão ser encerrados após expressa anuência do Gestor do Contrato ou do Fiscal Técnico.

4.4.8. Caso o técnico da CONTRATADA enseje dano irreparável a equipamento (s), ou sistema (s) ou dado (s) do Ministério da Justiça e Segurança Pública, por conta de conduta antiprofissional, erro ou quaisquer outros motivos fica a CONTRATADA obrigada a realizar a troca por equipamento igual ou superior ao que foi danificado ou normalização do sistema afetado.

4.4.9. 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.

4.5. ***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 2 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 o item 3 e Item 4 a CONTRATADA deverá atender às ordens de serviço emitidas, de acordo com o item Níveis Mínimos de Serviços Exigidos neste Termo de Referência.

4.6. ***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.

4.8. ***Requisitos de Arquitetura Tecnológica***

4.8.1. A CONTRATADA deverá disponibilizar ao Ministério da Justiça e Segurança Pública Arquitetura Tecnológica implementada para a prestação dos serviço atualizada e compatível com as necessidades do Ministério da Justiça e Segurança Pública.

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

4.9.1. A CONTRATADA deverá disponibilizar ao Ministério da Justiça e Segurança Pública documentação onde constem as especificações técnicas detalhadas dos produtos ofertados.

4.9.2. Deverá disponibilizar ainda os requisitos de projeto e de implementação, incluindo a descrição dos padrões dos serviços e método de gestão relacionados na seção "Descrição da Solução de TIC" e seção "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, a CONTRATADA, no que couber, será responsável pela implantação/disponibilização da solução contratada. Outrossim, quando aplicável, a disponibilização das licenças demandadas deve ser feita de acordo com os prazos definidos no item "Requisitos Temporais" deste Termo de Referência.

4.11. ***Requisitos de Garantia Contratual***

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

4.11.2. 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.

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

4.11.4. 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.

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

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

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

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

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

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

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

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

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

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

4.11.11. 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.

4.11.12. 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.

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

4.11.14. Será considerada extinta a garantia:

4.11.14.1. 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;

4.11.14.2. 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.

4.11.15. 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.

4.11.16. 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 Perfis e Experiência Profissional***

4.12.1. Para que haja garantia de qualidade no serviço executado e modernização das metodologias de Gestão de Risco e Segurança da Informação, a CONTRATADA deverá manter profissionais qualificados nas áreas funcionais, que deverão ser gerenciados exclusivamente pelo representante técnico da empresa CONTRATADA, de forma que o CONTRATANTE possa obter o menor tempo de resposta para quaisquer incidentes ocorridos no seu ambiente de Infraestrutura tecnológica, bem como alcançar a excelência no serviço de TI;

4.12.2. Esses recursos humanos deverão conhecer o funcionamento dos negócios internos da DTIC e demais áreas do Ministério, bem com executar os procedimentos de acordo com as regras de segurança;

4.12.3. As equipes deverão ser dimensionadas pela empresa CONTRATADA de forma a atender as demandas de acordo com os níveis mínimos de serviço exigidos estabelecidos. Para tanto, salienta-se que essa responsabilidade de formação da equipe de profissionais é exclusiva da empresa CONTRATADA;

4.12.4. Será de responsabilidade da CONTRATADA o cumprimento da legislação específica dos profissionais que prestarão o serviço à CONTRATANTE;

4.12.5. Os profissionais deverão utilizar vestimenta compatível com a utilizada pelos servidores do MJSP e portar crachá de identificação durante toda a prestação de serviço, **quando de atuação presencial nas dependências do MJSP;**

4.12.6. A CONTRATADA será responsável por qualquer deslocamento dos profissionais relacionados a execução do presente contrato. O tempo de deslocamentos não poderão ser utilizado para justificar o descumprimento dos ***Níveis Mínimos de Serviço Exigidos;***

4.12.7. Durante a execução dos serviços, a CONTRATADA deverá disponibilizar os profissionais com as qualificações especificadas neste Termo de Referência. As certificações devem estar ativas/válidas. As competências descritas podem estar presentes em diversos profissionais, cabendo a CONTRATADA manter o número adequado de prestadores para cada atividade, respeitando apenas o quantitativo mínimo porém não se limitando a ele;

4.12.8. **A CONTRATADA terá um prazo de 90 dias para se adequar aos requisitos exigidos de certificações de seus profissionais**, prazo esse que se inicia **a partir da data da reunião inicial após a assinatura contratual** e o mesmo pode ser renovado uma única vez por mais 90 dias, desde de que a CONTRATADA apresente justificativa a CONTRATANTE;

4.12.9. Durante a vigência contratual e a qualquer tempo, os profissionais da CONTRATADA serão avaliados pela CONTRATANTE, a qual poderá solicitar a substituição destes, caso não estejam correspondendo às necessidades e requisitos para cada perfil. Esta substituição deverá ocorrer em até 15 quinze dias, contados a partir da notificação por parte da CONTRATANTE;

4.12.10. Serão aceitos como documentos válidos para comprovação de qualificação técnica os documentos citados pela legislação trabalhista, tais como: Carteira de Trabalho e Previdência Social, Contrato de Trabalho, Recibo de Pagamento de Trabalhador Autônomo, Sócio, Diretor. Quando a descrição contida nestes documentos não for suficiente para a comprovação da experiência exigida, estes poderão ser complementados com atestado(s) ou declaração(ões), descrevendo as atividades realizadas pelo profissional, expedido(s) por pessoa jurídica de direito público ou privado;

4.12.11. Para a qualificação em conhecimentos exigidos para a execução dos serviços serão aceitos certificados de participação em cursos e/ou certificações emitidas por instituições certificadoras especializadas;

4.12.12. Todos os profissionais que compõem a equipe devem possuir residência física e fixa em território nacional e prestar os seus serviços em instalações sediadas no país;

4.12.13. Durante a execução deste serviço a CONTRATADA deverá disponibilizar os profissionais com as qualificações abaixo especificadas:

4.12.13.1. Formação: Nível Superior completo em uma das seguintes áreas: Análise de Sistemas, Ciência da Computação, Processamento de Dados, Sistemas de Informação, Informática, Engenharia da Computação, Segurança da Informação ou curso superior completo em qualquer área e especialização, com no mínimo 360 horas, na área de segurança da informação.

4.12.13.2. **Serviço de Security Operations Center - SOC:**

4.12.13.2.1. **Certificações** para a função de **Analista(s) SOC**:

4.12.13.2.1.1. AZ-500: Microsoft Azure Security Technologies (Microsoft) - Pelo menos um profissional

4.12.13.2.1.2. CompTIA Security+ (CompTIA) - Pelo menos um profissional;

4.12.13.2.1.3. Fortinet Network Security Expert 4 – NSE4 (Fortinet)- Pelo menos um profissional;

4.12.13.2.1.4. Certificação ITILv3 Foundation ou superior - Pelo menos um profissional.

4.12.13.2.2. **Experiência profissional** para a função de **Analista(s) SOC**:

4.12.13.2.2.1. Experiência mínima de 4 (quatro) anos em utilização de analisadores de protocolo para realização de troubleshooting em plataformas SIEM;

4.12.13.2.2.2. Experiência mínima de 2 (dois) anos em implantação, administração e gerência de centralizador de logs;

4.12.13.2.2.3. Experiência mínima de 2 (dois) anos em administração de sistemas operacionais Linux;

4.12.13.2.2.4. Experiência mínima de 2 (dois) anos em administração de sistemas operacionais Windows Server 2012 ou superior;

4.12.13.2.2.5. Experiência mínima de 2 (dois) anos em analise forense, como analise logs, correlacionamento de eventos, resposta a incidentes de segurança da informação (cibernética);

4.12.13.3. **Serviço de Tratamento e Resposta aos Incidentes Cibernéticos - CSIRT - Blue Team:**

4.12.13.3.1. **Certificações** para a função de **Especialista(s) Blue Team**:

4.12.13.3.1.1. AZ-500: Microsoft Azure Security Technologies (Microsoft)- Ao menos um profissional

4.12.13.3.1.2. Certified Information Systems Security Professional - CISSP (ISC^2) ou Certified Cloud Security Professional - CCSP (ISC^2) - Pelo menos um profissional;

4.12.13.3.1.3. CompTIA Cibersecurity Analyst - CySA+ (CompTIA) - Pelo menos um profissional;

4.12.13.3.1.4. Certified Ethical Hacker - CEH (EC-Council) - Pelo menos um profissional;

4.12.13.3.1.5. CERTIFIED NETWORK DEFENDER - CND (EC-Council) - Pelo menos um profissional;

4.12.13.3.1.6. Fortinet Network Security Expert 4 – NSE4 (Fortinet) - Pelo menos um profissional;

4.12.13.3.1.7. FortiWeb Specialist Exam (fortinet) - Pelo menos um profissional;

4.12.13.3.1.8. Certificação ITILv3 Foundation ou superior - Pelo menos um profissional.

4.12.13.3.2. **Experiência profissional** para a função de **Especialista(s) Blue Team**:

4.12.13.3.2.1. Experiência mínima de 8 (oito) anos em utilização de analisadores de protocolo para realização de troubleshooting em plataformas de SIEM;

4.12.13.3.2.2. Experiência mínima de 8 (oito) anos em implantação, administração e gerência de centralizador de logs;

4.12.13.3.2.3. Experiência mínima de 8 (oito) anos em administração de sistemas operacionais Linux e Windows Server 2012 ou superior;

4.12.13.3.2.4. Experiência mínima de 4 (quatro) anos em atividades de **Tratamento e Resposta aos Incidentes Cibernéticos Blue Team**;

4.12.13.3.2.5. Experiência mínima de 4 (quatro) anos em analise forense, como analise de logs, correlacionamento de eventos, resposta a incidentes de segurança da informação (cibernética);

4.12.13.4. **Serviço de Teste de Invasão - Red Team:**

4.12.13.4.1. **Certificações** para a função de **Especialista(s) Red Team**:

4.12.13.4.1.1. Licensed Penetration Tester - LPT (EC-Council), Certified Penetration Testing Professional - CPENT (EC-Council), Certified Expert Penetration Tester – CEPT (IACRB), Exploit Researcher and Advanced Penetration Tester – GXPN (GIAC) ou Offensive Security Certified Professional - OSCP (Offensive Security) - Ao menos um profissional;

4.12.13.4.1.2. Certified Ethical Hacker - CEH (EC-Council) - Pelo menos um profissional;

4.12.13.4.1.3. Certificação ITILv3 Foundation ou superior - Pelo menos um profissional.

4.12.13.4.2. **Experiência profissional** para a função de **Especialista(s) Red Team:**

4.12.13.4.2.1. Experiência mínima de 8 (oito) anos em administração de sistemas operacionais Linux e Windows Server 2012 ou superior;

4.12.13.4.2.2. Experiência mínima de 4 (quatro) anos em atividades de **Teste de Invasão - Red Team**;

4.12.14. A comprovação dos requisitos deverá ser composta de:

4.12.14.1. Documento digitalizado com apresentação de documento original válido ou ativa, cópia autenticada ou documento digital em que seja possível comprovar a autenticidade em site do emissor.

4.12.14.2. Experiência deverá ser comprovada através da carteira de trabalho, atestado de capacidade ou documentos formais e oficiais emitidos por terceiros que contrataram o serviço realizado pelo profissional, não sendo aceito currículo vitae ou informações de rede sociais;

4.12.14.3. Todos os documentos apresentados estarão sujeitos à diligência do CONTRATANTE para fins de confirmação das informações prestadas;

4.12.14.4. A **CONTRATADA deverá promover**, no prazo máximo de 90 dias, **a atualização das certificações de seus profissionais** caso haja expiração, atualização de versão ou migração para uma nova solução de TI devido a modernização do ambiente tecnológico do CONTRATANTE. Este prazo se iniciará a partir da comunicação formal do CONTRATANTE.

4.12.14.4.1. Caso uma certificação não seja mais válida, será aceita a nova certificação que substituiu a anterior.

4.12.15. Não existe restrição ou limite para acumulo de perfis em um mesmo profissional, uma vez que é de responsabilidade da CONTRATADA definir o quantitativo de profissionais envolvidos para cada serviço, porém, este(s) deve(m) compor única e exclusivamente a equipe ao qual foi apresentado em atendimento ao requisito da respectiva certificação.

4.13. ***Requisitos de Formação da Equipe***

4.13.1. A CONTRATADA deverá formar uma equipe com atributos de alta performance: participação; responsabilidade dos membros pelos resultados; clareza de objetivos; existência de um clima aberto e confiável entre os membros da equipe; flexibilidade; focalização; criatividade e ação rápida sobre problemas e oportunidades. Além das certificações necessárias conforme cada serviço.

4.14. ***Requisitos de Metodologia de Trabalho***

4.14.1. A CONTRATADA deverá nomear preposto para atuar como ponto de contato do CONTRATANTE em relação ao eventual descumprimento dos termos de serviço, exceto para assuntos de caráter técnico.

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

4.14.3. 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;

4.14.4. 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;

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

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

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 ou quaisquer outro tipo de informação ou dado obtido por conta da contratação.

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

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

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

4.15.5. A CONTRATADA deverá atender à legislação, principalmente à Instrução Normativa GSI/PR nº 01, de 13.06.2008, do Gabinete de Segurança Institucional da Presidência da República, a qual disciplina a gestão de segurança da Informação e Comunicações na Administração Pública Federal, bem como ao Decreto nº 3505, de 13 de junho de 2000, que institui a Política de Segurança da Informação nos órgãos e entidades da Administração Pública Federal.

4.15.6. A CONTRATANTE garantirá acesso a todos os logs e mecanismos de auditoria para a CONTRATADA, quando solicitado e previamente justificado;

4.15.7. 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:

4.15.7.1. Garantia de foro brasileiro;

4.15.7.2. Garantia de aplicabilidade da legislação brasileira;

4.15.7.3. 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;

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

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

4.15.7.6. 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;

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

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

4.15.8. Eventos e incidentes cibernéticos devem ser comunicados através de canais predefinidos de comunicação, disponibilizados pela CONTRATADA/FABRICANTE, de maneira rápida e eficiente e de acordo com os requisitos legais, regulatórios e contratuais.

4.15.9. Para os itens 1, 2 e 3 da Tabela 1, a CONTRATADA/FABRICANTE deverá oferecer, no mínimo:

4.15.9.1. Acesso ao centro de conformidade de segurança, um console baseado na Web para gerenciar funções relacionadas à segurança e conformidade, como prevenção de perda de dados, descoberta eletrônica e retenção;

4.15.9.2. Permitir o gerenciamento de ameaças, como filtragem de mensagens e anti-malware;

4.15.9.3. Permitir gerenciar o ciclo de vida do conteúdo gerado, por meio de configuração de mecanismos de importação de massa, de arquivamento e do uso de políticas de retenção de conteúdo, além de mecanismos de monitoramento dos dados, gerenciamento de caixas de correio inativas e gerenciamento de registros;

4.16. **Outros Requisitos Aplicáveis**

4.16.1. ***Requisitos de 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 e-mail: 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. ***Subcontratação***

4.16.2.1. 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;

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;

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

5.1.10. 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.

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

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

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

5.1.14. Disponibilizar as instalações com espaço físico, o mobiliário e as estações de trabalho necessárias à execução dos serviços nas dependências do Ministério.

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. 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.

5.2.18. 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.

5.2.19. 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.

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

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

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

5.2.23. 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.

5.2.24. 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.

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

5.2.26. 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.

5.2.27. 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 contatar os responsáveis (Importante esclarecer que os contatos principais ainda serão os comerciais, e que tais números serão utilizados apenas para os casos de emergência).

5.2.28. 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.

5.2.29. 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.

5.2.30. 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;

5.2.31. 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.

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

5.2.33. 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;

5.2.34. 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;

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

5.2.36. 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;

5.2.37. 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;

5.2.38. 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:

5.2.38.1. 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;

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

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

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

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

5.2.38.6. 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;

5.2.38.7. 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;

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

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

5.2.38.10. 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

5.2.39. A Contratada deverá apresentar, para aprovação da Contratante, no prazo máximo de 15 dias corridos, contados a partir da assinatura do contrato, Plano de Implantação dos Serviços, contendo cronograma detalhado de atividades a serem executadas pela Contratada.

5.2.40. Plano de Implantação deve conter, no mínimo, as seguintes informações: cronograma detalhado ao nível de atividades a serem desenvolvidas para a implantação de todos os serviços previstos no Termo de Referência; identificação de ferramentas e modelos a serem utilizados; configurações a serem realizadas; impactos e riscos, além do pessoal envolvido na execução dos serviços.

5.2.41. A Contratada deverá detalhar e repassar, conforme orientação e interesse do Ministério, todo o conhecimento técnico utilizado na implementação dos serviços, sem prejuízo da devida atualização da base de conhecimento ao longo de toda a execução.

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 dos serviços;

6.1.1.1.6. Alinhar prazo e informações que devem conter no relatório de diagnóstico inicial a ser realizado pela Contratada. O diagnóstico inicial das vulnerabilidades existentes deve conter relatório detalhado, inclusive, com procedimentos de correção/mitigação, a ser entregue à Contratante e deverá ser realizado no prazo máximo de 15 dias a contar da data de início prevista na Ordem de Serviço.

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, estes 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 Referência 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 Referência 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 ele 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.

6.1.1.6.6. A CONTRATADA deverá, num prazo de até 5 (cinco) dias úteis, a partir da assinatura do contrato, 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 2: será emitida uma ordem de serviço com as licenças relacionadas.

6.1.2.2. Item 3 e 4: 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.

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 CONTRATADA deverá considerar o horário de 8 horas às 19 horas como de horário normal de expediente do Ministério, para os dias úteis.

6.1.4.2. Deve ser possível a comunicação com o preposto fora do horário de atendimento. No caso de haver profissional da CONTRATADA prestando serviço para o MJSP em horários não úteis, também deverá ser designado preposto, que poderá ser acionado, ainda que remotamente, para receber determinações ou tratar questões, incidentes e problemas que sejam inadiáveis, a critério do MJSP.

6.1.4.3. A CONTRATADA deverá disponibilizar números de celular e escala do(s)profissional(ais) que responderão pelo papel de preposto(s).

6.1.4.4. A CONTRATADA deverá fornecer números telefônicos ou outros meios de comunicação para contato com o preposto, os supervisores e seu substitutos, mesmo fora do horário de expediente, sem que com isso ocorra qualquer ônus extra para o CONTRATANTE.

6.1.4.5. As atividades referentes aos itens 1, 2 e 3 deverão estar disponíveis para o CONTRATANTE, no regime 24/7/365 (todos os dias do ano em horário integral, de forma ininterrupta). Nos casos de ocorrências de incidentes e problemas graves, será exigida a presença dos colaboradores e do supervisor desta área na “Sala de Crise” da CONTRATANTE. Todos os níveis mínimos de serviço especificados neste documento deverão ser atendidos, independentemente do momento de abertura do chamado.

6.1.4.6. A sala de crise, é uma estrutura organizacional que visa resolver um problema pontual e urgente. A sala de crise poderá ser composta por pessoas de diversas empresas, a fim de colaborar com a resolução do eventual problema. A participação em uma sala de crise não deverá gerar ônus ao Ministério.

6.1.4.7. A tabela 8 apresenta a Forma de prestação de Serviço e os horários que os serviços devem ser prestados.

Tabela 8 - Forma de prestação de serviços e horário

Grupo	Item	Processo ITIL	Forma de Prestação do Serviço	Horário
1	1. Serviço de Security Operations Center - SOC 2. Serviço de Tratamento e Resposta aos Incidentes Cibernéticos - CSIRT - Blue Team	Gerenciamento de Eventos Gerenciamento de Acesso Central de Serviços Gerenciamento de operações de TIC (Controle de Operações de Segurança da	A forma de prestação dos serviços poderá ser presencial ou remota, conforme a necessidade do serviço, devendo ser acordado entre as partes, de maneira a garantir os níveis mínimos de serviços estabelecidos no presente instrumento.	De 0h00 ás 23h59 de segunda a domingo (24x7)

		Informação)		
		Gerenciamento Técnico	A forma de prestação dos serviços poderá ser presencial ou remota, conforme a necessidade do serviço, devendo ser acordado entre as partes, de maneira a garantir os níveis mínimos de serviços estabelecidos no presente instrumento.	De 19h00 às 07h00 de segunda a sexta (12x5) e de 0h00 ás 23h59 sábado e domingo (24x7)
		Gerenciamento de Aplicação		
		Gerenciamento de Continuidade de Negócio		
		Gerenciamento de Incidentes		
		Gerenciamento de Problemas		
		Gerenciamento de Mudança		
		Gerenciamento de Liberação e Implantação	A forma de prestação dos serviços poderá ser presencial ou remota, conforme a necessidade do serviço, devendo ser acordado entre as partes, de maneira a garantir os níveis mínimos de serviços estabelecidos no presente instrumento.	De 7h00 às 19h00 de segunda a sexta (12x5)
		Gerenciamento de Configuração e de Ativos de Serviços		
		Gerenciamento de Requisições		
		Gerenciamento de Conhecimento		
2	3. Serviço de Teste de Invasão - Red Team: Sistemas Web 4. Serviço de Teste de Invasão - Red Team: Infraestrrutura	Central de Serviços	A forma de prestação dos serviços poderá ser presencial ou remota, conforme a necessidade do serviço, devendo ser acordado entre as partes, de maneira a garantir os níveis mínimos de serviços estabelecidos no presente instrumento.	De 7h00 às 19h00 de segunda a sexta (12x5)
		Gerenciamento de Incidentes		
		Gerenciamento de Problemas		
		Gerenciamento de Requisições		
		Gerenciamento de Conhecimento		

6.1.4.8. Para fins de execução do contrato, a CONTRATADA deverá atender os requisitos técnicos especificados deste Termo de Referência e seus anexos. Todos os processos poderão ser amadurecidos conforme evolução da operação no ambiente de infraestrutura durante a execução do contrato.

6.1.4.9. As atividades de mudança, implantação ou publicação de novos serviços deverão ser realizadas em conformidade com os horários e períodos programados pela CONTRATANTE, onde estima-se que até 20% (vinte por cento) das solicitações abertas através de chamados poderão ser realizadas em horários noturnos e em dias não úteis, sem que haja qualquer ônus adicional para a CONTRATANTE.

6.1.4.10. Os atendimentos a chamados e a incidentes deverão observar os Níveis de Serviços dispostos no Níveis Mínimos de Serviço Exigidos, de forma que os incidentes que ocorrerem fora do expediente deverão ser atendidos remota ou presencialmente de forma a cumprir os níveis de serviços acordados.

6.1.4.11. Poderá haver trabalho noturno, nos finais de semana ou feriados, havendo fato que o justifique, tais como manutenções programadas, antecipação de prazos de entrega por parte do usuário, deslocamento de prestadores nos finais de semana, implementação de rotinas que necessitem de paralisação dos serviços disponibilizados aos usuários, análise de incidentes críticos, entre outros. Estes serviços extraordinários não implicarão em nenhuma forma de acréscimo ou majoração nos valores dos serviços, razão pela qual será improcedente a reivindicação à CONTRANTANTE de restabelecimento de equilíbrio econômico-financeiro, bem como, cobranças de horas-extras ou adicionais noturnos.

6.1.5. ***Locais de entrega***

6.1.5.1. O fornecimento dos serviços serão executados, quando realizados na modalidade presencial, no local apresentado na tabela 9.

Tabela 9 - Local de prestação de serviços

ÓRGÃO LICITANTE: MINISTÉRIO DA JUSTIÇA E SEGURANÇA PÚBLICA	
LOCALIZAÇÃO	**ENDEREÇO**
SEDE	Esplanada dos Ministérios, Palácio da Justiça, Bloco T, Edifício sede – CEP: 70064900 E-mail: crs@mj.gov.br Contato: Ivanildo de Oliveira da Silva JR

6.1.5.2. 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).

6.1.5.3. Os locais abrangidos por este contrato devem considerar as localidades remotas, na qual exista um prolongamento da rede do MJSP, tais como CICCN e penitenciárias federais ligadas ao núcleo central do MJSP, conforme especificado no estudo técnico preliminar (SEI 14628351), planilha de informações (SEI 15783908) e relatório (SEI 14628328).

6.1.6. ***Papéis e responsabilidades por parte da contratante e da contratada***

6.1.6.1. 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.

6.1.6.2. 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.

6.1.6.3. 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).

6.1.6.4. 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.

6.1.6.5. 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.

6.1.6.6. 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.

6.1.7. 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.

6.1.7.1. 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:

6.1.7.1.1. **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.

6.1.7.1.2. **Fiscal(is) Administrativo(s):**

a) Verificar aderência aos termos contratuais;

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

6.1.7.1.3. **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.

6.1.7.1.4. **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.

6.1.7.1.5. **Preposto(s):**

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 e deverá manter-se constante até a finalização do contrato.

6.1.8.2. Realização de transferência de conhecimento para equipe técnica da Área de Tecnologia da Informação e Comunicação do Ministério da Justiça e Segurança Pública em todas as tecnologias instaladas e/ou utilizadas, sistemas, produtos e soluções disponibilizada pela CONTRATADA com o fornecimento de perfil de acesso para a supervisão dos serviços prestados, assim como, atualização rotineira no estado da arte em termos de segurança da informação.

6.1.8.3. A CONTRATADA deverá fornecer subsídios para que a equipe técnica da Área de Tecnologia da Informação do Ministério da Justiça e Segurança Pública obtenha todo o conhecimento necessário para o perfeito entendimento da solução e serviços estando capacitada ao final do serviço contratado para manter um ambiente de SOC com equipes de Blue Team e Red Team disponível e íntegro até que ocorra nova contratação.

6.1.8.4. O processo de transferência deverá prever o repasse de conhecimento através de hands-on, scripts e documentação técnica elaborados pela CONTRATADA e homologada pelo Ministério da Justiça e Segurança Pública. Toda modificação/atualização deverá ser documentada e entregue à CONTRATANTE.

6.1.8.5. Caberá à CONTRATADA zelar e assegurar a transferência de todo conhecimento adquirido ou produzido para a CONTRATANTE;

6.1.9. ***Procedimentos de transição e finalização do contrato***

6.1.9.1. Os procedimentos de transição e o encerramento do contrato deverão observar as atividades e prazos da Tabela 10.

Tabela 10 - 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 antes do encerramento contratual
2. Elaborar e entregar o Plano de Transição Contratual	CONTRATADA	120 dias antes do encerramento contratual
3. Entregar todo o conhecimento desenvolvido que deverá ser repassado à Contratada/Nova empresa	CONTRATADA	30 dias antes do encerramento contratual
4. Convocar reunião de encerramento/transição contratual	CONTRATANTE	10 dias antes do encerramento contratual
5. Realizar reunião de encerramento/transição contratual	CONTRATANTE e CONTRATADA	5 dias antes do encerramento contratual
6. Elaborar Termo de Recebimento Definitivo do Contrato	CONTRATANTE	1 dia após o encerramento definitivo do contrato
TOTAL		**180 dias**

6.1.9.2. 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.

6.1.9.3. Ao término do contrato, o CONTRATANTE deverá realizar a devolução dos equipamentos alocados para a execução dos serviços. Fica a contratada obrigada a assegurar o retorno integral dos dados e informações sob sua custódia ao CONTRATANTE, no caso de término do 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 tópico ***Níveis Mínimos de Serviço Exigidos***.

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:

6.3.2.1. Ordem de Serviço (OS);

6.3.2.2. Plano de Inserção;

6.3.2.3. Termos de Recebimento;

6.3.2.4. Termo de Encerramento de OS;

6.3.2.5. Ofício;

6.3.2.6. Ata de Reunião;

6.3.2.7. Relatório;

6.3.2.8. Carta;

6.3.2.9. E-mail institucional/corporativo;

6.3.2.10. Ferramenta Web para registro de chamados;

6.3.2.11. Telefonia: Em caso de urgência, a comunicação será realizada por telefone sendo posteriormente formalizada.

6.3.3. A CONTRATADA deverá manter telefone disponível para a realização de comunicação em caso de urgência devendo manter a CONTRATANTE informada sobre qualquer alteração no seu número.

6.3.4. 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.

6.3.5. 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, a ser assinado pelo representante legal da Contratada.

6.4.3. O **Termo de Ciência** anexo I - E, deverá 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. 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 Serviço Exigidos***

7.3.1. Os serviços deverão ser executados com base nos parâmetros mínimos a seguir estabelecidos:

7.3.2. Os serviços deverão ser iniciados 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.

7.3.2.1. Os serviços deverão ser realizados, no prazo máximo de 15 dias após a assinatura do contrato, salvo as exceções permitidas sob a anuência do CONTRATANTE, sem ônus adicional para o CONTRATANTE.

7.3.2.2. A CONTRATADA deve disponibilizar endereço de correio eletrônico e acesso ao sistema de ITSM acessível pela Internet para registro de abertura de chamado técnico.

7.3.2.3. Todos os serviços serão prestados esperando-se a aplicação das melhores práticas e recomendações do mercado e dos fabricantes.

7.3.3. **Para o grupo 1 - itens 1, 2 e grupo 2 item 3 e 4:**

7.3.3.1. O modelo de medição adotado no contrato será um modelo híbrido, de pagamento de serviço por disponibilidade, condicionado ao alcance de metas de desempenho especificadas no Níveis Mínimos de Serviço Exigidos.

7.3.3.2. Nesse modelo, o valor total dos serviços é estabelecido quando da contratação, com base na disponibilidade estimada de profissionais para atendimento às demandas, porém o valor mensal a ser faturado é calculado com base nos resultados (Níveis Mínimos de Serviço Exigidos) alcançados pela CONTRATADA na prestação dos serviços.

7.3.3.3. Os valores apresentados nas planilhas de composição de custos e formação de preços, quando da apresentação de propostas, corresponderão aos valores máximos a serem faturados na hipótese de a CONTRATADA atingir a meta exigida em todos os indicadores mensais.

7.3.3.4. Não há previsão de bônus ou pagamentos adicionais para os casos em que a CONTRATADA superar as metas previstas, ou caso seja necessária à alocação de maior número de profissionais para o alcance das metas.

7.3.3.5. A superação de uma das metas não poderá ser utilizada para compensar o não atendimento de outras metas, em nenhuma hipótese.

7.3.3.6. A frequência de aferição e avaliação dos níveis de serviço será mensal, devendo a contratada elaborar Relatório Mensal de Atividades, apresentando-o ao Ministério até o quinto dia útil do mês subsequente ao da prestação do serviço.

7.3.3.7. Devem constar desse relatório, entre outras informações, os indicadores/metas de níveis de serviço alcançados, recomendações técnicas, administrativas e gerenciais para o próximo período e demais informações relevantes para a gestão contratual. O conteúdo detalhado e a forma do relatório gerencial serão definidos pelas partes.

7.3.3.8. Caberá à Comissão de Fiscalização do contrato analisar mensalmente o Relatório Mensal de Atividades executados pela Contratada, observando os indicadores e os níveis de serviço alcançados.

7.3.3.9. Caso a Contratada não cumpra as metas estabelecidas no mês, serão aplicadas as glosas, multas ou demais sanções previstas no termo de referência.

7.3.3.10. Nos casos em que a apuração ensejar desempenho abaixo da meta exigida, o valor correspondente à glosa será abatido do pagamento da fatura a vencer.

7.3.3.11. A CONTRATADA deve fornecer, uma mesma ferramenta para abertura de chamados para o Grupo 1, visando ao CONTRATANTE a possibilidade de acompanhamento do chamado registrado em uma equipe e encaminhada a outra equipe.

7.3.3.12. 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.

7.3.3.12.1. Para efeito desta contratação, estabelecem-se os seguintes níveis mínimos de serviço para a resposta e solução das requisições de serviço e incidentes. Os serviços serão medidos com base em indicadores e níveis mínimos de serviço, vinculados a fórmulas de cálculo específicas, e deverão ser executados pela CONTRATADA, e apurados mensalmente, de modo a alcançar as respectivas metas exigidas, conforme tabela 11.

7.3.3.12.2. As médias são um recurso para reduzir o tamanho dos dados históricos de aferição de performance de um item monitorado e podem ser diárias, semanais, quinzenais, mensais e por seguinte. Geralmente as ferramentas de monitoramento utilizam algoritmos que prevê, por exemplo, o armazenamento, a cada hora, de 4 métricas para cada item coletado: mínimo, média, máximo e quantidade. Ela está disponível apenas para os tipos de dados numéricos.

7.3.3.12.3. Para os itens de glosa da tabela 11, quando o percentual for baseado no tipo de **natureza e impacto ao negócio**, a referência a ser seguida será de acordo com a tabela 7 desse termo de referência, item 4.1.15.6.

7.3.3.12.4. Cabe à CONTRATADA comunicar ao Ministério e às Áreas responsáveis pelos serviços no caso de ocorrência de falhas ou erros funcionais dos serviços corporativos. A comunicação deverá ser feita por mensagem ou por meio telefônico dentro dos prazos previstos no Plano de Comunicação a ser entregue pela CONTRATANTE em até 10 dias após a assinatura do contrato.

7.3.3.12.5. O Plano de Comunicação é um documento interno da CONTRATANTE que define os setores a serem notificados conforme tipo de serviço, tempo máximo de espera, regras e padronização das mensagens, assim como a agenda de comunicação. A matriz de contatos deverá ser revisada mensalmente, devendo estar atualizada quanto aos serviços e gestores a serem comunicados, tanto quanto os contatos pertinentes à equipe da CONTRATADA.

7.3.3.12.6. Serão considerados os seguintes pontos no momento de contabilizar a quantidade mínima de serviços para vulnerabilidades não relatadas:

7.3.3.12.6.1. No início da atuação do SOC, após a assinatura do contrato, a Contratada deverá fazer um diagnóstico inicial das vulnerabilidades existentes e entregar o relatório detalhado, inclusive, com procedimentos de correção/mitigação, à Contratante no prazo máximo de 15 dias a contar da data de início prevista na Ordem de Serviço. A data da realização e o diagnóstico serão considerados como baseline para avaliação mensal de vulnerabilidades não relatadas e posteriormente diagnosticadas. As vulnerabilidades preexistentes deverão ser tratadas pela Contratada em conjunto com a contratante, conforme cronograma definido pela Contratante.

7.3.3.12.6.2. Não serão consideradas para fins de glosa as vulnerabilidades *zero day*.

> "Uma vulnerabilidade de dia zero é uma **falha de segurança de software recém-descoberta** que não foi corrigida, porque continua desconhecida para os desenvolvedores do software. Os desenvolvedores ficam sabendo sobre a existência de uma vulnerabilidade de dia zero existente apenas depois que tal ataque acontece. Eles têm “zero dia” de aviso prévio para corrigir a vulnerabilidade antes que o ataque aconteça." [https://www.avast.com/pt-br/c-zero-day]

7.3.3.12.6.3. Será considerado o padrão *Common Vulnerability Scoring System v3.1 (*CVSS v3.1) como base de pontuação para escala de classificação da severidade, conforme site do Fórum Global de equipes de respostas a incidentes e de segurança FIRST.org https://www.first.org/cvss/v3.1/specification-document, item *Qualitative Severity Rating Scale*.

7.3.3.12.6.4. Compete à contratada identificar e reportar vulnerabilidades decorrentes de falhas na implantação ou na aplicação de políticas de segurança aos sistemas corporativos.

7.3.3.12.7. Serão considerados os seguintes pontos no momento de contabilizar a quantidade mínima de serviços para incidentes ocorridos:

7.3.3.12.7.1. No primeiro mês a contar da data de início prevista na Ordem de Serviço, não serão contabilizados nenhum incidente de origem de vulnerabilidades identificadas no relatório de diagnóstico inicial realizado pela Contratada. As vulnerabilidades críticas e alta identificadas

deverão ter tratamento imediato e por isso serão contabilizadas em caso de incidente. A classificação da vulnerabilidade considera o padrão CVSS v3.1;

7.3.3.12.7.2. Incidentes ocorridos por vulnerabilidades zero day ou que não possuam correções ou mitigações por parte do desenvolvedor do software não serão contabilizados;

7.3.3.12.7.3. Incidentes ocorridos de vulnerabilidades relatadas e que a equipe de SOC/ Blue Team não foi autorizada a atuar, devido a impactos que a correção geraria, não serão contabilizadas desde que comprovadamente comunicadas em mais de uma ocasião;

7.3.3.12.7.4. Serão considerados incidentes sofridos com sucesso contra os serviços e sistemas do Ministério, excetuando-se os testes de invasão realizado pelo Red Team.

7.3.3.12.7.5. Incidentes comprovadamente ocorridos por fatores alheiros à atuação da contratada não serão computados para fins de aplicação de glosas e penalidades.

Tabela 11 - Quantidade Mínima de Níveis de Serviços para os itens 1, 2, 3 e 4

ID	Indicadores de Níveis de Serviço	Fórmula de Cálculo com base no mês calendário	Unidade	Meta Exigida	Glosas (sobre o valor mensal)
Serviço de Security Operations Center - SOC (Grupo 1 - Item 01)					
1	Mensal – Índice Monitoramento de Infraestrutura. (Falha ou incidente de segurança de algum serviço ou equipamento de infraestrutura de TIC que deveria estar sendo monitorado e que a **Plataforma de SIEM/SOAR/NTA/UEBA/CTI do Ministério** não foi devidamente configurada para tal apuração.)	Total de sistemas, serviços e equipamento monitorado pela Plataforma / Total de sistemas, serviços e equipamentos em produção x 100%	%	=100%	- 0,5% por cada falta constatada aplicado sob o valor mensal do item 01 Acima dos limites estabelecidos a administração poderá realizar rescisão unilateral da avença e aplicar as sanções previstas no presente instrumento.
2	Mensal – Índice de Plano de Comunicação. (Não cumpra o escopo ou os prazos especificados no Plano de Comunicação para serviços que apresentarem incidentes de segurança da informação)	Total de plano de comunicação entregue / Total de plano de comunicação cumprido o escopo e/ou prazo x 100%	%	=100%	- 0,5% por cada falta constatada aplicado sob o valor mensal do item 01 Acima dos limites estabelecidos a administração poderá realizar rescisão unilateral da avença e aplicar as sanções previstas no presente instrumento.
3	Mensal – Índice de Incidentes cibernéticos detectados. (Incidente cibernético de algum serviço do Ministério ocorrido sem que a **Plataforma de SIEM/SOAR/NTA/UEBA/CTI do Ministério tenha detectado porque** não foi devidamente configurada para tal detecção.)	Total de incidentes cibernético detectados pela Plataforma / Total de incidentes cibernético ocorridos x 100%	%	=100%	- 5% por cada falta constatada aplicado sob o valor mensal do item 01 e 02 Acima dos limites estabelecidos a administração poderá realizar rescisão unilateral da avença e aplicar as sanções previstas no presente instrumento.
4	Quantidade de Vulnerabilidade(s) não relatadas e posteriormente identificadas. Obs.: Ver item 7.3.3.12.6	Soma das quantidades de vulnerabilidades não relatadas e posteriormente identificadas	Qt	0	Quando da ocorrência de vulnerabilidades não identificadas a Contratada será glosada mensalmente conforme segue: - 1% por vulnerabilidade com severidade baixa, limitada a 48 ocorrências durante a vigência contratual. - 2% por vulnerabilidade com severidade média, limitada a 24 ocorrências durante a vigência contratual. - 3% por vulnerabilidade com severidade alta, limitada a 12 ocorrências durante a vigência contratual. - 5% por vulnerabilidade com severidade crítica, limitada a 4 ocorrências durante a vigência contratual. Aplicado sob o valor mensal dos itens 01 e 02. Caso algum dos limites de ocorrências seja superado, a administração poderá realizar rescisão unilateral da avença e aplicar as sanções previstas no presente instrumento, ou optar pela aplicação de glosa máxima permitida. A aplicação da glosa máxima será efetuada no pagamento referente ao mês de identificação do descumprimento da exigência.
5	Quantidade de Ataque(s) sofridos com sucesso. Obs.: Ver item 7.3.3.12.7	Soma das quantidades de ataques ocorridos com sucesso	Qt	0	Quando da ocorrência de ataques sofridos com sucesso a Contratada será glosada mensalmente conforme segue: - 10% por impacto ao negócio baixo por evento limitado a 3 ocorrências durante a vigência contratual. - 20% por impacto ao negócio médio por evento limitado a 2 ocorrências durante a vigência contratual. - 40% por impacto ao negócio alto por evento, limitados a 1 ocorrência durante a vigência contratual. Aplicado sob o valor mensal dos itens 01 e 02. Caso algum dos limites de ocorrências seja superado, a administração poderá realizar rescisão unilateral da avença e aplicar as sanções previstas no presente instrumento, ou aplicar pela glosa máxima permitida no mês de identificação do descumprimento da exigência, ou optar pela aplicação de glosa máxima permitida. A aplicação da glosa máxima será efetuada no pagamento referente ao mês de identificação do descumprimento da exigência.
6	Mensal - Índice de Disponibilidade do SOC. (Falha, degradação ou indisponibilidade de operação do SOC sediado nas instalações da CONTRATADA para a prestação dos serviços contratados)	Indisponibilidade de sistema/serviços monitorados. 100 x (Horas Totais no Período = Dias do Mês x Horas Dias - Horas de Manutenção Preventiva - Horas Indisponíveis causadas por Terceiros - Horas Indisponíveis no Mês) / (Horas Totais no Período = Dias do Mês x Horas Dias - Horas de Manutenção Preventiva - Horas Indisponíveis no Mês)	%	99,70% e/ou média de performance mensal auferida (será considerada a média histórica dos últimos 30 dias)	- 0,5% para cada décimo percentual ou fração menor que a meta definida por indicador até o limite de 98,70% e/ou degradação do desempenho de rede e processamento dos recursos de TIC do SOC superior a 10% da média mensal (será considerada a média histórica dos últimos 30 dias). - 1% para cada décimo percentual ou fração menor que a meta definida por indicador entre os limites de 98,69% até 97,70% e/ou degradação do desempenho de rede e processamento dos recursos de TIC do SOC superior a 20% da média mensal (será considerada a média histórica dos últimos 30 dias). - 1,5% para cada décimo percentual ou fração menor que a meta definida por indicador abaixo do limite de 97,69% e/ou degradação do desempenho de rede e processamento dos recursos de TIC do SOC superior a 30% da média mensal (será considerada a média histórica dos últimos 30 dias). Aplicado sob o valor mensal do item 01. Obs: Os cálculos se referem a todo o ambiente mantido, ou seja, uma ou mais aplicações/serviços monitorados, a formula de calculo é única, tendo como o limite total em 30%. Acima dos limites estabelecidos a administração poderá realizar rescisão unilateral da avença e aplicar as sanções previstas no presente instrumento.
Atendimento das Requisições e dos Incidentes (Grupo 1 - Itens 01 e 02)					
7	Mensal - Índice de abertura de **chamados** (incidente e ou requisição) de atendimento com **tratamento iniciado** em até 5 minutos.	Total de chamados recepcionadas em até 5 minutos do recebimento / Total de chamados recebidos x 100%	%	>=90%	- 0,1% por cada falta constatada aplicado sob o valor mensal do item 01 Acima dos limites estabelecidos a administração poderá realizar rescisão unilateral da avença e aplicar as sanções previstas no presente instrumento.
8	Mensal - Índice de **triagem** de incidentes e ou requisições abertos em até 15 minutos.	Total de triagem de incidentes e ou requisições abertos em até 15 minutos do recebimento / Total de chamados recebidos x 100%	%	>=90%	- 0,2% por impacto ao negocio Baixa - 0,4% por impacto ao negocio Médias e Altas Aplicado sob o valor mensal do item 01 Acima dos limites estabelecidos a administração poderá realizar rescisão unilateral da avença e aplicar as sanções previstas no presente instrumento.

ID	Indicadores de Níveis de Serviço	Fórmula de Cálculo com base no mês calendário	Unidade	Meta Exigida	Glosas (sobre o valor mensal)
9	Mensal - Índice de **investigação** de incidentes e ou requisições abertos em até 30 minutos.	Total de investigado de incidentes e ou requisições abertos em até 30 minutos do recebimento / Total de chamados recebidos x 100%	%	>=90%	- 0,3% por impacto ao negocio Baixa - 0,5% por impacto ao negocio Média - 1% por impacto ao negocio Alta Aplicado sob o valor mensal dos itens 01 e 02 Acima dos limites estabelecidos a administração poderá realizar rescisão unilateral da avença e aplicar as sanções previstas no presente instrumento.
10	Mensal - Índice de **resposta** a incidentes e ou requisições abertos em até 1 horas.	Total de resposta a incidentes e ou requisições abertos em até 1 horas do recebimento / Total de chamados recebidos x 100%	%	>=80%	- 0,3% por impacto ao negocio Baixa - 0,5% por impacto ao negocio Média - 1% por impacto ao negocio Alta Aplicado sob o valor mensal dos itens 01 e 02 Acima dos limites estabelecidos a administração poderá realizar rescisão unilateral da avença e aplicar as sanções previstas no presente instrumento.
11	Mensal - Índice de **resposta** a incidentes e ou requisições abertos em até 2 horas.	Total de resposta a incidentes e ou requisições abertos em até 2 horas do recebimento / Total de chamados recebidos x 100%	%	>=90%	- 0,3% por impacto ao negocio Baixa - 0,5% por impacto ao negocio Média - 1% por impacto ao negocio Alta Aplicado sob o valor mensal dos itens 01 e 02 Acima dos limites estabelecidos a administração poderá realizar rescisão unilateral da avença e aplicar as sanções previstas no presente instrumento.
12	Mensal – Índice recorrência de incidentes e ou requisições abertos (Reincidência de abertura de chamados por falta de atuação da Contratada)	Total de requisições e ou incidentes reabertos / Total de solicitações mês x 100%	%	<=1% do total de solicitações/mês	- 5% para quando for superior à meta definida até o limite de 2% dos incidentes; - 10% acumulativo para quando for superior a 2,1% até o limite de 5% dos incidentes; - 15% acumulativos para quando for superior a 5,1% até o limite de 8% dos incidentes. Aplicado sob o valor mensal dos itens 01 e 02 Acima dos limites estabelecidos a administração poderá realizar rescisão unilateral da avença e aplicar as sanções previstas no presente instrumento.
13	Mensal - Índice de atendimento para demandas dentro das dependências físicas do MJSP em situações de ocorrências de incidentes e problemas graves, conforme item 6.1.4.5, dentro de 15 minutos	Total de atendimentos a demandas em situações de ocorrências de incidentes e problemas graves em até 15 minutos / Total de atendimentos a demanda em em situações de ocorrências de incidentes e problemas graves x 100%	%	<=1% do total de solicitações/mês	- 5% para quando for superior à meta definida até o limite de 2% dos incidentes; - 10% acumulativo para quando for superior a 2,1% até o limite de 5% dos incidentes; - 15% acumulativos para quando for superior a 5,1% até o limite de 8% dos incidentes. Aplicado sob o valor mensal dos itens 01 e 02
Serviço de Teste de Invasão - Red Team (Grupo 2 - Item 3 e Item 4)					
14	Índice Ordens de Serviços Cumpridas Dentro do Prazo	Soma da quantidade de dias fora do prazo acordados.	Qt.	=0	Quando da ocorrência de atraso até 3 dias a Contratada será glosada conforme segue: - 10% por dia de atraso; Aplicado sob o valor da ordem de serviço do item 3 ou 4. Acima dos limites estabelecidos a administração poderá realizar rescisão unilateral da avença e aplicar as sanções previstas no presente instrumento
15	Índice de qualidade do relatório de acordo o item 4.1.16.15 - Relatório de Teste de Invasão deste Termo de Referência	Soma de inconformidade identificadas.	Qt.	=0	Quando da ocorrência de até 50% do total inconformidades de itens mencionados para o relatório a Contratada será glosada conforme segue: - 3% por inconformidade ; Aplicado sob o valor da ordem de serviço do item 3 ou 4. A administração poderá realizar rescisão unilateral da avença e aplicar as sanções previstas no presente instrumento nos seguintes casos: - Para uma ordem de serviço quando essa ultrapassar 50% de inconformidade; - 3 ordens de serviços seguidas ou 5 alternadas com até 50% de inconformidades.
16	Quantidade de vulnerabilidades críticas e altas não relatadas e posteriormente identificadas. Obs.: Ver item 7.3.3.12.6	Soma das quantidades de vulnerabilidades criticas e altas não relatadas e posteriormente identificadas	Qt.	=0	Descumprimento parcial se aplica as sanções administrativas de acordo com o item 7.4 deste termo (subitem 7.4.2.2.2)

7.3.3.12.8. Os chamados técnicos somente serão encerrados, atestados e validados quando todos os objetivos propostos forem plenamente atingidos, e todos os produtos e serviços realizados e entregues com a qualidade demandada e aprovada pela Equipe de Gestão do Contrato.

7.3.3.12.9. Durante o período de até 60 (sessenta) dias previstos para os cadastros, parametrizações e customizações da **Plataforma de SIEM/SOAR/NTA/UEBA/CTI do Ministério, bem como da ferramenta de ITSM da CONTRATADA**, serão consideradas e aplicadas as glosas citadas na tabela 11, sendo limitada a 25% nos primeiros 30 dias e 50% entre 30 e 60. E isto não exime a CONTRATADA de emitir os relatórios necessários para a avaliação e acompanhamento dos indicadores.

7.3.3.12.10. As **glosas serão limitadas ao total máximo de 50% por item de acordo com o faturamento mensal máximo.**

7.3.3.12.11. **A realização de glosas no limite estabelecido acima por falta no descumprimento dos Níveis Mínimos de Serviço Exigidos por dois meses consecutivos ou quatro não consecutivos durante a vigência do contrato, será considerada inexecução parcial dos serviços e sujeitará a CONTRATADA às sanções administrativas cabíveis. Para fins de proporcionalização das sanções será considerado o conjunto dos dois meses consecutivos ou quatro não consecutivos**.

7.4. ***Sanções administrativas***

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. 1% (um por cento) por dia sobre o valor da ordem de serviço em caso de atraso na execução dos serviços e entregas, 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. 5% (cinco 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, em caso de inexecução total da obrigação assumida;

7.4.2.2.4. 0,1% a 5%, conforme detalhamento constante das **tabelas 12 e 13**, 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 glosas e ou multas, 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 12 e 13:

Tabela 12 - Gradação das multas

GRAU	CORRESPONDÊNCIA
01	0,1% ao dia sobre o valor total mensal do item, limitado a incidência de 15 (quinze) dias.
02	0,2% ao dia sobre o valor total mensal do item, limitado a incidência de 15 (quinze) dias.
03	0,3% ao dia sobre o valor total mensal do item, limitado a incidência de 15 (quinze) dias.
04	1,6% ao dia sobre o valor total mensal do item, limitado a incidência de 15 (quinze) dias.
05	1% dos limites estabelecidos sobre o valor adjudicado do item.
06	2% dos limites estabelecidos sobre o valor adjudicado do item.
07	3% dos limites estabelecidos sobre o valor adjudicado do item.
08	0,5% ao dia sobre o valor do item adjudicado, limitado a 05 (cinco) dias.
09	0,2% sobre o valor do item adjudicado por relatório, limitado a 02 (duas) ocorrências.

Tabela 13 - Infrações

INFRAÇÃO		
Item(s) do(s) contrato(s)	DESCRIÇÃO	GRAU
1, 2, 3 e 4	Suspender ou interromper, salvo motivo de força maior ou caso fortuito, os serviços contratuais por dia e por unidade de atendimento.	04
1, 2, 3 e 4	Manter funcionário sem qualificação para executar os serviços contratados, por empregado e por dia.	03
1, 2,3 e 4	Recusar-se a executar serviço determinado pela fiscalização, por serviço e por dia.	02
1 e 2	Descumprir os limites estabelecidos nos itens 4 e 5 impacto ao negócio baixo da Tabela 11 - Quantidade Mínima de Níveis de Serviços para os itens 1, 2, 3 e 4	05
1 e 2	Descumprir os limites estabelecidos nos itens 4 e 5 impacto ao negócio médio da Tabela 11 - Quantidade Mínima de Níveis de Serviços para os itens 1, 2, 3 e 4	06
1 e 2	Descumprir os limites estabelecidos nos itens 4 e 5 impacto ao negócio alto e critico da Tabela 11 - Quantidade Mínima de Níveis de Serviços para os itens 1, 2, 3 e 4	07
3 e 4	Descumprir os limites dos dias estabelecidos no item 14 da Tabela 11 - Quantidade Mínima de Níveis de Serviços para os itens 1, 2, 3 e 4	08
3 e 4	Descumprir os limites estabelecidos no item 15 da Tabela 11 - Quantidade Mínima de Níveis de Serviços para os itens 1, 2, 3 e 4	09
Para os itens a seguir, deixar de:		
1, 2, 3 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, 2, 3 e 4	Indicar e manter durante a execução do contrato os prepostos previstos no edital/contrato.	01

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

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 será precedida do recebimento definitivo do serviço, conforme este Termo de Referência.

7.5.2. Quando houver glosa parcial dos serviços, a contratante deverá comunicar a empresa para que emita a nota fiscal ou fatura com o valor exato dimensionado.

7.5.3. O pagamento será efetuado pela Contratante no prazo de *30 (trinta)* dias, contados do recebimento da Nota Fiscal/Fatura.

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

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

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

7.5.5. 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:

7.5.5.1. o prazo de validade;

7.5.5.2. a data da emissão;

7.5.5.3. os dados do contrato e do órgão contratante;

7.5.5.4. o período de prestação dos serviços;

7.5.5.5. o valor a pagar; e

7.5.5.6. eventual destaque do valor de retenções tributárias cabíveis.

7.5.6. 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 a Contratante;

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

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

7.5.9. 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.

7.5.10. 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.

7.5.11. 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.

7.5.12. 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.

7.5.12.1. 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.

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

7.5.14. 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.

7.5.15. 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.

7.5.16. Nos casos de eventuais atrasos de pagamento, desde que a Contratada não tenha concorrido, de alguma forma, para tanto, o valor devido deverá ser acrescido de atualização financeira, e sua apuração se fará desde a data de seu vencimento até a data do efetivo pagamento, em que os juros de mora serão calculados à taxa de 0,5% (meio por cento) ao mês, ou 6% (seis por cento) ao ano, mediante aplicação das seguintes fórmulas:

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

$$I = (TX) \qquad I = \frac{(6 / 100)}{365} \qquad I = 0{,}00016438$$

TX = Percentual da taxa anual = 6%

7.5.17. Para os itens 1 e 2, a forma de pagamento será mensal;

7.5.17.1. Os pagamentos dos serviços serão efetuados mensalmente com a apresentação pela CONTRATADA de nota fiscal, juntamente com os relatórios gerenciais de serviços, quando serão contabilizados os serviços prestados e os pagamentos devidos.

7.5.18. Para o item 3 e 4, a forma de pagamento será feita conforme as Ordens de Serviços previamente acordadas.

7.5.18.1. O pagamento do serviço ocorrerá a qualquer tempo conforme quantidade de alvos demandados, após a efetiva realização dos procedimentos solicitados e a apresentação dos Relatórios definidos neste Termo de Referência para o item em questão.

7.5.19. 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.

7.6. ***Do Recebimento***

7.6.1. A emissão da Nota Fiscal/Fatura deve ser precedida do recebimento definitivo do objeto contratual, conforme Anexo I-M, após análises e elaboração de relatórios pela equipe de fiscalização e nos termos abaixo.

7.6.2. No prazo de até *5 dias corridos* do adimplemento da parcela, a CONTRATADA deverá entregar toda a documentação comprobatória do cumprimento da obrigação contratual;

7.6.3. O recebimento provisório será realizado pelo fiscal técnico após a entrega da documentação acima, da seguinte forma:

7.6.3.1. 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.

7.6.3.1.1. 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

7.6.3.1.2. 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.

7.6.3.1.3. O recebimento provisório também ficará sujeito, quando cabível, à conclusão de todos os testes de campo e à entrega dos Manuais e Instruções exigíveis.

7.6.3.1.4. No prazo de até *10 dias corridos* 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.

7.6.3.2. No prazo de até *10 dias corridos* 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.

7.6.3.2.1. 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.

7.6.3.2.2. 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.

7.6.3.2.2.1. Na hipótese de a verificação a que se refere o parágrafo anterior não ser procedida tempestivamente, reputar-se-á como realizada, consumando-se o recebimento provisório no dia do esgotamento do prazo.

7.6.4. No prazo de até *10 (dez) dias corridos* a partir do recebimento provisório dos serviços, o Fiscal Requisitante e Fiscal Técnico do Contrato deverá providenciar o recebimento definitivo, ato que concretiza o ateste da execução dos serviços, obedecendo as seguintes diretrizes:

7.6.4.1. 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;

7.6.4.2. Emitir Termo Circunstanciado para efeito de recebimento definitivo dos serviços prestados, com base nos relatórios e documentações apresentadas; e

7.6.4.3. O Gestor deverá comunicar a empresa para que emita a Nota Fiscal ou Fatura, com o valor exato dimensionado pela fiscalização*, com base no Instrumento de Medição de Resultado (IMR), ou instrumento substituto*.

7.6.5. 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 (Lei n° 10.406, de 2002).

7.6.6. 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.

8. ESTIMATIVA DE PREÇOS DA CONTRATAÇÃO

8.1. O valor total estimado da presente contratação é de R$ 8.504.157,58 (oito milhões, quinhentos e quatro mil cento e cinquenta e sete reais e cinquenta e oito centavos).

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.

Tabela 14 - Estimativa de Preços

Grupo	Item	Código SIASG CATSER	Descrição do Bem ou Serviço	Quantidade	Métrica ou Unidade de medida	Valor unitário (R$)	Valor Total (24 meses) (R$)
1	1	26000	Serviço de Security Operations Center - SOC	24	Unidade (Mensal)	106.044,63	2.545.071,08
	2	26000	Serviço de Tratamento e Resposta aos Incidentes Cibernéticos - CSIRT - Blue Team	24	Unidade (Mensal)	75.265,16	1.806.363,76
2	3	26000	Serviço de Teste de Invasão - Red Team: Sistemas Web	217	Unidade (Alvo)	15.195,57	3.297.438,69
	4	2600	Serviço de Teste de Invasão - Red Team: Infraestrutura	610	Unidade (Alvo)	1.402,11	855.284,05

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 de Despesa: 339040;**

9.1.3. **PTRES: 172184;**

9.1.4. **Plano Interno (PI): GL67OTCGLTI;**

9.1.5. Fonte: 0100;

9.1.6. Ação: 2000;

9.1.7. Plano Orçamentário (PO): 000C.

10. DA VIGÊNCIA DO CONTRATO

10.1. A **vigência do contrato será de 24 (vinte e quatro) meses** a contar de sua assinatura, com eficácia a partir de sua publicação, podendo ser prorrogado, no interesse da Contratante, por iguais e sucessivos períodos até o limite de 60 (sessenta) meses, conforme artigo 57, inciso II, da lei nº. 8666/93 e preservada as condições mais vantajosas para a administração.

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 abertura da sessão pública, que marca a 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 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. Para o grupo 1, o regime de execução será a de empreitada por preço global.

12.1.1.2. Para o grupo 2, 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 - 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 ou convite e ofertar o menor preço.

12.1.3. Modalidade

12.1.3.1. 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. Atestado(s) ou Declarações de Capacidade Técnica, fornecido(s) por pessoa jurídica de direito público ou privado, que comprove(m) aptidão para desempenho de atividade pertinente e compatível em características e quantidades com o objeto desta licitação, comprovando:

12.3.1.1. **Para o Grupo 1**

12.3.1.1.1. Experiência na prestação de serviços de administração de solução(ões) de **automação** (Orquestração, Automação e Resposta de Segurança (Security Orchestration, Automation, and Response - SOAR), de **análise e correlacionamento** (Monitoramento de estação de trabalho (Endpoint Detection and Response - EDR), Análise de Tráfego de Rede (Network Traffic Analysis - NTA), Análise de Comportamento de Usuário (User Entity and Behavior Analytics - UEBA), Análise de Inteligência de Ameaças Cibernéticas (Cyber Threat Intelligence - CTI) e de coleta (Informações de segurança e gestão de eventos (Security Informati on and Event Management - SIEM) para um total de, no mínimo de;

12.3.1.1.1.1. **10 (dez) sistemas e serviços de TI;**

12.3.1.1.1.2. **200 (duzentos) maquinas virtuais**;

12.3.1.1.1.3. **100 (cem) ativos de infraestrutura TI**;

12.3.1.1.1.4. **1200 (mil e duzentos) estações de trabalho, incluindo desktops e notebooks, e;**

12.3.1.1.1.5. **1200 (mil e duzentos) usuários de rede.**

12.3.1.2. **Para o Grupo 2**

12.3.1.2.1. Experiência na prestação de **serviços de testes de invasão** em empresa ou órgão da Administração Pública para exploração de vulnerabilidades de segurança da informação, que contenham pelo menos 1.000 usuários de sistema cadastrados e ativos, em conformidade

com boas práticas internacionais;

12.3.2. A quantidade especificada acima é justificável em razão de que representa aproximadamente de 30% (trinta por cento) do quantitativo a ser atendido por este Contrato, sendo este percentual considerado razoável e plenamente compatível em quantidades e características, os quais demonstrarão a capacidade do futuro fornecedor em prestar a integralidade dos serviços;

12.3.3. Será permitido o somatório de atestado(s) de capacidade técnica para efeito de comprovação de experiência na prestação dos serviços de características técnicas semelhantes ao objeto desta contratação, não se exigindo que todos tenham sido prestados a uma única pessoa jurídica de direito público ou privado.

12.3.4. Nos termos do art. 30, da Lei nº 8666/1993, é plenamente cabível a exigência de comprovação de experiência da licitante, indispensável e pertinente à garantia do cumprimento das obrigações da Administração. Dessa forma, não restringe o caráter competitivo do certame fixar quantitativos mínimos em compatibilidade com o princípio da razoabilidade, devendo as licitantes fazerem prova dos quantitativos mínimos, demonstrando a experiência acumulada por serviços executados e em execução. Prevendo o mínimo de segurança para a Administração, as empresas que na data do certame não provarem o mínimo exigido neste Termo de Referência, serão desclassificada do certame;

12.3.5. Todos os atestados apresentados na documentação da licitante deverão conter, obrigatoriamente, a especificação dos serviços executados, o nome e cargo do declarante e estar acompanhados de cópias dos respectivos contratos e aditivos e/ou outros documentos comprobatórios do conteúdo declarado, sob pena de desclassificação do certame;

12.3.6. Somente serão aceitos atestados expedidos após a conclusão do contrato ou se decorrido, pelo menos, um ano do início de sua execução, exceto se firmado para ser executado em prazo inferior;

13. DA EQUIPE DE PLANEJAMENTO DA CONTRATAÇÃO E DA APROVAÇÃO

13.1. A Equipe de Planejamento da Contratação foi instituída pela PORTARIA SAA Nº 25, DE 30 DE JULHO DE 2020 (12273687) e alterada pela PORTARIA SAA/SE/MJSP Nº 80, DE 15 DE DEZEMBRO DE 2021 (16709100).

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

I - **Integrante Requisitante:** Ivanildo de Oliveira da Silva JR, SIAPE 2535600, CPF 031.033.324-59.

II - **Integrante Requisitante Substituto:** Joédes Cardoso da Silva, SIAPE 3730955, CPF 523.656.891-91.

III - **Integrante Técnico:** Cintia Mye Yonekawa Yamaguti, SIAPE 3201981, CPF 619.425.371-15.

IV - **Integrante Técnico Substituto:** Madson Luiz Magno da Silva, CPF 047.519.171-45.

V - **Integrante Administrativo:** Gustavo Henrique Corrêa de Paula Maciel, CPF 916.497.571-15.

VI - **Integrante Administrativo Substituto:** Lorenna Ayres Leal Lima, SIAPE 1710987.

Aprovo,

Autoridade Máxima da Área de TIC	
Nome	Leonardo Bueno de Melo
Cargo	Diretor de TIC (Substituto)
Matrícula	1363771

14. ANEXOS

São partes integrantes deste Termo de Referência os seguintes anexos.
ANEXO I - A - PROPOSTA DE PREÇOS.
ANEXO I - B - MODELO DE ORDEM DE SERVIÇO – O.S.
ANEXO I - C - RELATÓRIO DE CHAMADO TÉCNICO – RCTA.
ANEXO I - D - MODELO DE DECLARAÇÃO DE VISTORIA.
ANEXO I - E - TERMO DE CIÊNCIA.
ANEXO I - F - TERMO DE COMPROMISSO.
ANEXO I - G - MODELO DE DECLARAÇÃO DE RENÚNCIA À VISTORIA.
ANEXO I - H - MODELO DE PLANO DE INSERÇÃO.
ANEXO I - I - MODELO DE PLANO DE FISCALIZAÇÃO.
ANEXO I - J - MODELO DE DECLARAÇÃO DE SUSTENTABILIDADE AMBIENTAL.
ANEXO I - K - PLANILHA DE AVALIAÇÃO DE TREINAMENTO.
ANEXO I - L - TERMO DE RECEBIMENTO PROVISÓRIO.
ANEXO I - M - TERMO DE RECEBIMENTO DEFINITIVO.
ANEXO I - N - ESTUDO TÉCNICO PRELIMINAR(15854445).
ANEXO I - O - PORTARIA 513 MJSP(15854486).

Documento assinado eletronicamente por **Cintia Mye Yonekawa Yamaguti**, **Integrante Técnico(a)**, em 20/12/2021, às 11:20, com fundamento no § 3º do art. 4º do Decreto nº 10.543, de 13 de novembro de 2020.

Documento assinado eletronicamente por **IVANILDO DE OLIVEIRA DA SILVA JUNIOR**, **Integrante Requisitante**, em 20/12/2021, às 12:19, com fundamento no § 3º do art. 4º do Decreto nº 10.543, de 13 de novembro de 2020.

Documento assinado eletronicamente por **Gustavo Henrique Correa de Paula Maciel**, **Integrante Administrativo**, em 20/12/2021, às 12:43, com fundamento no § 3º do art. 4º do Decreto nº 10.543, de 13 de novembro de 2020.

Documento assinado eletronicamente por **Leonardo Bueno de Melo**, **Diretor(a) da Tecnologia da Informação e Comunicação - Substituto(a)**, em 20/12/2021, às 14:42, com fundamento no § 3º do art. 4º do Decreto nº 10.543, de 13 de novembro de 2020.

15854445 08006.000003/2021-38

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

ESTUDO TÉCNICO PRELIMINAR DA CONTRATAÇÃO
PROCESSO Nº 08006.000003/2021-38

INTRODUÇÃO

O 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.

O presente estudo tem por objetivo demonstrar a viabilidade técnica e econômica da contratação de empresa especializada para o fornecimento de **Serviço de Centro de Operações de Segurança - SCO (Security Operations Center - SOC) com funcionamento e suporte 24h por dia e 7 dias por semana, Serviço de tratamento e resposta aos incidentes cibernéticos - CSIRT - Blue Team e Serviço de teste de invasão - Red Team** e garantia dos serviços pelo período de 24(vinte e quatro) meses, renováveis até o limite de 60(sessenta) 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. O Ministério da Justiça e Segurança Pública possui um ambiente composto por uma diversidade de tecnologias, pessoas que as acessam, sistemas, locais e informações que juntas elevam a complexidade da gestão de segurança da informação.

1.2. O SIEM a ser utilizado na prestação de serviço, e os softwares de SOAR/NTA/UEBA/CTI, serão fornecidos pelo MJSP. Outros softwares necessários para a prestação de serviço devem ser fornecidos pela Contratada, conforme detalhado em outros itens deste ETP.

1.3. No que diz respeito a diversidade de Tecnologias, quantitativos consolidados, relação de sistemas e outras informações, constam no **relatório de informações sobre a infraestrutura** (14628328).

Tabela 1 - Resumo dos itens de infraestrutura

Itens	Descrição	totais
1.	Equipamentos e tecnologias utilizadas no MJSP	728
2.	Total de estações de trabalho (14868691)	3.125
3.	Total de usuários cadastrados no AD	5.460
4.	Sistemas críticos, essenciais e outros	217
5.	Tecnologias de nuvem contratada Oracle e Microsoft	3
6.	Total de chamados para janeiro e fevereiro 2021 - N3 - Segurança(14656980)	219

Fonte: Relatório de **relatório de informações sobre a infraestrutura** (14628328) e Anexo Planilha de Sistemas Web (15983136).

1.4. 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. Com a transformação digital cada vez mais presente nas organizações, riscos, ameaças e vulnerabilidades que antes não existiam, começaram a surgir. Com dados e informações na nuvem, transações feitas através da internet e redes Wi-Fi, facilitam o dia a dia. Mas também abrem brechas de segurança para ataques de *hackers*, roubo de informações e outras ameaças à segurança virtual.

1.5. De acordo com o relatório de violação de dados de final de ano 2019 da Identity Theft Resource Center - ITRC, houve exposição de registros, sensíveis ou não, em centenas de vazamentos, conforme a figura 1:

INDUSTRY	# OF BREACHES	# OF SENSITIVE RECORDS EXPOSED	# OF NON-SENSITIVE RECORDS EXPOSED
Business	644	18,824,975	705,106,352
Medical/Healthcare	525	39,378,157	1,852
Banking/Credit/Financial	108	100,621,770	20,000
Government/Military	83	3,606,114	22,747
Education	113	2,252,439	23,103
2019 TOTALS:	1,473	164,683,455	705,174,054

Figura 1 - End of Year Data Breach Report 2019 - Identity Theft Resource Center

1.6. De acordo com a figura 2, temos os tipos de violações de dados por método de ataque e segmento da indústria:

# OF DATA BREACHES PER METHOD PER INDUSTRY						
Method	Banking	Business	Education	Government	Medical	Totals
Hacking/Intrusion (includes Phishing, Ransomware/Malware and Skimming)	31	291	29	35	191	577
Unauthorized Access	45	223	59	15	196	538
Employee Error/Negligence/ Improper Disposal/Lost	12	42	15	19	73	161
Accidental Web/Internet Exposure	12	44	7	8	17	88
Physical Theft	2	17	0	2	32	53
Insider Theft	6	12	2	3	10	33
Data on the Move	0	15	1	1	6	23

Figura 2 - End of Year Data Breach Report 2019 - Identity Theft Resource Center

1.7. No segmento governo, o método de ataque mais utilizado foi Hacking/Intrusion com cerca de 42,2%, assim como, em todos os outros segmentos. Não se deve considerar o número de violações de dados de forma absoluta, mas se deve levar em consideração a sensibilidade do dado violado não somente, o prejuízo financeiro imediato associado.

1.8. **Panorama no Brasil - Estatísticas de incidentes**

1.9. No Brasil, o CERT.br é o Grupo de Resposta a Incidentes de Segurança para a Internet, mantido pelo NIC.br, do Comitê Gestor da Internet no Brasil. É responsável por tratar incidentes de segurança em computadores que envolvam redes conectadas à Internet no Brasil.

1.10. Atua como um ponto central para notificações de incidentes de segurança no Brasil, provendo a coordenação e o apoio no processo de resposta a incidentes e, quando necessário, colocando as partes envolvidas em contato.

1.11. O CERT.br mantém estatísticas sobre notificações de incidentes a ele reportados. Estas notificações são voluntárias e refletem os incidentes ocorridos em redes que espontaneamente os notificaram ao CERT.br. Os dados sumarizados são apresentados na figura 3.

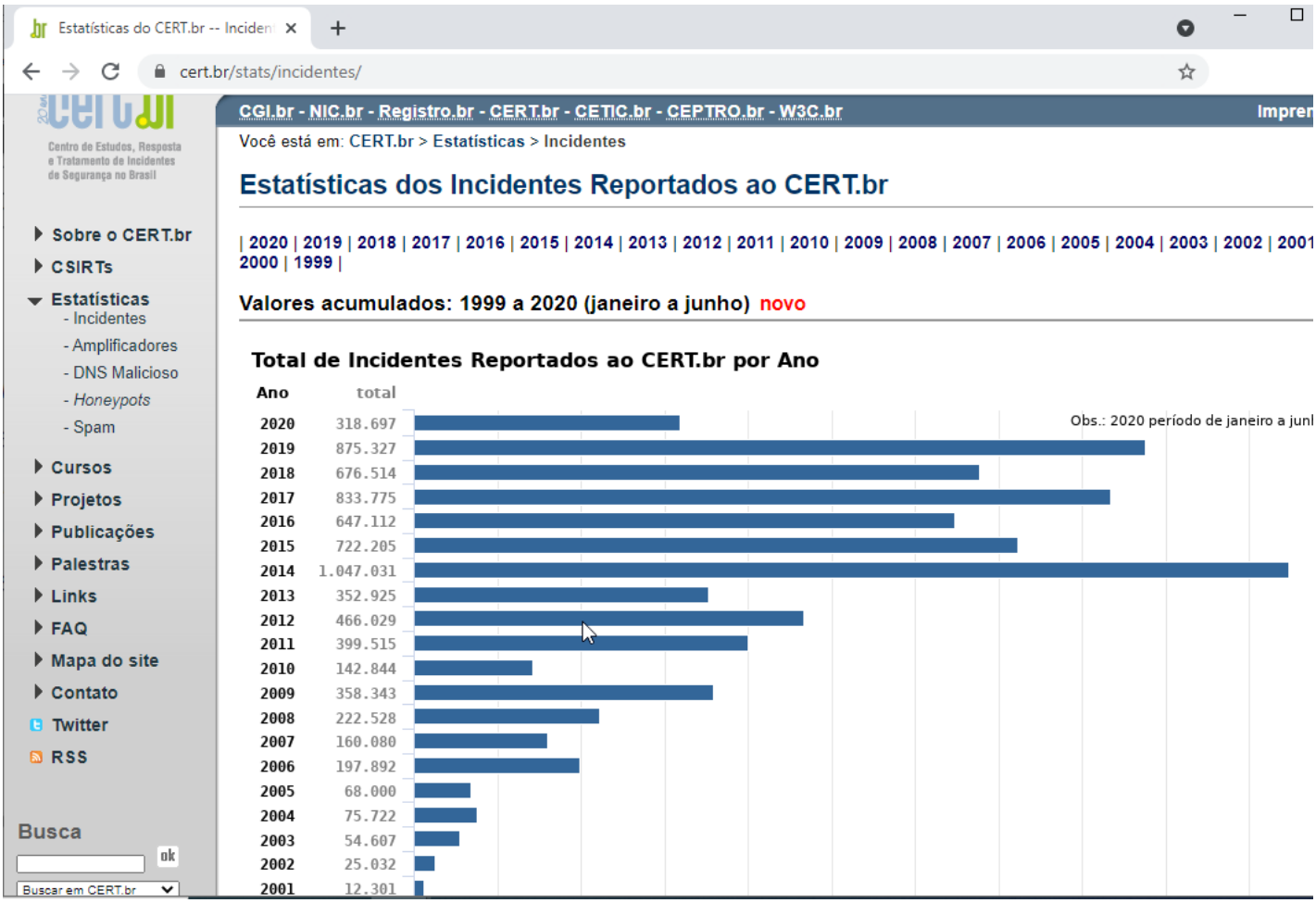

Figura 3 - Total de incidentes reportados, Fonte: CERT.br disponível em https://www.cert.br/stats/incidentes/ acesso em 13/05/2021.

1.12. **Incidentes Reportados ao CERT.br -- Janeiro a Junho de 2020**

1.13. A Tabela 2 apresenta os Totais Mensais e Anual Classificados por Tipo de Ataque.

Tabela - 2: Totais Mensais e Anual Classificados por Tipo de Ataque.

Mês	Total	worm (%)	dos (%)	invasão (%)	web (%)	scan (%)	fraude (%)	outros (%)

jan	**35094**	6703	19	3579	10	54	0	999	2	20704	59	2701	7	354	1
fev	**40229**	8215	20	7424	18	52	0	897	2	21184	52	2319	5	138	0
mar	**63313**	9316	14	16837	26	93	0	1045	1	31633	49	3111	4	1278	2
abr	**55255**	7680	13	6092	11	110	0	1458	2	36287	65	3537	6	91	0
mai	**59820**	10698	17	4815	8	122	0	2225	3	38389	64	3512	5	59	0
jun	**64986**	13033	20	7417	11	184	0	2187	3	39243	60	2844	4	78	0
Total	**318697**	55645	17	46164	14	615	0	8811	2	187440	58	18024	5	1998	0

Fonte: CERT.br disponível em https://www.cert.br/stats/incidentes/2020-jan-jun/total.html acesso em 13/05/2021.

1.14. A Figura 4 apresenta de forma gráfica os tipos de ataque.

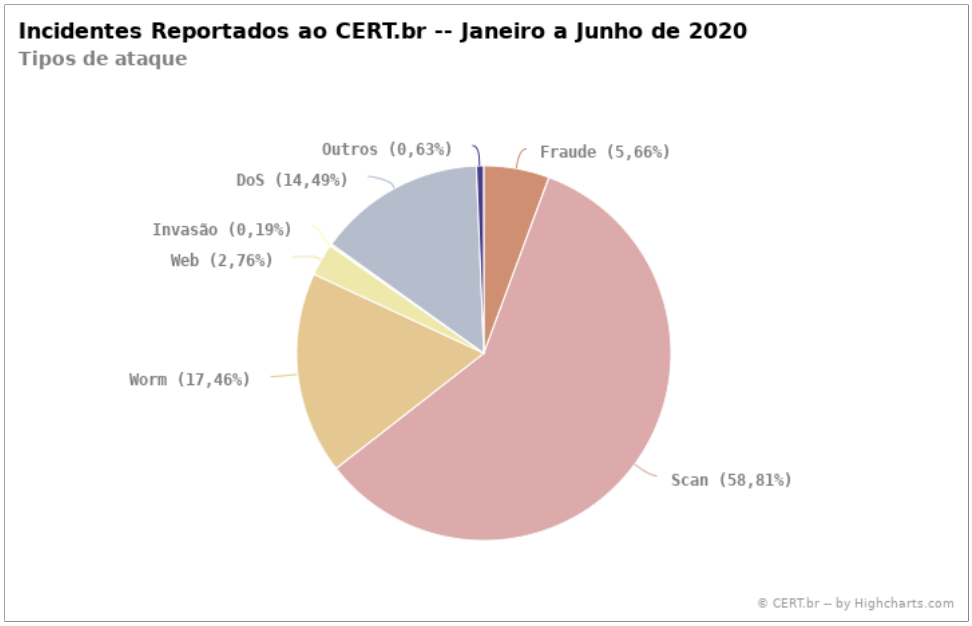

Figura 4 - Tipos de ataque - Fonte: CERT.br disponível em https://www.cert.br/stats/incidentes/2020-jan-jun/tipos-ataque.html acesso em 13/05/2021.

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.

1.15. 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.

1.16. A figura 5 relaciona os scans reportados por porta .

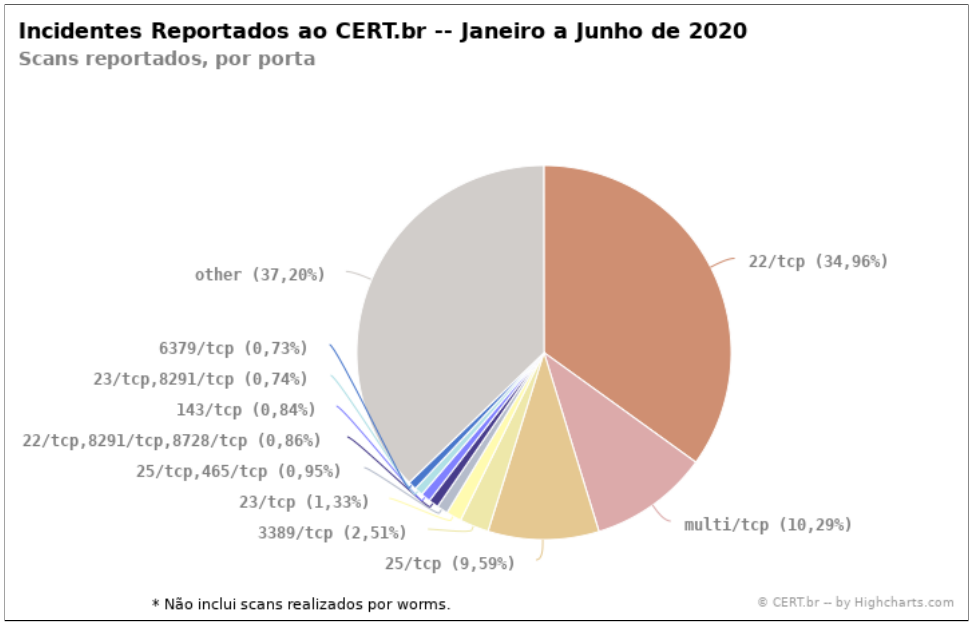

Figura 5 - Scans reportados, por porta - Fonte: CERT.br disponível em https://www.cert.br/stats/incidentes/2020-jan-jun/scan-portas.html acesso em 13/05/2021.

1.17. Na Figura 6 são apresentadas as Notificações sobre equipamentos participando em ataques DoS.

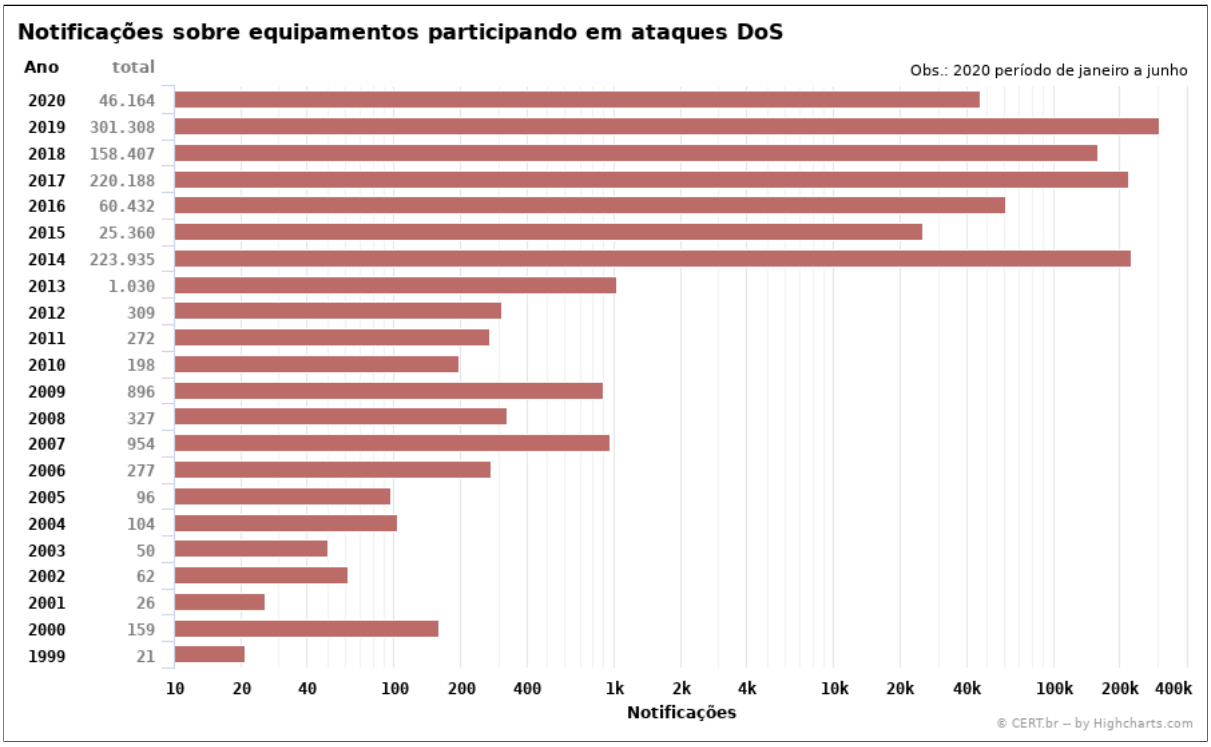

Figura 6 - Notificações sobre equipamentos participando em ataques DoS - Fonte: CERT.br disponível em https://www.cert.br/stats/incidentes/2020-jan-jun/dos.html acesso em 13/05/2021.

1.18. Na Figura 7 são apresentadas as Tentativas de Fraudes.

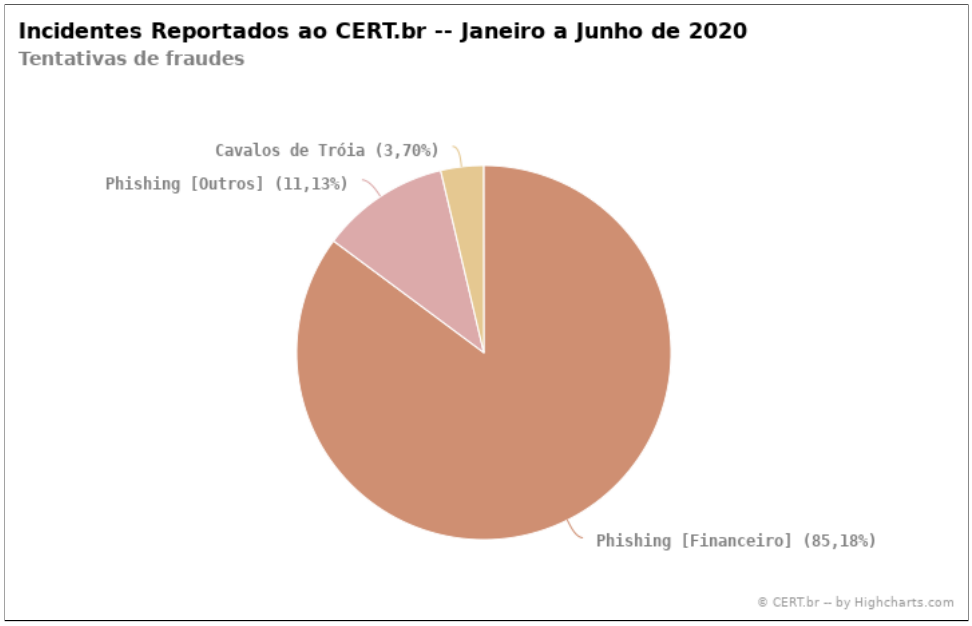

Figura 7 - Tentativas de fraudes - Fonte: CERT.br disponível em https://www.cert.br/stats/incidentes/2020-jan-jun/fraude.html acesso em 13/05/2021.

1.19. Na Figura 8 são apresentados os totais de incidentes reportados ao CERT.BR.

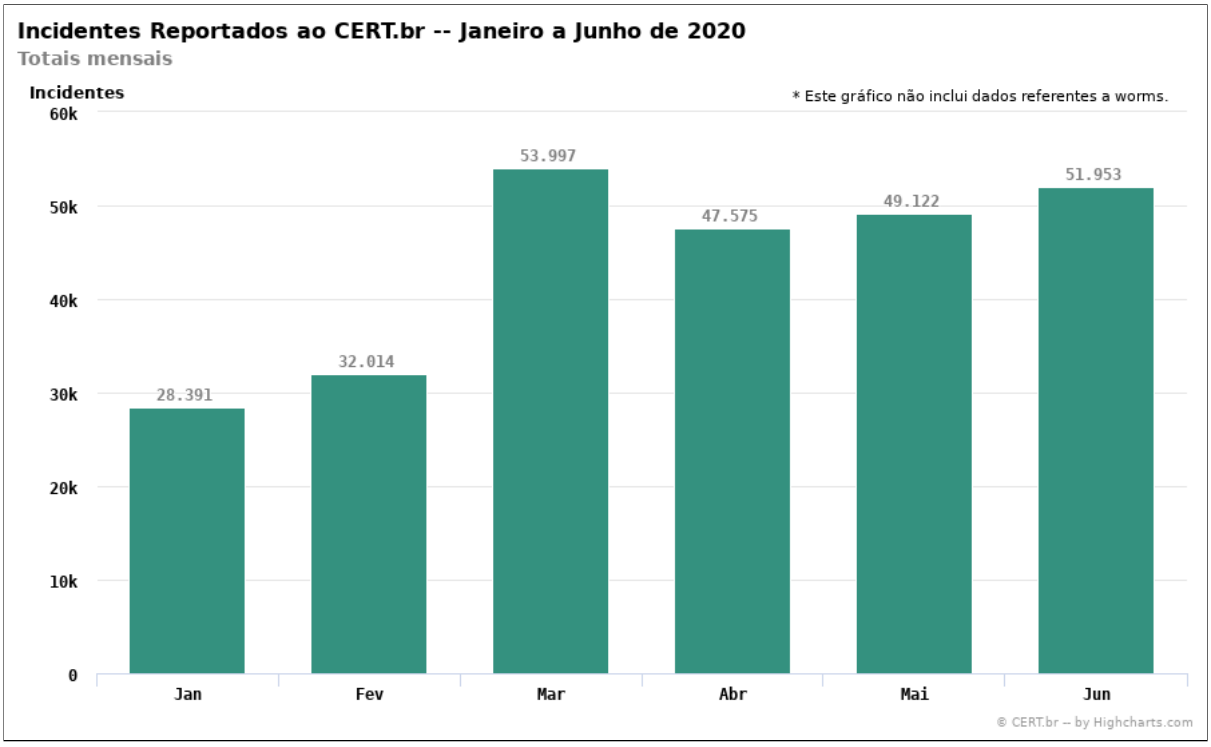

Figura 8 - Totais mensais - Fonte: CERT.br disponível em https://www.cert.br/stats/incidentes/2020-jan-jun/total-mensal.html acesso em 13/05/2021.

1.20. Na Figura 9 são apresentados os totais de incidentes reportados ao CERT.BR, considerando a origem do ataque.

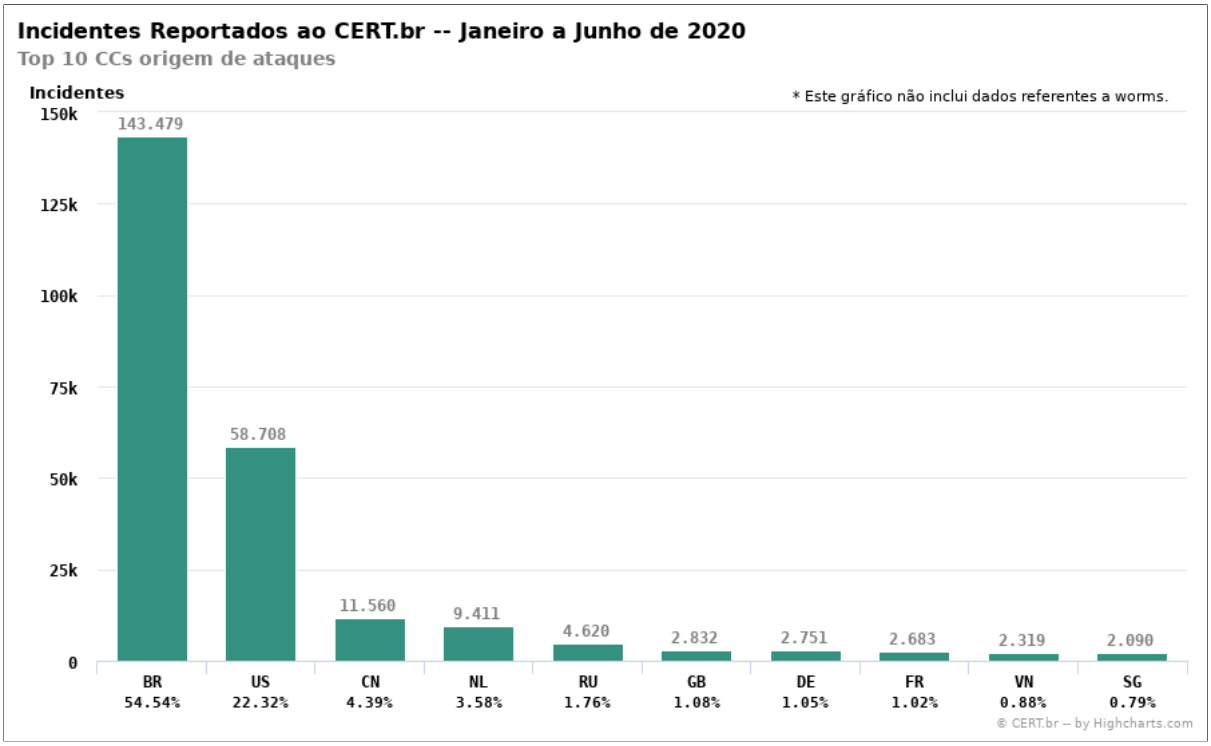

Figura 9 - Top 10 Country Codes origem de ataques - Fonte: CERT.br disponível em https://www.cert.br/stats/incidentes/2020-jan-jun/top-cc.html acesso em 13/05/2021.

1.21. Diante desse cenário complexo e misto, a contratação de uma equipe dedicada ao monitoramento, prevenção e reposta a incidentes de segurança se torna imprescindível.

1.22. É possível perceber a função de um *Security Operations Center - SOC,* a partir do trecho extraído da brochura do *Kaspersky for Security Operations Center,* conforme a seguir:

> "As businesses learn to better protect themselves, criminals are simultaneously devising increasingly sophisticated techniques to penetrate their security barriers. Attracted by the unprecedented financial rewards that cyberattacks can deliver, growing numbers of threat actors are actively seeking and targeting undiscovered security flaws. In this environment, many organizations are establishing Security Operations Centers (SOCs) to combat security issues as they arise, providing a swift response and a decisive resolution." (https://media.kaspersky.com/en/business-security/enterprise/brochure-soc-powered-by-kl-eng.pdf)

> "À medida que as empresas aprendem a se proteger melhor, os criminosos estão simultaneamente planejando cada vez mais técnicas sofisticadas para penetrar em suas barreiras de segurança. Atraídos pelas recompensas financeiras sem precedentes que os ciberataques podem oferecer, um número crescente de atores de ameaças está ativamente buscando e direcionando falhas de segurança não descobertas. Nesse ambiente, muitas organizações estão estabelecendo Centrais de Operações de Segurança SOCs para combater os problemas de segurança à medida que surgem, fornecendo uma resposta rápida e uma resolução decisiva." (tradução livre)

1.23. Partindo dessa percepção, um SOC (utilizaremos o acrônimo em inglês), é um ente centralizado com a função de monitoramento contínuo de ameaças, análise dessas ameaças, bem como, para prevenção e mitigação de incidentes de cibersegurança.

1.24. A crescente demanda pela eficiência na segurança da informação fez com que as organizações passassem a lidar com o assunto de forma mais estratégica. A formação de um Blue Team e um Red Team é um bom exemplo disso.

1.25. Com atribuições específicas, as equipes promovem um trabalho de cibersegurança em nível mais elevado nas empresas. Cada uma delas tem sua importância e o alinhamento entre as duas traz inúmeros benefícios.

1.26. O Red Team é formado com o objetivo de realizar testes de ciberataque na empresa. Estamos falando de profissionais com alto conhecimento sobre as principais ameaças e ataques existentes, sendo capazes de simular tentativas de penetrar na rede e ou sistemas. Com isso, eles se tornam capazes de identificar vulnerabilidades e, consequentemente, eliminá-las.

1.27. Resumidamente, eles assumem o papel de alguém que tentaria atacar a empresa — o que geralmente pode envolver a contratação de alguém de fora, sem o olhar acostumado àquele ambiente. Os ataques podem envolver engenharia social para enviar phishing aos funcionários, por exemplo.

1.28. O papel do Blue Team é justamente se opor aos ataques, inclusive aqueles ensaiados pelo Red Team. Assim, ele deve desenvolver estratégias para aumentar as defesas, modificando e reagrupando os mecanismos de proteção da rede para que eles se tornem mais fortes.

1.29. Um time desse tipo deve ter também um alto nível de conhecimento sobre a natureza das ameaças da rede. Entretanto, eles devem ser capazes não só de eliminar brechas, mas de reformular a infraestrutura de defesa como um todo.

1.30. Podemos extrair o que se entende por Blue Team, Red Team e Purple Team a partir das definições da autoridade mundial no tema, SANs:

- Blue Team:

> "[...] focus is to defend the organization from digital/cyber attacks. In truth, while everything that improves the defensive security posture could be construed as Blue Team, there is an overt emphasis on discovering and defending against attacks". (https://wiki.sans.blue/#!index.md)

> "[...] focado em defender a organização de digital/cyber ataques. Na verdade, enquanto tudo que promova a postura defensiva de segurança possa ser entendida como Blue Team, há uma ênfase na descoberta e defesa contra esses ataques. " (Tradução Livre)

- Red Team:

> "[...] would be those playing the role of the adversary. [...] So Red Team acts as Offense and Blue Team as Defense." (https://wiki.sans.blue/#!index.md)

"[...] serial aqueles que atuam o papel de adversários. [...] Então o Red Team atua como ofensiva e Blue Tema como defensiva." (Tradução Livre)

- Purple Team:

"[...] They typically report to a as a "third" team; think of it as a concept aimed at bringing the red and blue teams together to create purple team exercises. Red teams and blue teams should be encouraged to work as a joint team, to share insights beyond just reporting, to create a strong feedback loop, and to look for detection and prevention controls that can realistically be implemented for immediate improvement. " (https://www.sans.org/purple-team?msc=ptcourse-faq-lp)

"[...] Eles se denominam como o 'terceiro' time; pense nisso como um conceito que visa reunir as equipes vermelhas e azuis para criar exercícios de purple team. Equipes vermelhas e azuis devem ser incentivadas a trabalhar como uma equipe conjunta, para compartilhar ideias além somente gerar relatórios, a criar um forte ciclo de feedback, e a procurar controles de detecção e prevenção que possam ser implementados realisticamente para melhoria imediata."

1.31. A SANS - System Administration, Networking and Security é uma empresa especializada em segurança da informação e treinamento de cybersegurança. Definição o que é SANS :

SANS is the most trusted and by far the largest source for cybersecurity training in the world. We offer training through several delivery methods including OnDemand (self paced) and instructor-led both Live Online (virtual) and In-Person. Our cybersecurity courses are developed by industry leaders in numerous fields including network security, digital forensics, offensive operations, cybersecurity leadership, industrial control systems, and cloud security. Courses are taught by real-world practitioners who are the best at ensuring you not only learn the material, but that you can apply it immediately when you return to the office. In addition to top-notch training, we offer certification via GIAC, an affiliate of the SANS Institute featuring over 35 hands-on, technical certifications in cyber security. We offer a Master's Degree, graduate and undergraduate certificate programs through SANS Technology Institute, as well as numerous free resources including newsletters, whitepapers and webcasts.

SANS é a mais confiável e de longe a maior fonte de treinamento em segurança cibernética do mundo. Oferecendo treinamento por meio de vários métodos de entrega, incluindo OnDemand (individualizado) e ministrado por instrutor ao vivo online (virtual) e presencial. Os cursos de segurança cibernética são desenvolvidos por líderes do setor em diversos campos, incluindo segurança de rede, análise forense digital, operações ofensivas, liderança em segurança cibernética, sistemas de controle industrial e segurança em nuvem. Os cursos são ministrados por profissionais do mundo real que são os melhores em garantir que você não apenas aprenda o material, mas também que possa aplicá-lo imediatamente ao retornar ao escritório. Além do treinamento de alto nível, oferece certificação via GIAC, uma afiliada do SANS Institute com mais de 35 certificações técnicas práticas em segurança cibernética. Oferece programas de certificado de mestrado, pós-graduação e graduação por meio do SANS Technology Institute, bem como diversos recursos gratuitos, incluindo boletins, white papers e webcasts.

1.32. Considerando as definições acima inseridas para Blue Team, Red Team e Purple Team, podemos afirmar, simplificadamente que o Blue Team é o elo de defesa e sua operação, o Red Team seria o ente de ataque o qual checa as defesas implementadas pelo Blue Team. O Purple Team seria o esforço coordenado envolvendo os dois grupos para examinar novas técnicas de invasão, desenvolver defesas melhoradas e enfrentar ataques de equipe vermelha.

1.33. De acordo com o modelo de arquitetura de segurança adaptativa proposto pelo Gartner, uma organização somente obterá sucesso na luta contra os crimes cibernéticos se seu SOC for capaz de predizer, prever, detectar e responder efetivamente as ameaças, conforme podemos visualizar na figura 10 :

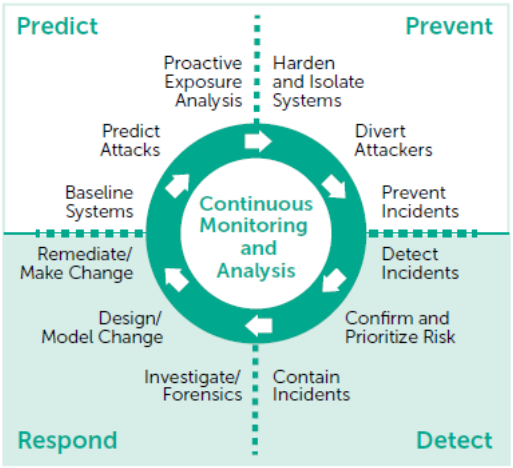

Figura 10 - Gartner, Designing an Adaptive Security Architecture for Protection From Advanced Attacks, February 2014. (retirado da brochura do Kaspersky for Security Operations Center)

1.34. Levando esse modelo em consideração o Ministério da Justiça e Segurança Pública objetiva contratar um serviço o qual contemple as equipes de Blue Team, Red Team e Purple Team, de forma 24h por dia e 7 dias por semana para o monitoramento e defesa de primeiro nível, em horário comercial para o suporte de segundo nível, e sob demanda para atividades de Red Team.

1.35. Busca-se com o presente Estudo Técnico Preliminar demonstrar a necessidade que o Ministério da Justiça e Segurança Pública possui em contratar um serviço de SOC, assim como, identificar as necessidades de negócio, tecnológicas, bem como, os demais requisitos necessários e suficientes à escolha dessa solução de TIC. Os quais serão apresentados na tabela 3.

Tabela - 3: Identificação das necessidades de negócio, tecnológicas e demais requisitos

Identificação das necessidades de negócio		**Alinhamento ao PDTIC 2021**
1	Reduzir riscos associados a perda de dados, comprometimento dos sistemas, imagem institucional do ministério e do governo brasileiro	A0077 - Contratação de serviço de SOC
2	Melhorar a assertividade nos investimentos em soluções de segurança da informação efetivamente necessárias	
3	Reduzir os riscos associados aos ativos críticos	

4	Aumentar a maturidade de segurança da informação
5	Economizar tempo e reduzir a complexidade, identificando e saneando a segurança da informação antes da implantação dos sistemas
6	Aumentar a segurança dos ativos reduzindo ou eliminando os pontos cegos
7	Desenvolver relatórios e apurações especiais, painéis gerenciais para apoio à tomada de decisão dos gestores, quanto ao risco da instituição.
8	Garantir a segurança da informação e comunicação no âmbito do Ministério da Justiça e o sigilo das informações dos cidadãos
9	Implantar e fortalecer as equipes de tratamento de incidentes de segurança
10	Definir e implantar mecanismos mais efetivos de responsabilização de colaboradores por eventos relacionados à Segurança da Informação e Comunicação
11	Contribuir para o aumento da capacidade de resiliência dos ativos de informação e das infraestruturas críticas
12	Instituir práticas de auditoria de Segurança da Informação e Comunicações
13	Manter uma equipe ininterrupta de resposta rápida e efetiva a ataques e incidentes de segurança da informação
14	Implantar o estado da arte em termos de segurança da informação
15	Multiplicar o efetivo na área de segurança da informação
16	É necessário que a solução leve em consideração a segurança no serviço em nuvem, garantindo a privacidade e a segurança dos dados

Identificação das necessidades tecnológicas	
1	Monitorar ininterruptamente de forma automatizada a sensibilidade dos dados de acordo com a Lei Geral de Proteção de Dados
2	Monitorar ininterruptamente de forma automatizada os recursos de TI do Ministério da Justiça e Segurança Pública e suas unidades
3	Implantar ferramenta de gerenciamento e correlação de eventos de segurança - SIEM
4	Implantar tecnologias de prevenção, detecção e resposta rápida a incidentes de segurança da informação
5	Prover análise interna e externa dos ativos de TIC, com escopo em segurança da informação, a partir de ferramentas do Ministério da Justiça e Segurança Pública ou próprias
6	Implantar painel em tempo real que demonstre a situação atual em termos de risco e segurança da informação do Ministério da Justiça e Segurança Pública
7	Prover relatórios *Post Mortem* dos ataques à infraestrutura do Ministério da Justiça e Segurança Pública
8	Sugerir melhorias na infraestrutura de TIC do ministério, com escopo em segurança da informação, indicando os riscos quando não implementadas

Demais requisitos necessários e suficientes à escolha da solução de TIC	
1	Atuar de forma sincronizada com o Network Operations Center - NOC
2	Manter equipe 24 horas por dia e 7 dias por semanas de forma ininterrupta provendo os serviços SOC e **Blue Team** ao Ministério da Justiça e Segurança Pública
3	Prover equipe sob demanda da Coordenação de Riscos e Segurança da informação para atividades de SOC relacionadas a **Red Team.**
4	Prover equipe de **Purple Team** para coordenação das equipes de **Blue Team** e **Red Team**.

2. **ESTIMATIVA DA DEMANDA – QUANTIDADE DE BENS E SERVIÇOS**

2.1. O Ministério da Justiça e Segurança Pública possui a necessidade de contratação dos seguintes serviços os quais serão detalhados e motivados separadamente conforme a seguir:

2.1.1. - **Serviço de *Security Operations Center* - SOC** destinado a ser o ente central da estrutura de monitoramento e controle dos incidentes de segurança da informação, operando 24h por dia e 7 dias por semana para suporte de primeiro nível na triagem, investigação e resposta a incidente.

2.1.2. - **Serviço de Tratamento e Resposta aos Incidentes Cibernéticos - CSIRT - Blue Team** responsável por atuar sob o comando do SOC quando da ocorrência de incidentes de segurança da informação ou sempre que solicitado visando contribuir com a melhoria da segurança da informação, sendo 24h por dia e 7 dias por semana para apoio ao suporte de primeiro nível e demais níveis realizado pelo SOC e em horário comercial, sendo 12h por dia 5 dias por semana, para suporte sob demanda.

2.1.3. - **Serviço de Teste de Invasão - Red Team** responsável por realizar testes independentes de penetração e análise de segurança mediante demanda da Coordenação de Riscos e Segurança da Informação - CRS.

2.1.4. Para um melhor entendimento foi definido um diagrama de relacionamento dos serviços e seus respectivos componentes, objeto da presente contratação, com os demais serviços da DTIC adaptado de acordo com o Framework para implementar um SOC de Schinagl, S., Schoon, K., & Paans, R. (2015). A framework for designing a security operations centre (SOC). Proceedings of the Annual Hawaii International Conference on System Sciences, 2015-March, 2253–2262. https://doi.org/10.1109/HICSS.2015.270.

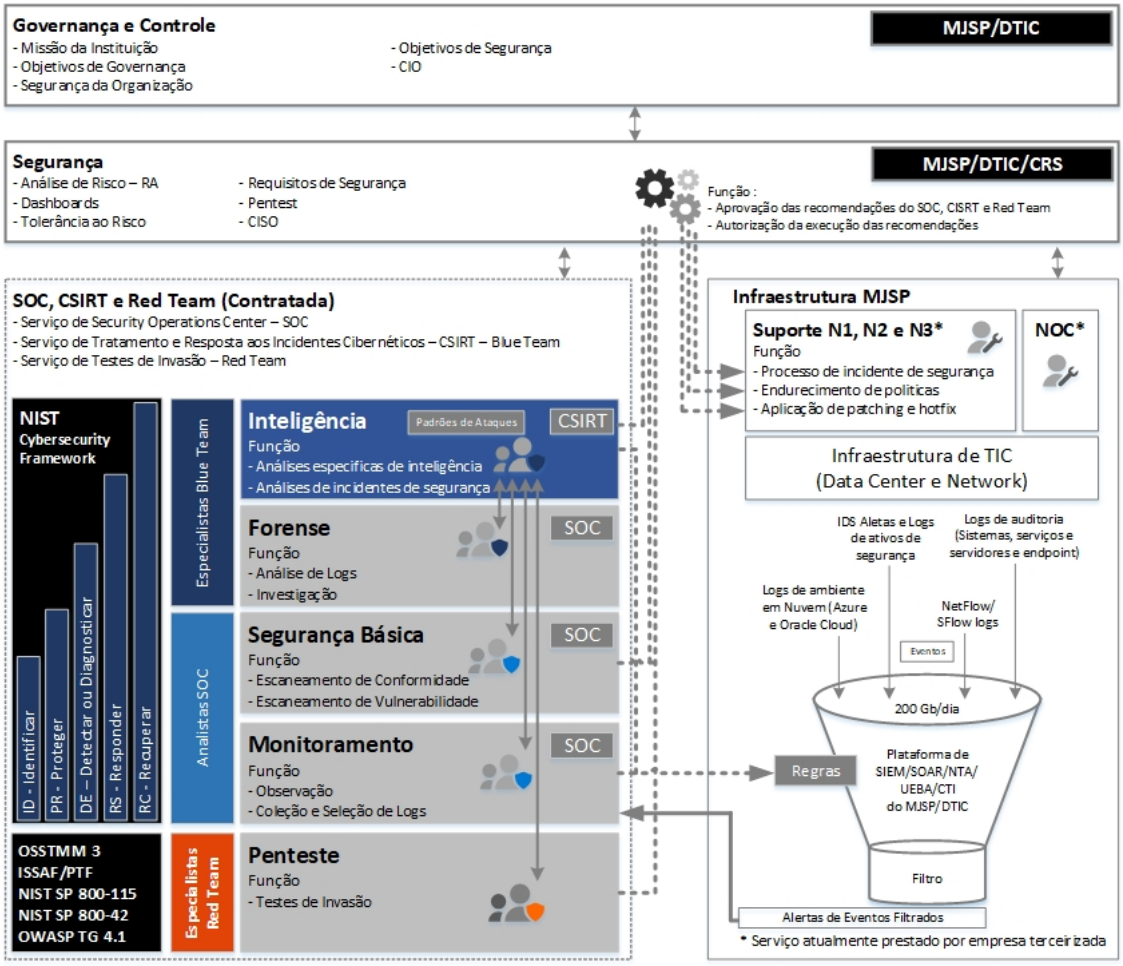

Figura 11 - Diagrama de relacionamento dos serviços e seus respectivos componentes com os demais serviços da DTIC.

2.1.5. Na Figura 11 é apresentado o diagrama de interação, para a presente contração, entre o MJSP representado pela DTIC e a CRS com o papel de gestores estratégicos, táticos e operacionais com a Infraestrutura de TIC do MJSP e os serviços de SOC, de Tratamento e Resposta a Incidentes Cibernéticos e de Testes de Invasão.

2.1.5.1. A DTIC com o papel de Governança e Controle atuando na gestão estratégica realizando a conformidade e função:

2.1.5.1.1. Missão da Instituição;

2.1.5.1.2. Objetivos de Governança;

2.1.5.1.3. Segurança da Organização;

2.1.5.1.4. Objetivos de Segurança;

2.1.5.1.5. CIO (*Chief Information Officer*);

2.1.5.2. A CRS com o papel de Segurança atuando na gestão tática e operacional e realizando conformidade e funções:

2.1.5.2.1. Análise de Risco;

2.1.5.2.2. Dashboards;

2.1.5.2.3. Tolerância ao Risco;

2.1.5.2.4. Requisitos de Segurança;

2.1.5.2.5. Pentest;

2.1.5.2.6. CISO (*Chief Information Security Officer*);

2.1.5.2.7. Intermediando as ações de aprovação e autorizações das requisições entre o CSIRT e SOC com a Infraestrutura de TIC do MJSP;

2.1.5.3. O Serviços de SOC, CSIRT e Red Team executando de forma colaborativa e integrada e conforme o framework de segurança cibernética (CSF) do NIST para CSIRT e SOC, bem como OSSTMM 3, ISSAF/PTF, NIST SP 800-115 e 800-42 e OWASP TB 4.1 para o Red Team, os papeis:

2.1.5.3.1. Inteligência - através da equipe de especialistas Blue Team do CSIRT com as funções de Análise especificas de inteligência e de incidentes de segurança de acordo com os Padrões de Ataques;

2.1.5.3.2. Forense - através da equipe de especialistas Blue Team com as funções de Análise de Logs e Investigação;

2.1.5.3.3. Segurança Básica - através da equipe de analistas do SOC com as funções de Escaneamento de conformidade e vulnerabilidade;

2.1.5.3.4. Monitoramento - através da equipe de analistas do SOC com as funções de Observação e Coleção e Seleção de Logs dos alertas de eventos e realizando a ajustes devidos de regras da Plataforma de SIEM/SOAR/NTA/UEBA/CTI do MJSP.

2.1.5.3.5. Pentest - através da equipe de especialistas Red Team com a função de Testes de invasão.

2.1.5.4. Infraestrutura de TIC do MJSP executando a sustentação do parque computacional com os papeis e componentes:

2.1.5.4.1. Suporte N1, N2 e N3 - através de equipe técnica terceirizada com a realização das funções do processo de incidente de segurança, endurecimento de políticas e aplicação de patching e hotfix, aprovadas pela CRS, de requisições feitas pela CSIRT, SOC e Red Team.

2.1.5.4.2. NOC - através de equipe técnica (atualmente terceirizada) com a monitoramento da infraestrutura de TIC.

2.1.5.4.3. Plataforma de SIEM/SOAR/NTA/UEBA/CTI do MJSP com um consumo aproximado de 200 GB/dia de eventos sendo:

2.1.5.4.3.1. Logs de ambientes em Nuvem (Azure e Oracle Cloud);

2.1.5.4.3.2. IDS Alertas e Logs de ativos de segurança;

2.1.5.4.3.3. NetFlow/ SFlow Logs;

2.1.5.4.3.4. Logs de auditoria (Sistemas, serviços, servidores e endpoint);

2.2. **Serviço de Security Operations Center - SOC**

2.2.1. O SOC funcionará de forma ininterrupta 24 horas por dia e 7 dias por semana realizando as seguintes atividades, não se restringindo somente a elas:

2.2.1.1. Monitoramento continuo e análise, predizendo, prevendo, detectando e respondendo efetivamente as ameaças de todos incidentes de segurança.

2.2.1.2. Gerar painéis dinâmicos e em tempo real da situação atual de segurança do Ministério informando através de um score o nível de segurança.

2.2.1.3. Atuar como suporte de primeiro nível aos incidentes de segurança identificando, classificando, interrompendo, catalogando todas as tentativas de ataque aos sistemas e à infraestrutura do ministério.

2.2.1.4. Demandar ao NOC ou ao Suporte N1, N2 e N3 da infraestrutura de TIC do Ministério medidas a serem tomadas para evitar ou conter incidente.

2.2.1.5. Atuar no sentido de interromper um incidente quando da inoperância do NOC ou suporte N1, N2 e N3, dentro dos serviços autorizados em reunião inicial entre a CONTRATANTE e CONTRATADA, os quais o SOC poderá agir em substituição ao NOC. Todas as ações tomadas devem ser posteriormente repassadas ao NOC ou suporte da infraestrutura e a CRS.

2.2.1.6. Outros serviços os quais o SOC atuará em substituição ao NOC, poderão ser definidos durante a vigência do contrato, por meio de reuniões entre a CONTRATANTE e a CONTRATADA

2.2.1.7. Atuar em harmonia com o NOC do ministério.

2.2.1.8. Prestar o serviço de SOC realizando a **detecção, triagem, investigação e resposta a incidente** de eventos utilizando Plataforma de SIEM/SOAR/NTA/UEBA/CTI do Ministério que possui as seguintes funções:

2.2.1.8.1. Camada de Automação:

2.2.1.8.1.1. Orquestração, Automação e Resposta de Segurança (Security Orchestration, Automation, and Response - SOAR);

2.2.1.8.2. Camada de Análise e Correlacionamento:

2.2.1.8.2.1. Monitoramento de estação de trabalho (Endpoint Detection and Response - EDR);

2.2.1.8.2.2. Análise de Tráfego de Rede (Network Traffic Analysis - NTA);

2.2.1.8.2.3. Análise de Comportamento de Usuário (User Entity and Behavior Analytics - UEBA);

2.2.1.8.2.4. Análise de Inteligência de Ameaças Cibernéticas (Cyber Threat Intelligence - CTI);

2.2.1.8.3. Camada de coleta:

2.2.1.8.3.1. Informações de segurança e gestão de eventos (Security Information and Event Management - SIEM).

2.2.1.9. Configurar, monitorar e operar a Plataforma de SIEM/SOAR/NTA/UEBA/CTI do Ministério.

2.2.1.10. Caso as ferramentas de propriedade do Ministério não atendam a completa execução dos serviços objeto da presente contratação a contratada poderá adotar solução tecnológica complementar em termo de hardware e software.

2.2.1.11. A CONTRATADA poderá utilizar soluções de hardware e software proprietárias desde que previamente autorizadas pelo CONTRATANTE, arcando a CONTRATADA com todos os custos diretos e indiretos inerentes a utilização de solução tecnológica e seus licenciamentos necessários.

2.2.1.12. Garantir a implementação do Modelo Adaptativo de Arquitetura de Segurança para Proteção de ataques avançados da Gartner exibido na figura 10.

2.2.2. Prevê-se que o SOC funcionará como o centralizador de todas as informações de segurança da informação e suporte de primeiro nível, por isso, a necessidade de seu funcionamento ser ininterrupto. O dimensionamento da equipe do SOC será a cargo da contratada em quantitativo mínimo que garanta o monitoramento ininterrupto de seu funcionamento, a qualidade das informações prestadas e estar apta a atuar no estado da arte em termos de segurança da informação, assim como cumprir os Acordos de Nível de Serviço determinados.

2.3. **Serviço de Tratamento e Resposta aos Incidentes Cibernéticos - CSIRT - Blue Team**

2.3.1. O **Blue Team** funcionará de forma ininterrupta associado ao SOC para atividades de apoio ao suporte de primeiro nível e contenção de ataques, bem com, para atividades e suporte de segundo nível em diante.

2.3.2. No que diz respeito ao time de primeiro nível, este atuará associado ao SOC de forma ininterrupta uma vez que o nível de qualificação para essas atividades são inferiores aos de segundo nível.

2.3.3. Considerando que a equipe de especialistas de atividades e suporte em segundo nível em diante exige uma qualificação elevada e visando uma redução dos custos na contratação, o Ministério estima que a necessidade por esse tipo de profissional poderá ser utilizada em horário comercial, quando em necessidade urgente devido a um ataque, ou sob demanda fora do horário comercial.

2.3.4. Destacam-se algumas atividades que a equipe de especialistas Blue Team será responsável, não se restringindo somente a estas:

2.3.4.1. Apoiar na atividade de configuração, manutenção e operação a Plataforma de SIEM/SOAR/NTA/UEBA/CTI do Ministério, a partir das informações monitoradas pelo SOC realizando a correlação dos eventos e configuração de suas regras de inteligência.

2.3.4.2. Atuar como suporte de segundo nível em diante.

2.3.4.3. Defender o ministério nos incidentes de segurança.

2.3.4.4. Promover a melhoria da segurança da informação do Ministério.

2.3.4.5. Fazer cessar ou interromper os ataques à infraestrutura do Ministério.

2.3.4.6. Atuar em harmonia com o NOC do Ministério.

2.3.4.7. Atuar sob orientação do **CRS** quando de análises realizadas pelo **Red Team**.

2.3.4.8. Sugerir melhorias na segurança da informação do ministério a partir das melhores práticas internacionais.

2.3.4.9. Prover a transferência de conhecimento ao corpo técnico da CRS de sistemas, produtos e soluções utilizados com o fornecimento de perfil de acesso para a supervisão dos serviços prestados.

2.3.4.10. Implantar, configurar e suportar as tecnologias necessárias ao melhoramento da segurança da informação do Ministério.

2.3.4.11. Prover relatórios sob demanda.

2.3.4.12. Manter em funcionamento o painel de segurança da informação com as informações definidas de indicadores de performance e níveis de serviços acordados.

2.3.5. Analisar, remediar, conter e documentar os eventos de segurança da informação que foram transformados em um incidente de segurança da informação. Tal serviço deverá ser executado obedecendo os frameworks de segurança cibernética do NIST CSF (Cybersecurity Framework) e boas práticas de mercado ou framework definido pelo Ministério.

2.3.6. Monitoramento da rede sociais, Dark Web e Deep Web com ferramentas adequadas para monitoramento de informações sensíveis e de interesse do Ministério a respeito de segurança da cibernética.

2.3.7. Apoiar a CRS na avaliação, elaboração e revisão de relatórios segurança e privacidade.

2.4. **Serviço de Teste de Invasão - Red Team**

2.4.1. O **Red Team** funcionará sob demanda da CRS sem o conhecimento dos outros entes.

2.4.2. Muitas vezes pelo fato de uma equipe estar diretamente associada aos eventos de monitoramento, configuração e suporte, algumas brechas deixam de ser observadas, não por descuido, mas por uma "visão de túnel". Diante disso, torna-se crucial que exista uma equipe que possa ter uma visão externa ao processo e é nesse cenário que o **Red Team** torna-se essencial.

2.4.3. Destacam-se algumas atividades que o **Red Team** será responsável, sob demanda, não se restringindo somente a estas:

2.4.3.1. Infligir ataques a infraestrutura de segurança interna e externa de rede e sistemas do ministério de modo não destrutivo.

2.4.3.2. Realizar tentativas de Data Exfiltration, Internal & External Reconnissance, ShadowMap Scan, Vulnerability Assessment, Social Engineering, Exploitaion, Pivoting / Lateral Movements, entre outros, a rede e aos sistemas do ministério, obedecendo o framework de segurança MITRE ATT&CK que utiliza base global de conhecimento das táticas, técnicas e procedimentos (TTP's) utilizados por atacantes para avaliar a efetividade dos controles de segurança.

2.4.3.3. Gerar relatórios detalhado das tentativas.

2.4.3.4. Sugerir após o ataque melhorias na infraestrutura a serem implementadas pela equipe de Infraestrutura de TIC do Ministério com o apoio da equipe de **Blue Team**, após as devidas aprovações e autorizações da CRS.

2.4.4. O time de Red Team deve ser independente do **Blue Team**. Além disso, os dias de suas incursões não devem ser de conhecimento da equipe de defesa.

2.5. Os serviços citados anteriormente justificam-se devido ao diminuto corpo técnico do Ministério da Justiça e Segurança Pública, visando a não interrupção e o tratamento efetivo das descobertas do Red Team.

3. ANÁLISE DE SOLUÇÕES

3.1. IDENTIFICAÇÃO DAS SOLUÇÕES

3.1.1. Foram identificadas 4 possíveis soluções, conforme relacionadas na tabela 4.

Tabela 4 - Possíveis soluções

Id	Descrição da Solução
1	Realização dos Serviços de SOC, Blue Team, Red Team e Purple Team pelos servidores lotados na Coordenação de Riscos e Segurança do Ministério da Justiça e Segurança Pública
2	Ampliação da Contratação do Network Operations Center - NOC
3	Aquisição de Equipamentos de Segurança e/ou Softwares
4	Contratação como Serviço

3.2. ANÁLISE COMPARATIVA DE SOLUÇÕES

3.2.1. Na tabela 5 é realizada uma análise comparativa de soluções, que foram mapeadas no MJSP.

Tabela 5 - Análise Comparativa de soluções

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
	Solução 4	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	
	Solução 4			X

Requisito	Solução	Sim	Não	Não se Aplica
A Solução é composta por software livre ou software público? (quando se tratar de software)	Solução 1			X
	Solução 2			X
	Solução 3		X	
	Solução 4			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
	Solução 4			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
	Solução 4			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
	Solução 4			X

4. **REGISTRO DE SOLUÇÕES CONSIDERADAS INVIÁVEIS**

4.1. **Solução 1**

4.1.1. **Descrição:** A solução um considera a utilização do corpo de servidores lotados na Coordenação de Risco e Segurança - CRS para desempenhar as tarefas de SOC, Blue Team, Red Team e Purple Team.

4.1.2. **Justificativa:** Segundo dados do Portal de Gestão de Pessoas, disponível na intranet em maio de 2021, a força de trabalho do Ministério da Justiça e Segurança Pública é de 1.333 pessoas, sendo que destas apenas 410 são do quadro próprio, ou seja, correspondem ao ativo permanente do órgão, conforme apresentado na figura 12.

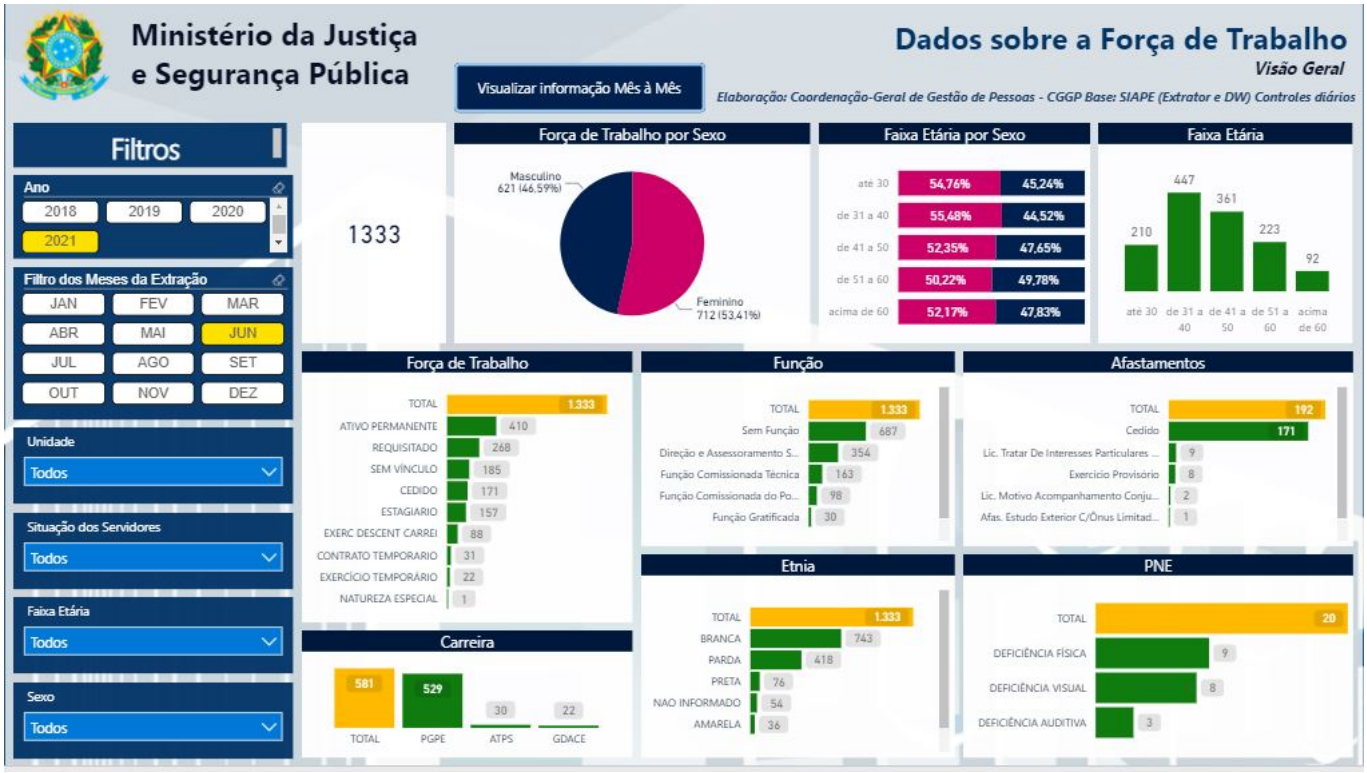

Figura 12 - Força de trabalho do MJSP, Fonte: Portal Gestão de Pessoas, disponível em https://justicagovbr.sharepoint.com/sites/intra-CGGP/SitePages/For%C3%A7a-de-Trabalho.aspx, acesso em 09/06/2021.

4.1.3. Na Diretoria de Tecnologia da Informação e Comunicação são 78 pessoas, sendo que destas apenas 8 são do quadro de ativo permanente, conforme apresentado na figura-13.

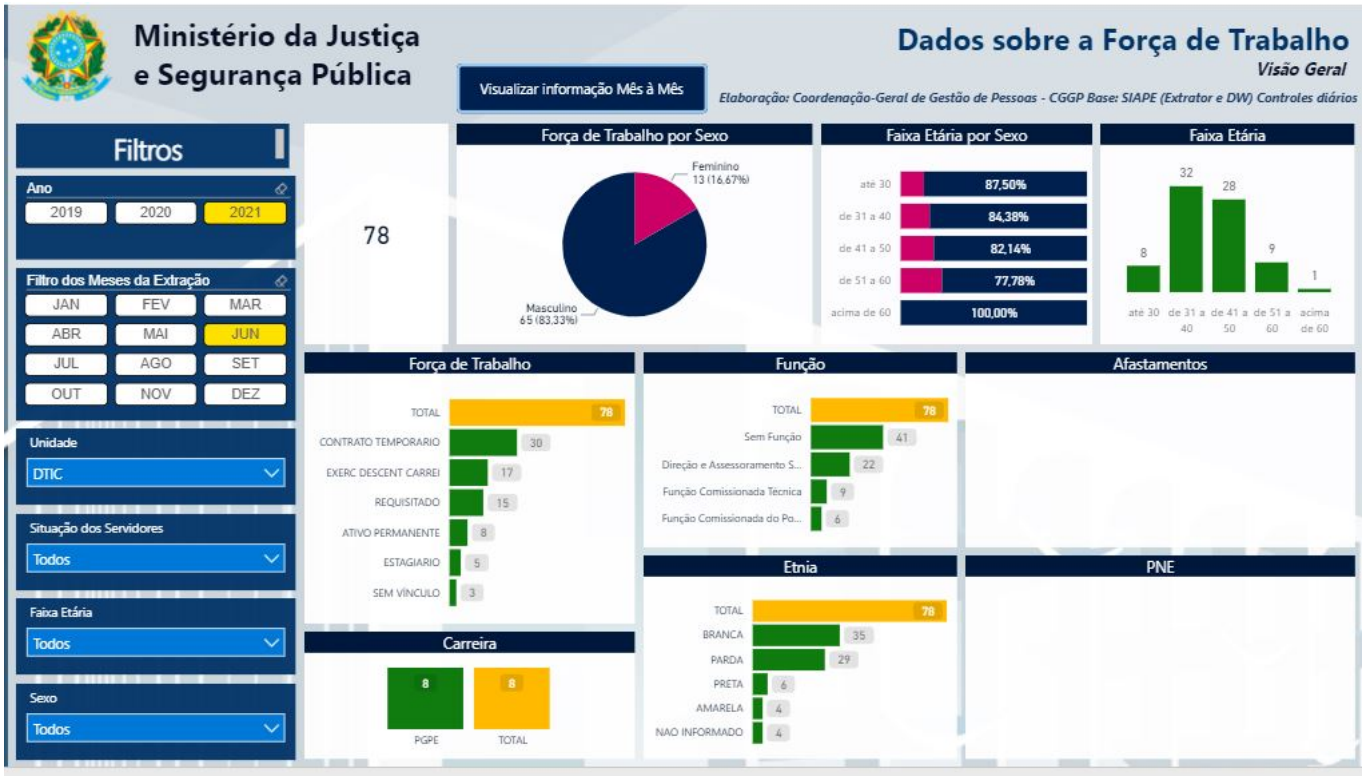

Figura 13 - Força de trabalho da DTIC, Fonte: Portal Gestão de Pessoas, disponível em **https://justicagovbr.sharepoint.com/sites/intra-CGGP/SitePages/For%C3%A7a-de-Trabalho.aspx**, acesso em 09/06/2021.

4.1.4. Baseado nas recomendações da Gartner, o estudo "Como planejar, projetar, operar e evoluir um SOC" publicado em 6 de setembro de 2018 (https://www.gartner.com/document/3889122?ref=cust_reco_sdemail&docType=RESEARCH), um dos pré-requisitos para implantar o SOC:

> *"um SOC 24/7 interno exigirá uma equipe de oito a 12 pessoas no mínimo. Se não houver esses recursos, comece seu planejamento de SOC com uma opção híbrida que depende substancialmente de um ou mais provedores de serviços, em particular para funções que precisam de cobertura 24 horas por dia, 7 dias por semana."*

4.1.5. Baseado nas recomendações da Gartner, considerando o quantitativo de pessoas do quadro de ativo permanente na Diretoria de Tecnologia e Comunicação, conforme item 4.1.3, e considerando o quantitativo de ativos instalados no MJSP, de acordo com Relatório sobre Informações da Infraestrutura do MJSP SEI (14628328), a criação de um SOC com pessoal interno não seria viável.

4.1.6. Verifica-se que o atual modelo de contratações, por meio a compra de produtos e a contratação de serviços de operação, não são suficientes para fazer frente à velocidade com que surgem novos tipos de ameaças, e principalmente, a velocidade com que o mercado de segurança evolui e lança novos produtos. Diante deste cenário, o Gartner desenvolveu o conceito de Managed Security Services - MSS. Neste modelo empresas especialistas de segurança, atuando por meio de Security Operations Center – SOC, ofertam diversas soluções de segurança na modalidade de serviço. As maiores vantagens desta modalidade são:

- Maior flexibilidade com relação à aquisição de produtos;
- Os serviços podem ser contratados sob demanda, conforme a necessidade e disponibilidade financeira do cliente;
- Maior velocidade de inserção de novas tecnologias;
- Utilização de profissionais altamente capacitados e especialistas em cibersegurança, que dificilmente atuariam em um único cliente de pequeno porte;
- Menor custo total de propriedade (Total Cost of Ownership – TCO), tendo em vista os custos de compra, operação e capacitação contínua a longo prazo.

4.1.7. É importante destacar que no caso específico do segmento de informática, o processo de execução indireta tem se consolidado nos últimos anos, em decorrência das normas legais, de orientações do TCU e do seu comprovado sucesso. Ele desonera as organizações dos altos custos de operação e manutenção da infraestrutura do ambiente de tecnologia da informação, especialmente quanto aos esforços diretos e indiretos de manutenção e para aperfeiçoamento de quadro de profissionais especializados nestas atividades. Ainda, possibilita ao quadro técnico interno dedicar-se às principais tarefas definidas em seu Regimento Interno do Ministério da Justiça e Segurança Pública:

I - elaborar, estabelecer, manter e propor mudanças nas políticas, normas, controles e metodologias de Gerenciamento de Riscos e de Segurança da Informação de TIC do Ministério;

II - coordenar a elaboração da Política de Segurança da Informação e Comunicações – POSIC e demais planos ou normas relacionados à segurança da informação da TIC;

III - promover e disseminar a cultura de Gerenciamento de Segurança de TIC;

IV - assessorar o Comitê de Segurança da Informação nas questões que envolvem tecnologias em segurança da informação e comunicações;

V - planejar, coordenar e controlar as ações associadas à Segurança da Informação e Comunicações de TIC;

VI - prospectar e propor a adoção de mecanismos, equipamentos e recursos para melhoria da segurança de TIC;

VII - acompanhar e monitorar as atividades, operações e incidentes de segurança de TIC, atuando quando necessário em seu bloqueio em última instância;

VIII - identificar as necessidades de qualificação técnica de sua equipe;

IX - gerenciar as divisões vinculadas à área de atuação da coordenadoria;

X - atuar de forma integrada e sistêmica com as coordenações e divisões da DTIC;

XI - realizar análises, varreduras, inspeções, prospecções, testes e auditorias de segurança no âmbito do ministério; e

XII - desempenhar outras competências típicas da unidade, delegadas pela autoridade superior ou conforme determinação legal.

4.1.8. Diante do exposto acima, é necessária a terceirização de parte dos serviços operacionais, permanecendo sob responsabilidade do quadro de servidores, as funções de gestão e de planejamento, intransferíveis para empresas terceirizadas.

4.1.9. Apesar de ter sido realizando um concurso para servidores temporários no Ministério da Justiça e Segurança Pública esse concurso não previu vagas para a especialidade de segurança da informação. Ainda que houvesse vagas nesse concurso, seria necessário também viabilizar, do ponto de vista normativo e operacional, a utilização de servidores do órgão em regime de escala de trabalho e/ou de plantão 24x7, considerando que os incidentes de segurança da informação não possuem hora específica para ocorrer. Atualmente não é permitido no âmbito do Ministério o regimento de escala de trabalho e/ou de plantão 24x7 para os seus servidores. Desta forma, essa solução é considerada inviável.

4.2. **Solução 2**

4.2.1. **Descrição:** A solução dois considera a ampliação da Contratação do Network Operations Center - NOC para desempenhar as tarefas de SOC, Blue Team, Red Team e Purple Team.

4.2.2. **Justificativa:** O Ministério da Justiça e Segurança Pública possui o Contrato nº 40/2019 (10267604), o qual tem por objeto a 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 de 1º, 2º e 3º níveis, a usuários 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 Comunicações - TIC.

4.2.3. Dentre os vários serviços incluídos no contrato supracitado está o NOC, responsável pela monitoração da infraestrutura de TIC, conforme definido no Termo de Referência (9629880), referente a contratação de empresa especializada na prestação de serviço de *service desk* e sustentação de infraestrutura de tecnologia para organização.

4.2.4. Um *Network Operations Center* - NOC, "é responsável por lidar com incidentes que afetem a performance ou disponibilidade, enquanto o SOC lida com incidentes de segurança que afetam os ativos de segurança"[1].

4.2.5. O NOC lida com problemas relacionados ao gerenciamento, monitoramento e controle das redes dentro da infraestrutura. Isso inclui servidores, máquinas virtuais e bancos de dados. Esses itens mantêm o fluxo de dados para os aplicativos e sistemas usados pelo órgão. Quando a rede, site, servidores ou aplicativos caem, o NOC é responsável por encontrar a origem do problema e fazer tudo funcionar novamente. Eles estão garantindo que a infraestrutura de TI permaneça em funcionamento.

4.2.6. Outras funções do NOC incluem relatórios de desempenho e recomendações de melhoria, resposta à interrupção, planejamento de capacidade, alerta de acordo com procedimentos de escalação definidos e garantir a coordenação entre redes díspares.

4.2.7. Ter uma equipe NOC pronta para monitorar e resolver os problemas antes que eles se manifestem aos usuários funciona melhor para minimizar o tempo de inatividade do órgão. Os NOCs geralmente têm uma sala de controle central configurada para vigiá-los e alertá-los sobre possíveis complicações que ameaçam a infraestrutura de uma organização.

4.2.8. Enquanto um NOC trabalha para manter as redes, aplicativos e outros equipamentos em funcionamento, um SOC (Security Operations Center) rastreia ameaças inteligentes que fazem tentativas hostis de entrar na infraestrutura de uma organização. Esses esforços podem vir de dentro ou de fora da organização, incluindo malwares e outros softwares suspeitos projetados para roubar dados ou causar interrupção na rede.

4.2.9. Cabe a um SOC proteger as organizações contra e-mails contendo vírus e outras ameaças acessadas acidentalmente pelos funcionários. Eles rastreiam tentativas não autorizadas de entrar na rede de uma organização, usando ferramentas de monitoramento de segurança e outros recursos para aprender os padrões e se adaptar às táticas usadas.

4.2.10. Outras funções SOC incluem, mas não se limitam a, monitorar e impedir o vazamento de dados, avaliar novos softwares para vulnerabilidades, manter as ferramentas de segurança e patches atualizados, acompanhar tendências relacionadas a diferentes ameaças cibernéticas, implementar medidas anti-DDOS e executar testes de intrusão. A tabela 6 apresenta as principais diferencias entre os conceitos de NOC e SOC.

Tabela 6 - Diferença entre NOC E SOC

DIFERENÇAS	NOC	SOC
Significado da sigla	Centro de Operações de Rede (Network Operations Center).	Centro de Operações de Segurança (Security Operations Center).
Terminologia	Usado para lidar com desafios relacionados ao gerenciamento, monitoramento e controle das redes no ecossistema de TI do cliente.	Rastreia ameaças à infraestrutura, fazendo tentativas de usar a vulnerabilidade e entrar em uma rede.
Papel fundamental	Para cumprir acordos de nível de serviço e gerenciar incidentes relacionados a disponibilidade para atingir o tempo de atividade máximo.	Para proteger a propriedade intelectual, proteger as informações confidenciais do cliente e gerenciar incidentes relacionados a disponibilidade, integridade e confidencialidade.
Objetivos	Para monitorar o desempenho.	Para monitorar a segurança.
Tecnologia	Acesso a dados em tempo real.	Acesso a dados em tempo real e históricos.
Ferramentas	Software de monitoramento de falhas, problemas e desempenho.	Qualidade de serviço, experiência do cliente e software de marketing.
Habilidades	* Infraestrutura de rede * Análise de dados, * Solução de problemas e * Conhecimento de tecnologia.	* Infraestrutura de segurança * Modelagem de serviço * Interpretação de dados * Comunicação.
Métricas	Abordagem reativa.	Abordagem reativa e proativa.
Impacto nos negócios	Operacional.	Estratégico.

Fonte: adaptado de https://ipwithease.com/noc-vs-soc/

Nota: 1 - SOC vs NOC, qual a diferença?. <https://realprotect.net/blog/qual-diferenca-security-operations-center-soc-vs-network-operations-center-noc/> Página da internet. Acesso em 13/05/2021.

4.2.11. Percebe-se que as atividades desempenhadas por ambos os centros de operação são diferentes, um destinado a segurança da informação enquanto o outro a infraestrutura de redes.

4.2.12. Isso posto, a possível solução de ampliar o Contrato nº 40/2019 (10267604) para desempenhar as tarefas de SOC, Blue Team, Red Team e Purple Team torna-se inviável, pois poderia ser considerado como uma alteração do objeto licitatório, uma vez que incluiria serviços não previstos originalmente na licitação.

4.2.13. Além disso, não é recomendável que quem proveja os serviços de rede verifique se ela é efetivamente segura uma vez que, muitas vezes, falhas na verificação do próprio trabalho podem acontecer. A norma ISO 27001 considera a segregação de funções no Sistema de Gestão de Segurança da Informação (SGSI) para minimizar o risco de uma única posição possa ter a oportunidade de comprometer as atividades de uma organização.

4.2.14. A principal razão de se aplicar a segregação de funções é prevenir a realização e ocultação de fraude e erro no curso normal das atividades, uma vez que havendo mais de uma pessoa para realizar uma atividade se minimiza a oportunidade de transgressões e aumenta as chances de se detectá-la, assim como de se detectar erros não intencionais.

4.3. **Solução 3**

4.3.1. **Descrição:** A solução três considera a aquisição de Equipamentos de Segurança e/ou Softwares para desempenhar as tarefas de SOC, Blue Team, Red Team e Purple Team.

4.3.2. **Justificativa:** A simples aquisição de equipamentos ou softwares de segurança não exime a necessidade de pessoas para operá-los. Não adianta ter diversos alarmes, indicadores, sugestão ou inteligência artificial sem que se tenha o ente humano para tratar os alarmes, observar os indicadores, implementar as sugestões ou programar e manter a inteligência artificial.

4.3.3. Atualmente o Ministério da Justiça e Segurança Pública possui, como é possível observar no no **relatório de informações sobre a infraestrutura** (14628328), um vasto *pool* de Tecnologias, sendo o elo mais fraco dessa corrente de segurança da informação a quantidade de pessoas dedicadas a análise, monitoramento, controle e gestão dessas tecnologias.

4.3.4. Por isso, a simples aquisição de mais tecnologia apenas irá aumentar esse *pool*, não aumentando a segurança da informação do Ministério.

5. **ANÁLISE COMPARATIVA DE CUSTOS (TCO)**

5.1. **CÁLCULO DOS CUSTOS TOTAIS DE PROPRIEDADE**

5.1.1. **Solução Viável 4**

5.1.2. **Descrição: Contratação de um SOC, Blue Team, Purple Team e Red Team como serviço**

5.1.3. De acordo com o curso PCTI - Planejamento da Contratação de TI da Escola Nacional de Administração Pública - ENAP, em seu Módulo 2 - Análise de Viabilidade da Contratação e Plano de Sustentação (figura-13), temos que:

Total Cost of Ownership - TCO

O *Total Cost of Ownership* ou Custo Total de Propriedade é um critério de escolha entre alternativas tecnológicas muito utilizado no setor privado. Este conceito defende que, ao se comparar duas ou mais Soluções de Tecnologia da Informação, não se deve considerar apenas o custo de aquisição (ou de desenvolvimento) de cada uma delas. Deve-se considerar o custo total que a aquisição e consequente propriedade daquele ativo trará ao contratante. Engloba, assim, custos de aquisição/desenvolvimento, instalação, treinamento, operação e manutenção.

Figura 14 - TCO - Total Cost of Ownership. Disponível em: https://repositorio.enap.gov.br/bitstream/1/1131/1/M%C3%B3dulo_2.pdf, atualizado em: dezembro de 2013. Acesso em 13/05/2021.

5.1.4. Das soluções apresentadas na tabela 4, apenas a solução 4, item 5.1.1, ou seja, a contratação da solução como serviço se mostra viável devido as características e especificidades do Ministério. Além disso, a contratação do serviço de SOC não envolverá aquisição por parte do Ministério da Justiça e Segurança Pública de qualquer bem, software ou sistema. Apenas o serviço prestado de SOC, Blue Team, Purple Team e Red Team será contratado. Os ativos, bens, sistemas, insumos necessários a execução do serviços que forem providos pela contratada, em complemento aos disponibilizados pelo Ministério, serão devolvidos ao final do contrato, exceto as informações produzidas durante a prestação do serviço.

5.1.5. Diante disso, para estimar o custo total de propriedade, utilizaremos uma contratação similar, realizada pelo Conselho da Justiça Federal do DF, Pregão Eletrônico nº 1 de 2020, ocorrida no dia 05 de fevereiro de 2020.

5.1.6. Devido as características e especificidades tanto do Conselho da Justiça Federal do DF quanto do Ministério da Justiça e Segurança Pública, adaptações serão realizadas e justificadas.

5.1.7. O pregão do CJF considerou a contratação dos seguintes itens:

1. **Item 1 do pregão- Serviço de operação e atendimento a requisições**: para sustentar e operar todas as soluções e produtos de segurança do CJF, bem como a realização permanente de ações proativas (gap analysis) voltadas para a segurança do parque computacional do CJF com o objetivo de mantê-lo estável, disponível e integro.
2. **Item 2 do pregão - Serviço de gestão de incidentes de segurança (CSIRT - Blue Team)**: para analisar, remediar, conter e documentar os eventos de segurança da informação que foram transformados em um incidente de segurança da informação, obedecendo os principais frameworks de gestão de incidentes de segurança da informação e boas práticas de mercado.
3. **Item 3 do pregão - Serviço de gestão de vulnerabilidades**: que tem por objetivo, de forma proativa e recorrente, identificar possíveis vulnerabilidades de segurança da informação no ambiente a fim de evitar que ataques cibernéticos obtenham sucesso explorando vulnerabilidades conhecidas.
4. **Item 4 do pregão - Serviço de monitoramento e visibilidade de ataques cibernéticos**: visando o monitoramento contínuo e ininterrupto de ataques cibernéticos direcionados ao CJF, através de correlacionamento de logs, análise de pacotes de rede, comportamento anômalo de usuários, aplicações, serviços e infraestrutura que possam gerar eventos de segurança da informação, aos quais devem ser analisados, podendo estes serem transformados em um incidente de segurança da informação.

5. **Item 5 do pregão - Serviço de orquestração, automação e resposta de segurança (SOAR)**: serviços e infraestrutura que possam gerar eventos de segurança da informação, aos quais devem ser analisados, podendo estes serem transformados em um incidente de segurança da informação.
6. **Item 6 do pregão - Serviço de testes de invasão (Red Team)**: tem como objetivo principal identificar, mapear e documentar possíveis vulnerabilidades nos sistemas, processos e ativos de infraestrutura tecnológica. Esses testes envolvem, necessariamente, o uso de técnicas e ferramentas específicas para tentar obter acesso não autorizado e privilegiado aos ativos e informações, bem como a indicação de soluções para a correção das vulnerabilidades encontradas.

5.1.8. O presente Estudo Técnico Preliminar visa a contratação, conforme expresso alhures, dos seguintes itens:

5.1.8.1. **Serviço de Security Operations Center - SOC**: conforme item 2.2 deste estudo.

5.1.8.2. **Serviço de Blue Team**: conforme item 2.3 deste estudo.

5.1.8.3. **Serviço de Red Team**: conforme item 2.4 deste estudo.

5.1.9. A tabela 7 apresenta a comparação dos serviços contratados pelo CJF com os serviço almejados pelo Ministérios da Justiça e Segurança Pública chegamos as seguintes conclusões de equivalência, quando possível.

5.1.10. Cabe registrar que a ata do pregão do Conselho da Justiça Federal - CJF foi inserido no presente processo sob o numero de documento (13624102). Foi inserido no presente processo o Edital do Conselho da Justiça Federal, sob o número de documento (13624084).

Tabela 7 - Equivalência dos serviços contratados pelo CJF e os almejados pelo MJSP.

MJSP	CJF
Serviço de Security Operations Center - SOC	Serviço de operação e atendimento a requisições
Serviço de Blue Team	Serviço de gestão de incidentes de segurança (CSIRT - Blue Team)
Serviço de Red Team	Serviço de testes de invasão (Red Team)

5.1.11. Além da equivalência devemos comparar o tempo de prestação dos serviços no CJF com os desejados pelo MJSP. Visando comparar os serviços para ambos os órgãos criamos a tabela 8.

Tabela 8 - Método de comparação utilizado para estimar o valor.

MJSP	Prestação	CJF	Prestação		Forma de Comparação
Serviço de Security Operations Center - SOC	24h x 7 dias	Serviço de operação e atendimento a requisições	Segunda-feira até Sexta-feira		Será dividido o valor dos itens pelas quantidades de horas contratadas e multiplicado pela necessidade do MJSP
			Remoto	Presencial	
			9h até 20h = 11 horas	13h até 21h = 8h	
Serviço de Blue Team	Horário Comercial	Serviço de gestão de incidentes de segurança (CSIRT - Blue Team)	24h x 7 dias 1 vez por mês		Será dividido o valor dos itens pelas quantidades de horas contratadas e multiplicado pela necessidade do MJSP
Serviço de Red Team	Sob demanda	Serviço de testes de invasão (Red Team)	Sob demanda por sistema (15 Sistemas)		Será utilizado valor integral devido aos itens serem equivalentes
Serviço de Purple Team	Não comparado por estar incluído nos outros serviços ou não estar relacionado com prestação em horas.				

5.1.12. Considerando as tabelas 7 e 8 chegamos aos custos por hora e serviço para o CJF, apresentados na tabela 9:

Tabela 9 - Custo final por hora ou serviço

Serviço CJF	Custo do Item de Serviço e Quantidade de Horas	Total final por hora ou serviço [2]
Serviço de operação e atendimento a requisições	Horas por mês de 22 dias úteis com 11 horas remotas por dia: 242 horas Valor [1] do item 1 por mês: R$ 56.520,00	R$ 233,55 por hora
Serviço de monitoramento e visibilidade de ataques cibernéticos	15GB/dia ou 440 EPS R$ 8.705,62	R$ 580,37 por GB/dia
	1000 ativos R$ 4.249,97	R$ 4,24 por ativo
	1 Gbps R$ 13.261,75	R$ 13.261,75 por 1 Gbps
Serviço de orquestração, automação e resposta de segurança (SOAR)	24h x 7 dias R$ 24.670,00	R$34,26 por hora
Serviço de gestão de incidentes de segurança (CSIRT - Blue Team)	24h x 7 dias R$ 18.443,65	R$ 25,62 por hora
Serviço de testes de invasão (Red Team)	Para 1 sistemas que geralmente possui 10 alvos em média R$ 11.508,40	R$ 11.508,40 por sistema ou R$ 1.150,84 por alvo
Serviço de gestão de vulnerabilidades	Uma vez por mês independente do tempo que levar para conclusão R$ 17.040,65	R$ 17.040,65

1 Ata do pregão publicado no comprasnet (http://comprasnet.gov.br/livre/pregao/ata2.asp?co_no_uasg=90026&numprp=000012020&f_lstSrp=T&f_Uf=DF&f_numPrp=12020&f_coduasg=&f_tpPregao=E&f_lstICMS=T&f_dtAberturaIni=&f_dtAberturaFi
2 Considerado um mês de 30 dias.

5.1.13. Diante das equivalências demonstradas pela Tabela 7, 8 e 9, podemos estimar o custo total de propriedade para a contratação dos serviços no MJSP. Conforme tabela 10. Os serviços "Serviço de monitoramento e visibilidade de ataques cibernéticos", "Serviço de orquestração, automação e resposta de segurança (SOAR)" e "Serviço de gestão de vulnerabilidades" não foram considerados por tratarem de serviços relacionados a contratação de software, que não são objeto da contratação sendo realizada pelo MJSP.

Tabela 10 - Custo estimado para o MJSP.

Custo Total de Propriedade – Memória de Cálculo

Com o auxílio das tabelas 7, 8 e 9 chegamos a uma estimativa para o custo de uma possível contratação para o Ministério da Justiça e Segurança Pública, que é apresentado na tabela 10:

Serviço MJSP	Serviço CJF associado	Valor por hora ou Serviço	Quantidade horas ou serviço MJSP	Total
Serviço de Security Operations Center - SOC + Blue Team Suporte Nivel 1	Serviço de operação e atendimento a requisições	R$ 233,55 por hora	24h x 7 dias = 720 horas 720 x 24 meses = 17.280	17.280 x R$ 233,55 =**168.156,00 por mês e R$ 4.035.744,00 por 24 meses**
Serviço de Blue Team Suporte Nível 2 em diante	Serviço de gestão de incidentes de segurança (CSIRT - Blue Team)	R$ 25,62 por hora	24h x 7 dias = 720 horas 720 x 24 meses = 17.280	720 horas x R$ 25,62 = **R$ 18.446,40 por mês e R$ 442.713,60 por 24 meses**
Total Mensal (Continuo):				**R$186.602,40**
Serviço de Red Team	Serviço de testes de invasão (Red Team)	R$ 1.150,84 por alvo	Sob demanda 217 Sistemas + 14 Appliance de Segurança + 110 Ativos de Rede + 68 Host Físico no Datacenter + 400 Sistemas Operacionais de Servidores + 18 Sistemas de Armazenamento = 827 alvos Considerando que um sistema possui em média 10 ativos (Gateway de Rede, Firewall, DNS, Balanceador de Carga, Firewall de APP, 2x Servidores de App, 2x Servidores de Transação, Servidor de Banco de Dados - Clusterizado dentre outros ativos)	827 alvos x R$ 1.150,84 = R$ 951.744,68 / 24 meses **= 39.656,02 por mês**
Total (sob demanda):				**R$ 951.744,68**
Total 24 meses				R$ 5.430.202,28

5.1.14. Cabe o registro de que equipe de planejamento buscou junto a contratações similares, mas não encontrou uma métrica precisa e comum de mercado para definir o quantitativo e variação dos serviços de SOC sem considerar a contratação de software. Nesse sentido o dimensionamento da equipe para execução adequada dos serviços será de responsabilidade da CONTRATADA, devendo ser suficiente para o cumprimento integral dos níveis mínimos de serviço exigidos.

5.1.15. Considerando o valor mensal de **R$ 186.602,40** referente aos serviços contínuos, foi multiplicado por 12 meses, para chegar ao valor anual de **R$ 2.239.228,80** e somado a metade do valor estimado referente ao serviço de testes de invasão (Red Team) de 24 meses que é de R$ **475.872,34**, chega-se ao total de **R$ 2.715.101,14** para 12 meses, conforme valores unitários e totais da tabela 10**.**

5.2. **MAPA COMPARATIVO DOS CÁLCULOS TOTAIS DE PROPRIEDADE (TCO)**

5.2.1. A tabela 11 apresenta a estimativa dos cálculos totais de propriedade para os próximos 5 anos, conforme memória de cálculo explicada no item 5.1.14. Não foram identificadas métricas de variação para a contratação que não esteja relacionada ao ICTI (índice de custo da tecnologia da informação) ou a valores de repactuação que poderão ocorrer. O valor pago por hora para a contratação de serviço não envolve software ou log em sua formação e não foi identificada relação adotada pelos fornecedores na variação de pessoas em uma equipe de SOC que pudesse compor a variação dos valores abaixo.

Tabela 11 - Estimativa dos cálculos totais de propriedade para os próximos 5 anos

Descrição da solução	Estimativa de TCO ao longo dos anos					Total para 5 anos
	Ano 1	Ano 2	Ano 3	Ano 4	Ano 5	

						de Contratação
Solução Viável 4	**R$ 2.715.101,14**	R$ **2.715.101,14**	R$ **2.715.101,14**	R$ **2.715.101,14**	R$ **2.715.101,14**	**R$13.575.505,70**

DESCRIÇÃO DA SOLUÇÃO DE TIC A SER CONTRATADA

5.3. A solução de contratação de um SOC, Blue Team e Red Team terá o seu detalhamento realizado junto ao Termo de Referência, porém, podemos descrever essa solução com menos detalhes visando obter junto a fornecedores no mercado uma estimativa de custos dessa contratação. Dessa forma, passamos a descrever em mais detalhes, mas ainda superficialmente as características da solução.

5.4. Após análise de uma contratação similar junto ao Conselho de Justiça Federal, chegou-se a conclusão que contratar em itens separados um Purple Team não traria benefícios concretos a essa contratação e dessa forma, optou-se por inserir esses serviços nos demais itens sendo seus detalhes explicitados no Termo de Referência. Devido a essa opção, optou-se também por estender o serviço de Blue Team de suporte em segundo nível também de forma ininterrupta atuando em sincronia com o SOC.

5.4.1. A solução será composta por 3 (três) itens de serviço integrados, não se limitando aos descritos abaixo, os quais serão detalhados no Termo de Referência:

5.4.1.1. **Serviço de Security Operations Center - SOC;**

5.4.1.2. **Serviço de Tratamento e Resposta aos Incidentes Cibernéticos - CSIRT - Blue Team;**

5.4.1.3. **Serviço de Testes de Invasão - Red Team;**

5.4.1.4. **O Serviço de Security Operations Center - SOC** e o **Serviço de Tratamento e Resposta aos Incidentes Cibernéticos - CSIRT - Blue Team** atuarão em conjunto e envolve os seguintes serviços, conforme *Information Technology Infraestructure Library* – ITIL e com as atividades dos processos do volume de **Transição de Serviços e Operação de Serviços**;

5.4.1.4.1. Gerenciamento de Configurações e de Ativo de Serviços;

5.4.1.4.2. Gerenciamento de Mudanças;

5.4.1.4.3. Gerenciamento de Liberações e Implantação;

5.4.1.4.4. Gerenciamento do Conhecimento;

5.4.1.4.5. Gerenciamento de Evento;

5.4.1.4.6. Gerenciamento de Incidente;

5.4.1.4.7. Gerenciamento de Problema;

5.4.1.4.8. Gerenciamento de Requisição;

5.4.1.4.9. Gerenciamento de Acesso;

5.4.1.4.10. Desempenhar atividades de 3º nível de **Operação de Serviços** das funções:

5.4.1.4.10.1. Central de Serviços;

5.4.1.4.10.2. Gerenciamento de Operações de TI (Controle de Operações de Segurança da Informação);

5.4.1.4.10.3. Gerenciamento Técnico;

5.4.1.4.10.4. Gerenciamento de Aplicação;

5.4.1.4.11. Ambos os serviços desempenharão os seguintes objetivos e propósitos:

5.4.1.4.11.1. Gerenciar a capacidade e recursos requeridos para empacotar, construir, testar e implementar as liberações no ambiente de produção.

5.4.1.4.11.2. Estabelecer e manter a integridade dos ativos de serviços e suas configurações.

5.4.1.4.11.3. Prover conhecimento de qualidade para a organização.

5.4.1.4.11.4. Prover mecanismos de implementação eficientes e padronizados.

5.4.1.4.11.5. Garantir que os serviços possam ser gerenciados, operados e suportados conforme os requisitos definidos.

5.4.1.4.11.6. Realizar as atividades e processos necessários para garantir o gerenciamento e a entrega dos serviços conforme níveis de serviços aqui definidos.

5.4.1.4.11.7. Gerenciar continuamente a tecnologia em uso para entregar e suportar os serviços.

5.4.1.4.11.8. Melhorar a percepção de qualidade e a satisfação de usuários e clientes quanto ao uso dos serviços do MJSP.

5.4.1.4.11.9. Prover mecanismos eficientes para tratamento das questões relativas ao dia-a-dia dos serviços.

5.4.1.4.11.10. Monitoramento e Análise remota de toda a infraestrutura do Ministério, utilizando-se de análise dos logs disponibilizados em tempo real através da Plataforma de SIEM/SOAR/NTA/UEBA/CTI do Ministério. Para o devido dimensionamento do esforço de trabalho necessário a Contratada deverá estimar um quantitativo mínimo de pessoal capaz de monitorar, analisar, operar e acompanhar a Plataforma de SIEM/SOAR/NTA/UEBA/CTI para um volume de no mínimo 200 GB/dia e 5000 EPS (Despacho nº 333, nº SEI 14781049). O cálculo do valor de EPS foi estimado utilizando a ferramenta LogPoint e distribuição realizada no Despacho 80 (nº SEI 14612910) com alteração nas quantidades existentes.

5.4.1.4.11.11. Configuração, manutenção, monitoramento e operação da Plataforma de SIEM/SOAR/NTA/UEBA/CTI do Ministério. sendo responsável pela solicitação da coleta dos logs ao Ministério.

5.4.1.4.11.12. Realização de atividades de preparação do processo de coleta de logs, incluindo a normalização, filtragem, redução, agregação e priorização. O processamento, normalização, armazenamento, e demais atividades de correlacionamento de logs que serão realizadas nas ferramentas da Plataforma de SIEM/SOAR/NTA/UEBA/CTI do Ministério, a partir dos dados disponibilizados pelo Ministério.

5.4.1.4.11.13. A CONTRATADA deverá disponibilizar uma ferramenta de ITSM (Information Technology Service Management) para registro, acompanhamento e controle dos Incidentes e Requisições de Segurança e gerir todo o ciclo de vida dos chamados de SOC. Ao final do contrato, as bases de dados das ferramentas utilizadas, com todos os dados, inclusive históricos das demandas, solicitações, atendimentos e demais informações relativas à prestação de serviços deverão ser entregues e permanecerão sob custódia exclusiva do Ministério;

5.4.1.4.11.14. Resposta aos incidentes por meio de monitoramento, análise e despacho, operando de forma sincronizada ao NOC do Ministério e, em caso de inoperância do NOC, atuar em substituição ao NOC dentro dos serviços autorizados em reunião inicial entre a

CONTRATANTE e CONTRATADA, visando minimizar as consequências e proteger as informações e ativos do ministério. Todas ações tomadas devem ser posteriormente repassadas ao NOC ou suporte da infraestrutura e a CRS.

5.4.1.4.11.15. Sugestão de ajustes de configuração dos dispositivos visando reduzir a probabilidade de ataques, sendo a execução desses ajustes de responsabilidade do NOC do ministério.

5.4.1.4.11.16. Realização de transferência de conhecimento para equipe técnica do ministério em todas as tecnologias instaladas e/ou utilizadas, sistemas, produtos e soluções instaladas pela CONTRATADA com o fornecimento de perfil de acesso para a supervisão dos serviços prestados, assim como, atualização rotineira no estado da arte em termos de segurança da informação.

5.4.1.4.11.17. Execução de serviços técnicos especializados, sob demanda e de maneira eventual.

5.4.1.4.11.18. Prestação remota dos serviços, sendo a presença física somente quando necessário ou mediante justificativa.

5.4.1.4.11.19. Utilização das ferramentas, soluções e equipamentos de segurança instalados no ministério.

5.4.1.4.11.20. Alocação de equipamentos e softwares quando necessários à consecução das atividades de segurança da informação e ao atendimento das especificações técnicas do objeto durante o prazo de vigência do contrato, incluindo garantia, manutenção, atualização dos produtos e monitoramento de segurança em regime 24x7 (vinte e quatro horas por dia, sete dias por semana).

5.4.1.4.11.21. Prestação de informações e realização de demandas através de chamados técnicos do ministério, sob autorização e controle da Coordenação de Riscos e Segurança da Informação.

5.4.1.4.11.22. Disponibilização de pessoal técnico qualificado mediante certificação oficial e experiência profissional em todos os itens da possível contratação.

5.4.1.4.11.23. Análise fim a fim dos incidentes e ataques.

5.4.1.4.11.24. Apoiar a CRS na elaboração de minuta de comunicação à Autoridade Nacional de Proteção de Dados (ANPD) quanto ao registro de incidentes junto ao Ministério, de acordo com o Art. 48 da LGPD .

5.4.1.4.11.25. Apoiar a CRS na elaboração de minuta de comunicação à Autoridade Policial quanto ao registro de incidentes com classificação de crimes cibernético junto ao Ministério.

5.4.1.4.11.26. Apoiar o Ministério na retenção de informações de acordo com os mecanismos de retenção e guarda de registros de conexão, nos termos da Lei 12.965/2014 que estabeleceu os princípios, garantias, direitos e deveres para o uso da Internet no Brasil.

5.4.1.4.11.27. Para divulgação de ações de segurança da informação (Alertas, Conscientização e Recomendações) aos usuários finais, equipes de TIC e aos gestores com o objetivo de fortalecer uma estrutura para projetar, implementar, monitorar, manter e melhorar a segurança da informação consistente com a cultura organizacional, conforme preceitua a ABNT NBR ISO/IEC 27000, bem como para acompanhamento e avaliação dos indicadores de performance e serviços de SOC e CSIRT pelos gestores de TIC do Ministério a CONTRATADA deverá desenvolver e manter um **Portal WEB de CSIRT do Ministério** hospedado na infraestrutura da CONTRATANTE, para a disponibilização de tais informações, como também informações para registro de notificações por usuários externos ao Ministério com uso de tecnologias seguras, definidas pela CRS, para comunicações através de canal seguro.

5.4.1.4.11.28. Disponibilização de painel para acompanhamento em tempo real do status de segurança do ministério, dos alertas gerados pelas ferramentas que compõem o SOC, dos incidentes reportados, dos ataques em andamento ou contidos, das vulnerabilidades descobertas, enfim, de todas as informações de segurança da informação.

5.4.1.4.11.29. A Contratada deverá disponibilizar a Contratante acesso aos sistemas que utilize na prestação do serviço e que não sejam do MJSP.

5.4.1.4.12. O **Serviço de Tratamento e Resposta aos Incidentes Cibernéticos - CSIRT - Blue Team** deverá ser observadas as orientações e técnicas emanadas pelos padrões internacionais, além de outros apresentados pela CONTRATADA, caso haja em seu portfólio normativos que comprovadamente complementem os demonstrados abaixo:

5.4.1.4.12.1. NIST Cybersecurity Framework, Version 1.1 ou mais recente;

5.4.1.4.12.2. NIST Privacy Framework, Version 1.0 ou mais recente;

5.4.1.4.12.3. NIST Special Publication 800-61 Revision 2 (Computer Security Incident Handling Guide);

5.4.1.4.12.4. NIST Special Publication 800-115 (Technical Guide to Information Security Testing and Assessment);

5.4.1.4.12.5. SANS Incident Handler's Handbook;

5.4.1.4.12.6. CIS Control, Version 7.1 ou mais recente;

5.4.1.4.12.7. ISO/IEC 27035-1:2016 - Information technology — Security techniques — Information security incident management — Part 1: Principles of incident management;

5.4.1.4.12.8. ISO/IEC 27035-2:2016 - Information technology — Security techniques — Information security incident management — Part 2: Guidelines to plan and prepare for incident response;

5.4.1.4.12.9. ISO/IEC 27035-3:2020 - Information technology — Information security incident management — Part 3: Guidelines for ICT incident response operations;

5.4.1.4.13. Monitoramento e Análise de Logs e Eventos com capacidade, atualmente em aproximadamente 200GB/dia ou 5.000 EPS. O cálculo do valor de EPS foi estimado utilizando a ferramenta LogPoint e distribuição realizada no Despacho 80 (nº SEI 14612910) com alteração nas quantidades existentes.

5.4.1.4.14. Monitoramento da rede sociais, Dark Web e Deep Web com ferramentas adequadas para monitoramento de informações sensíveis e de interesse do Ministério a respeito de segurança da cibernética.

5.4.1.4.15. Para fins de execução do contrato, a CONTRATADA deverá atender os requisitos técnicos especificados deste ETP. Todos os processos poderão ser amadurecidos conforme evolução da operação no ambiente de infraestrutura durante a execução do contrato.

5.4.1.5. O **Serviço de Teste de Invasão - Red Team** envolve os seguintes serviços, conforme *Information Technology Infraestructure Library* – ITIL e com das atividades dos processos do volume de **Transição de Serviços e Operação de Serviços**;

5.4.1.5.1. Gerenciamento do Conhecimento;

5.4.1.5.2. Gerenciamento de Incidente;

5.4.1.5.3. Gerenciamento de Problema;

5.4.1.5.4. Gerenciamento de Requisição;

5.4.1.5.5. Desempenhar atividades de 2º e 3º nível de **Operação de Serviços** das funções:

5.4.1.5.5.1. Central de Serviços;

5.4.1.6. Serviços de Red Team desempenhará os seguintes objetivos e propósitos:

5.4.1.6.0.1. Estabelecer e manter a integridade dos ativos de serviços e suas configurações.

5.4.1.6.0.2. Prover conhecimento de qualidade para a organização.

5.4.1.6.0.3. Garantir que os serviços possam ser gerenciados, operados e suportados conforme os requisitos definidos.

5.4.1.6.0.4. Realizar as atividades e processos necessários para garantir o gerenciamento e a entrega dos serviços conforme níveis de serviços aqui definidos.

5.4.1.6.0.5. Gerenciar continuamente a tecnologia em uso para entregar e suportar os serviços.

5.4.1.6.0.6. Prover mecanismos eficientes para tratamento das questões relativas ao dia-a-dia dos serviços.

5.4.1.6.1. Realização de testes de penetração.

5.4.1.6.2. Identificar, mapear e documentar possíveis vulnerabilidades nos sistemas, processos e ativos de infraestrutura tecnológica. Esses testes envolvem, necessariamente, o uso de técnicas e ferramentas específicas para tentar obter acesso não autorizado e privilegiado aos ativos e informações, bem como a indicação de soluções para a correção das vulnerabilidades encontradas.

5.4.1.6.3. A CONTRATADA deverá disponibilizar ferramenta de ITSM (Information Technology Service Management) para registro, acompanhamento e controle dos Incidentes e Requisições de Segurança e gerir todo o ciclo de vida dos chamados de RED TEAM. Ao final do contrato, as bases de dados das ferramentas utilizadas, com todos os dados, inclusive históricos das demandas, solicitações, atendimentos e demais informações relativas à prestação de serviços deversão ser entregues e permanecerão sob custódia exclusiva do Ministério;

5.4.1.6.4. O Serviço de Testes de Invasão será do tipo externo e interno e terá como objetivo principal identificar, mapear, documentar, controlar e corrigir possíveis vulnerabilidades nos sistemas, processos e ativos de infraestrutura tecnológica. Para a realização dos testes de invasão deverão ser observadas as orientações e técnicas emanadas pelos padrões internacionais, além de outros apresentados pela CONTRATADA, caso haja em seu portfólio normativos que comprovadamente complementem os demonstrados abaixo:

5.4.1.6.4.1. OSSTMM 3 (The Open Source Security Testing Methodology Manual) ;

5.4.1.6.4.2. ISSAF/PTF (Information Systems Security Assessment Framework);

5.4.1.6.4.3. NIST Special Publication 800-115 (Technical Guide to Information Security Testing and Assessment);

5.4.1.6.4.4. NIST Special Publication 800-42 (Guideline on Network Security Testing);

5.4.1.6.4.5. OWASP TESTING GUIDE 4.1 The Open Web Application Security Project.

5.4.1.6.5. Neste documento os termos “pentest”, teste de penetração, teste de intrusão e testes de invasão, são considerados sinônimos;

5.4.1.6.6. Os alvos dos “Testes de Invasão” bem como as premissas e condições para realização destes serão, necessariamente, definidos e aprovados através de demanda por parte do Ministério;

5.4.1.6.7. A Contratada deverá observar que os testes de invasão serão executados internamente (qualquer ponto da rede corporativa do Ministério) e externamente (através da Internet);

5.4.1.6.8. Todas as fases dos “Testes de Invasão” serão acompanhadas e supervisionadas a critério do Ministério;

5.4.1.6.9. Quaisquer atividades que possa comprometer ou prejudicar algum ambiente ou ativo deverá ser imediatamente reportada, antes de sua execução, haja vista a necessidade de manter a disponibilidade dos ambientes e serviços ativos;

5.4.1.6.10. O teste de invasão deverá obedecer às seguintes fases:

5.4.1.6.10.1. Planejamento;

5.4.1.6.10.2. Descoberta;

5.4.1.6.10.3. Ataque;

5.4.1.6.10.4. Relatório Teste de Invasão;

5.4.1.6.10.5. Reunião para apresentação do relatório de recomendações e descrição das atividades executadas durante o teste;

5.4.1.6.10.6. Reavaliação, novo teste pós remediação;

5.4.1.6.10.7. Relatório Final do Teste de Invasão.

5.4.1.7. Para fins de execução do contrato, a CONTRATADA deverá atender os requisitos técnicos especificados deste ETP. Todos os processos poderão ser amadurecidos conforme evolução da operação no ambiente de infraestrutura durante a execução do contrato.

5.5. Matriz de Responsabilidade R.A.C.I

5.5.1. Para um melhor entendimento das responsabilidades a serem executadas pelos serviços objeto da presente contratação, foi definido uma Matriz de Responsabilidade R.A.C.I apresentado a seguir, a qual esta alinhada com a Figura 11 - Diagrama de relacionamento dos serviços e seus respectivos componentes com os demais serviços da DTIC e envolve todos os atores com participação no SOC e na Área de Segurança Cibernética ;

Tabela 12 - Matriz de Responsabilidade R.A.C.I - Plataforma de SIEM/SOAR/NTA/UEBA/CTI do Ministério e Área de Segurança da Cibernética

Matriz de Responsabilidade R.A.C.I - Plataforma de SIEM/SOAR/NTA/UEBA/CTI do Ministério e Área de Segurança da Cibernética														
Serviços		Transição de Serviços				Operação de Serviços								
		Processos				Processos					Funções			
Situação	Descrição	Ger. de Configurações e de Ativo de Serviços	Ger. de Mudanças	Ger. de Liberações e Implantação	Ger. do Conhecimento	Ger. de Evento	Ger. de Incidente	Ger. de Problema	Ger. de Requisição	Ger. de Acesso	Central de Serviços	Ger. de Operações de TI	Ger. Técnico	Ger. de Aplicação
Nova contratação	Solução de SOC	C/I	C/I	C/I	C/I	C/I	C/I	C/I	C/I	C/I	C/I	C/I	C/I	C/I
	Serviços de CSIRT Blue Team	R/C/I	R/C/I	R/C/I	R/C/I	R/C/I	R/C/I	R/C/I	R/C/I	R/C/I	R/C/I	R/C/I	R/C/I	R/C/I
	Serviços de Red Team	-	-	-	R/C	-	R/C	R/C	R/C/I	-	R/C/I	-	-	-
Contratação existente	Serviço de NOC	C/I	C/I	C/I	C/I	C/I	C/I	C/I	C/I	C/I	C/I	C/I	C/I	C/I
	Serviços de Infraestrutura	R/C/I	R/C/I	R/C/I	R/C/I	R/C/I	R/C/I	R/C/I	R/C/I	R/C/I	R/C/I	R/C/I	R/C/I	R/C/I
Contratante	**MJSP\DTIC\CRS**	**A/C/I**	**A/C/I**	**A/C/I**	**A/C/I**	**A/C/I**	**A/C/I**	**A/C/I**	**A/C/I**	**A/C/I**	**A/C/I**	**A/C/I**	**A/C/I**	**A/C/I**

Legenda:
R: Responsável por executar uma atividade;
A: Autoridade, quem responde pela atividade, o dono
C: Consultado, quem deve ser consultado e participar da decisão ou atividade no momento que for executada;
I: Informado, quem deve receber a informação de que uma atividade foi executada;
Obs.: As atividades da nova contratação são junto a Plataforma de SIEM/SOAR/NTA/UEBA/CTI do Ministério e não conflitará com as atividades da contratação existente, pois a mesma, atuará de forma subsidiária ao contrato existente quando da necessidade de ações junto a Área de Segurança Cibernética, conforme definido no item 2.2.1.5 desse Estudo Técnico Preliminar.

5.6. Indicadores de performance do Serviço de Security Operation Center - SOC

5.6.1. A frequência de aferição dos indicadores de performance será mensal, porém com registros diários quando aplicável, devendo a contratada elaborar Relatório Mensal de Atividades, apresentando-o ao Ministério até o quinto dia útil do mês subsequente ao da prestação do serviço.

5.6.2. Devem constar desse relatório, entre outras informações, os indicadores de performance, metas de níveis de serviço alcançados, recomendações técnicas, administrativas e gerenciais para o próximo período e demais informações relevantes para a gestão contratual. O conteúdo detalhado e a forma do relatório gerencial serão definidos pelas partes.

5.6.3. Caberá à Comissão de Fiscalização do contrato analisar mensalmente o Relatório Mensal de Atividades executados pela Contratada, observando os indicadores e os níveis de serviço alcançados.

5.6.4. Os indicadores de performance são flexíveis em quantidade e qualidade e estão descritos na tabela a seguir:

Tabela 13 - Indicadores de Performance do Serviço SOC

Categoria	Subcategoria	Métrica	Unidade de medida
Governança	Conformidade	Quantidade de violações de políticas	número
		Porcentagem de sistemas com controles de segurança testados	percentual
	Privacidade	Quantidades de incidentes notificados a ANPD	número
	CSIRT	Avaliação da Maturidade do CSIRT de acordo com o "ENISA CSIRT maturity assessment model versão 2.0 - 30 de abril de 2019"	Nível e percentual de evolução
	Orquestração	Automação/Orquestração dos processos continuidade de negocio e resposta a incidentes cibernéticos	Nível e percentual de evolução
Técnico	Ameaças	Nível de segurança	Classificação de cores
		Atribuição de ameaças a atores (usando inteligência de ameaças)	a definir
	Vulnerabilidade	Tempo para remediação da vulnerabilidade	tempo
		Gravidade da vulnerabilidade	escala
		Incidentes de vulnerabilidade conhecida vs. desconhecida	número/escala
		Exposição à vulnerabilidade	escala
	Risco	Posição de risco	escala
		Risco por sistema/serviço	escala
		Principais riscos	texto
		Tipos de casos (MITRE ATT&CK)	número
	Alerta	Tempo por investigação de alerta	tempo
		Índice de geração de alerta	número/escala
		Número de alertas que permanecem por analisar (em aberto)	número
		Criticidade de um alerta	escala
	Incidente	Prioridade de incidentes	texto
		Total de incidentes por mês	número
		Número de ataques bem sucedidos	número/percentual
		Tempo médio de detecção (MTTD)	tempo
		Tempo médio para resolução/recuperação (MTTR)	tempo
		Custo por incidente	valor/texto
		Sucesso na mitigação	número/percentual
	Resiliência	Tempo médio gasto por ataque (MTTA)	tempo
		Eficiência defensiva	escala
		Repercussão do ataque	texto
		Quantidade de interrupções	número e percentual
		Tempo de interrupções	tempo
Pessoas	Performance	Número de incidentes encerrados em um turno	número
		Produtividade do analista	número
		Análise de escalação de caso	número
Gerais	Performance	Taxa de falso positivo	percentual
		Tempo médio de analise	tempo
		Nível de disponibilidade	percentual
	Cobertura	Quantidade de ativos monitorados	número
		Quantidade de ativos monitorados vs. Quantidade total de ativos	número e percentual

5.7. **Plataforma de SIEM/SOAR/NTA/UEBA/CTI do Ministério**

5.7.1. Como forma de avaliar os recursos da **Plataforma de SIEM/SOAR/NTA/UEBA/CTI do Ministério, Microsoft Azure Sentinel,** foi realizado um estudo comparativo entre os principais fornecedores de produtos que compõem a solução incluindo serviços de Plataforma como Serviço (PaaS), os quais são apresentados na tabela a seguir:

Tabela 14 - Benchmark SIEM + SOAR + UEBA

Benchmark SIEM + SOAR + UEBA versão 15/03/2021				
Funcionalidades\Players	**Microsoft**	**Exabeam**	**LogRhythm**	**Splunk**
SaaS (1)	Azure Sentinel	EXABEAM CLOUD PLATFORM (19)	LogRhythm Cloud	Splunk Cloud
SaaS no Brasil (1)	Sim	Sim (20)		Não (AWS e GCP) (14)
SIEM (2)	Azure Sentinel	Exabeam Security Management Platform	LogRhythm NextGen SIEM Platform	Splunk Enterprise Security
SOAR (2)	Azure Sentinel	Exabeam	LogRhythm's	Splunk Phantom

		Security Management Platform	SmartResponse™	
UEBA (Monitoramento de Usuários)	Azure Sentinel UEBA	Exabeam Security Management Platform	LogRhythm UserXDR	Splunk UBA
Recursos de ML e AI	Sim	Sim (23)	Sim (36)	Sim (MLTK)
Integração Exchange	Sim	Sim (25)	Sim com solução de terceiro (37)	Sim
Certificações externas que a solução possui		SOC 2 Tipo II (20)	SOC 2 Type I e GDPR (39)	SOC 2 Tier II / ISO/IEC 27001:2013 (3)
Ferramenta de compliance de implantação do cliente (Cybersecurity Posture Score and Compliance)	CMMC 4 e MITRE ATT&CK	GDPR, GPG, HIPAA, FISMA, PCI DSS, SOX (26)	CCF, GDPR, ISSO 27001, NIST (38)	FISMA, HIPAA, PCI
Tipo de licenciamento	Ingestão de dados GB (Logs)	Eventos de Segurança por segundo (27)	Ingestão de dados GB (Logs) (35)	Baseado em infraestrutura sem limites de dados ou por GB/dia (8)
Tipos de Retenção	90 dias de retenção incluso (6)	Retenção ilimitada (22)	90 dias de retenção incluso (40)	90 dias de retenção incluso (8)
Suporte a integração com nuvens	AWS, GCP e Oracle Cloud (OCI) (5 e 7)	AZURE, AWS e GCP (25)	Azure e AWS (41)	Azure, AWS e GCP (15 e 28)
Node Forward	Sim (5)	Sim (29)	Sim (44)	Sim (17)
Agent Forward	Sim (5)	Sim (29)	Sim (44)	Sim (18)
Suporte protocolos	Common Event Format (CEF), Syslog or REST-API (5)	Syslog e API (30)	UDP Syslog Device, TCP Syslog Device, NetFlow v1, v5 or v9 Device, IPFIX Device, J-Flow Device, sFlow Device e SNMP Trap Device (44)	HTTP Event Collector (HEC), Syslog e SNMP
Network Logs - Suporte a protocolos de flow (Netflow ou sFlow) - visão norte/sul e leste/oeste	Não (utiliza o logstash)	Sim (31)	Sim (43)	Sim (NetFlow ou IPFIX, Sflow e JFlow) (11)
Suporte a conectores	Sim (5)	Sim (24)		Sim (16)
Formas de Transferência de dados				VPN limitado a 1000 GB dia (14)
Arquitetura	Cloud | Local	MSSP | Hibrido | Local (21)		Cloud | Local
Suporte a Detecção e resposta de endpoint (EDR) Nativo	Sim - Windows Defender ATP + MS Defender Security Center (13)	Não (Integração com ferramentas de terceiros) (25)	Sim. (LogRhythm's Endpoint Monitoring and Forensics) (42 e 43)	Não (Integração com ferramentas de terceiros (Ex. Cisco Security Platforms) (12)
Processo de Gestão de Incidente e Problema (ITSM) Nativo	Não (Suporta com o uso de conector ServiceNow, System Center, Provance e Cherwell	Não (Suporte Atlassian JIRA e ServiceNow) (25)	LogRhythm Incident Management (40)	
Suporte a Inteligência Contra Ameaças Ciberneticas Nativo (CTI)	Não (Integração com ferramentas de terceiros) (34)	Não (Integração com ferramentas de terceiros) (25)	Sim (LogRhythm Threat Intelligence Services (TIS)) (46)	Sim (47)
Normalização de Dados (Parser Normalization)	OSSEM (9)	Exabeam Auto Parser Generator (APG) (32)	MDI Fabric (45)	CIM (10)

Obs.: Os campos que estão em branco ainda não foram possíveis identificar a informação pública no site do fabricante.

Fontes:
1 https://marketplace.fedramp.gov/#!/products
2 http://www.planalto.gov.br/ccivil_03/_ato2019-2022/2020/decreto/D10222.htm
3 https://www.splunk.com/pdfs/legal/splunk-ISO-27001-certificate.pdf
4 https://techcommunity.microsoft.com/t5/azure-sentinel/what-s-new-cybersecurity-maturity-model-certification-cmmc/ba-p/2111184

5 https://docs.microsoft.com/en-us/azure/sentinel/connect-data-sources
6 https://azure.microsoft.com/en-us/pricing/details/monitor/
7 https://techcommunity.microsoft.com/t5/azure-sentinel/azure-sentinel-the-connectors-grand-cef-syslog-direct-agent/ba-p/803891
8 https://www.splunk.com/en_us/software/pricing.html
9 https://ossemproject.com/intro.html
10 https://docs.splunk.com/Documentation/CIM/4.18.0/User/UsetheCIMtonormalizedataatsearchtime
11 https://docs.splunk.com/Documentation/StreamApp/7.3.0/DeployStreamApp/UseStreamtoingestNetflowandIPFIXdata
12 https://conf.splunk.com/files/2019/slides/SECS2899.pdf
13 https://docs.microsoft.com/en-us/azure/sentinel/microsoft-365-defender-sentinel-integration
14 https://docs.splunk.com/Documentation/SplunkCloud/8.1.2101/Service/SplunkCloudservice
15 https://www.splunk.com/en_us/blog/tips-and-tricks/getting-microsoft-azure-data-into-splunk.html
16 https://splunkbase.splunk.com/
17 https://docs.splunk.com/Documentation/Splunk/8.1.2/Indexer/forwardersdirecttopeers
18 https://www.splunk.com/en_us/download/universal-forwarder.html
19 https://www.exabeam.com/wp-content/uploads/2020/02/EXA_Data-Sheet_Cloud-Platform.pdf
20 https://www.exabeam.com/newsroom/exabeam-expands-international-availability-of-cloud-based-siem-to-help-organizations-modernize-security-operations/
21 https://www.exabeam.com/siem-guide/siem-architecture/
22 https://www.exabeam.com/siem-guide/siem-buyers-guide/
23 https://www.exabeam.com/information-security/machine-learning-for-cybersecurity/
24 https://www.exabeam.com/product/cloud-connectors/
25 https://www.exabeam.com/wp-content/uploads/2020/03/Data-Integrations-WP-Mar20.pdf
26 https://docs.exabeam.com/en/data-lake/i35/data-lake-user-guide/111941-exabeam-data-lake-reports.html#UUID-486e3195-13c5-8e7d-3569-2de7f762228e
27 https://www.exabeam.com/siem-guide/siem-architecture/#sizing
28 https://www.splunk.com/en_us/app-integrations.html
29 https://docs.exabeam.com/en/data-lake/i36/exabeam-data-lake-collector-guide/119236-exabeam-data-lake-agent-log-collectors.html
30 https://docs.exabeam.com/en/aws/all/amazon-web-services-setup-guide/UUID-d5c8b4f7-e188-c622-9722-16408f646425.html
31 https://docs.exabeam.com/en/content/all/how-content-works-guide/53754-event-types-and-required-fields.html
32 https://www.exabeam.com/siem/auto-parser-generator-now-available-for-customers/
33 https://docs.microsoft.com/en-us/learn/modules/incident-management-sentinel/
34 https://docs.microsoft.com/pt-br/azure/sentinel/import-threat-intelligence
35 https://logrhythm.com/wp-content/uploads/2020/03/logrhythm-cloud-data-sheet-1.pdf
36 https://logrhythm.com/products/logrhythm-user-xdr/
37 https://gallery.logrhythm.com/joint-solution-briefs/logbinder-for-exchange-joint-solution-brief.pdf
38 https://gallery.logrhythm.com/data-sheets/logrhythm-for-compliance-data-sheet.pdf
39 https://gallery.logrhythm.com/terms-and-conditions/logrhythm-cloud-security-overview-final-2019-05.pdf
40 https://gallery.logrhythm.com/terms-and-conditions/logrhythm-cloud-security-overview-final-2019-05.pdf
41 https://logrhythm.com/solutions/security/cloud-security/
42 https://gallery.logrhythm.com/data-sheets/endpoint-monitoring-and-forensics-data-sheet.pdf
43 https://gallery.logrhythm.com/data-sheets/na-data-sheet-sysmon.pdf
44 https://docs.logrhythm.com/docs/sysmon/system-monitor-installation-guide/networking-and-communication
45 https://gallery.logrhythm.com/data-sheets/data-processing-and-indexing-tiers-data-sheet.pdf
46 https://logrhythm.com/blog/logrhythm-threat-intelligence-services-stix-via-taxii/
47 https://www.splunk.com/en_us/resources/videos/splunk-threat-intelligence-demo.html

5.7.2. Observa-se conforme Tabela acima que a Plataforma da Microsoft - Azure Sentinel é um produto o qual possui todos os requisitos e funcionalidades comuns para o segmento.

5.7.3. Após a avaliação técnica, essa equipe de planejamento da contratação realizou uma comparação de preços entre as soluções comercializada no pais e com objetivo de avaliar custos entre as opções de solução disponíveis no mercado nacional como serviço que compõe (software e hardware), foi realizado uma pesquisa entre as tecnologias que possuem preços públicos na internet bem como preços público presente na ATA do Pregão 01/2020 do Conselho da Justiça Federal, apresentados na tabela a seguir.

Tabela 15 - Comparação de Preços Públicos entre os softwares de SOC

Comparação de Preços Públicos entre os softwares de SOC										
		Microsoft			**RSA - Empresa ISH (Pregão 01/2020 - CJF)**		**Logrhythm - Empresa APURA (Pregão 01/2020 - CJF)**		**ELK - Empresa NCT (Pregão 02/2020 - CJF)**	
Produtos Cloud envolvidos	**SOAR**	**1 - Azure Sentinel 2 - Log Analytics do Azure Monitor**			**Item 5 - RSA Netwitness Orchestrator**		**Item 5 - LogRhythm**		**Item 5 - ServiceNow**	
	Endpoint Análise				**Item 3 - TENABLE NESSUS, ACUNETIX e RSA Archer VM**		**Item 3 - Tenable**		**Item 3 - Qualys**	
	Network Análise				**Item 4.3 - NTA RSA Netwitness Packets**		**Item 4.3 - LogRhythm**		**Item 4.3 - ELK/IXIA/VIAVI**	
	UEBA				**Item 4.2 - UBA - RSA UEBA Essentials + Analytics**		**Item 4.2 - LogRhythm**		**Item 4.2 - ELK**	
	Inteligência de Ameaça				**Item 2 - CTI RSA ARCHER ISSUE**		**Não informado**		**Item 2 - Recorder Future**	
	SIEM				**item 4.1 - RSA Netwitness Logs**		**Item 4.1 0 LogRhythm**		**Item 4.1 - ELK**	
Referência		**Reservado***			**Ata do Pregão (6)**		**Ata do Pregão (6)**		**Ata do Pregão (6)**	
		Item	**Unitário**	**Total (Mensal)**	**Unitário**	**Total (Mensal)**	**Unitário**	**Total (Mensal)**	**Unitário**	**Total (Mensal)**
Logs	**100 GB/dia de logs**	1	R$ 979,78 por dia	R$ 29.393,40	R$ 580,03 por GB ingerido (2)	R$ 58.037,46	R$ 507,05	R$ 50.705,07	R$ 950,71	R$ 95.071,33
		2	R$ 1920,37 por dia	R$ 57.611,10	R$ 4,24 por ativo (3)	R$ 16.960,00	R$ 3,71	R$ 14.851,84	R$ 6,96	R$ 27.847,56
	Processamento de 1 Gbps de volume de rede	N/A	R$ 0,00 incluído (1)	R$ 0,00 incluído (1)	R$ 13261,75 para 1Gbps (4)	R$ 13.261,75	R$ 4.681,28	R$ 4.681,28	R$ 8.777,42	R$ 8.777,42
Endpoits	**4000**	N/A	R$ 0,00 incluído (1)	R$ 0,00 incluído (1)	R$ 11,36 por endpoint (5)	R$ 45.440,00	R$ 4,73	R$ 18.920,00	R$ 10,33	R$ 41.333,33
Total Mês				**R$ 87.004,50**		**R$ 133.699,21**		**R$ 89.158,19**		**R$ 173.029,65**
Total Ano				**R$ 1.044.054,00**		**R$ 1.604.390,52**		**R$ 1.069.898,24**		**R$ 2.076.355,76**

Obs.: Foram considerando apenas os itens de software do Pregão do CJF e os valores constante na Ata do Pregão 01/2020 (http://comprasnet.gov.br/livre/pregao/ata2.asp?co_no_uasg=90026&numprp=000012020&f_lstSrp=T&f_Uf=DF&f_numPrp=12020&f_coduasg=&f_tpPregao=E&f_lstICMS=T&f_dtAberturaIni=&f_dtAberturaFim=)
* Retenção gratuita por 90 dias
https://azure.microsoft.com/pt-pt/pricing/details/azure-sentinel/
https://azure.microsoft.com/pt-pt/pricing/details/monitor/
1 - Azure Activity Logs, Office 365 Audit Logs (all SharePoint activity and Exchange admin activity) and alerts from Microsoft Defender products (Azure Defender, Microsoft 365 Defender, Microsoft Defender for Office 365, Microsoft Defender for Identity, Microsoft Defender for Endpoint), Azure Security Center, Microsoft Cloud App Security, and Azure Information Protection can be ingested at no additional cost into both Azure Sentinel, and Azure Monitor Log Analytics. não faz parte do os logs do Azure Active Directory conforme link https://azure.microsoft.com/pt-pt/pricing/details/azure-sentinel/ na aba de FAQ.
2 - Item 4.1 do edital do CJF ao custo mensal de R$ 8.705,62 para 15GB/dia.
3 - Item 4.2 do edital do CJF ao custo mensal de 4.249.97 para 1000 ativos.
4 - Item 4.3 do edital do CJF ao custo mental de 13.261,75 para processar no mínimo 1 Gbps.
5 - Item 3 do edital do CJF ao custo mensal dividido por 1500 endpoint.
6 - Para chegar ao valor dos itens 4.1, 4.2 e 4.3 foram identificados na proposta original da empresa o percentual correspondente ao item 4 e assim utilizado.

5.7.4. Na realização da pesquisa e sua comparação identificou-se que o produto da Microsoft Azure Sentinel frente aos demais produtos (RSA, Logrhythm e ELK) não cobra pelo processamento de tráfego de rede e monitoramento de dispositivos endpoint, cujo os produtos são Microsoft, diferente dos demais, o que apresenta ser uma estratégia de mercado adotado pelos fabricantes na comercialização de seus produtos, pois o somatório de todos os produtos/serviços se mostra mais vantajoso quando do produto da Microsoft Azure Sentinel é comparado.

5.7.5. Diante dos preços mensais e totais constantes na tabela acima é possível identificar que a média mensal de preço das soluções pesquisada foi de R$ 111.428,70 e o melhor valor foi da Plataforma da Microsoft Azure Sentinel, o que demonstra que a permanência da **Plataforma de SIEM/SOAR/NTA/UEBA/CTI do Ministério, Microsoft Azure Sentinel,** representa o melhor custo beneficio para a administração bem como, a melhor estratégia da presente contratação.

5.8. **Dimensionamento da força de trabalho pela CONTRATADA.**

5.8.1. Para o dimensionamento da força de trabalho da CONTRATADA, o fluxo de dados do Ministério a ser considerado de forma escalável, sob demanda e de acordo com o item 6.2.1.1.12, será conforme segue;

Tabela 16 - Fluxo de dados do Ministério coletado pela Plataforma de SIEM/SOAR/NTA/UEBA/CTI do Ministério

Descrição	Estimativa adicionais a serem dimensionados de acordo com a demanda e utilização	Quantidade Estimada inicial (GB/dia e EPS)	Retenção Hot e Warm (Tipo 1)	Retenção Cold (Tipo 2)	Retenção Frozen (Tipo 3)
Logs de ambiente em Nuvem (Azure e Oracle Cloud)	5 x 100GB/dia | 2.000 EPS	5 GB/dia | 100 EPS	1 mês	6 meses	12 meses
IDS Aletas e Logs de ativos de segurança		30 GB/dia | 1000 EPS	15 dias	6 meses	12 meses
NetFlow/SFlow logs		10 GB/dia | 300 EPS	1 mês	6 meses	12 meses
Logs de auditoria (Sistemas, serviços e servidores e endpoint)		55 GB/dia | 600 EPS	72 horas	6 meses	12 meses
Quantitativo máximo	**500GB/dia | 12.000 EPS**	**100GB/dia | 2.000 EPS**	-	-	-

5.9. **Itens que compõe a pretensa contração**

5.9.1. A tabela 17 apresenta os itens a serem contratados, para o período de dois anos (24 meses).

Tabela 17 - Itens a serem contratados

Grupo	Item	Descrição do item	Quantidade	Métrica ou Unidade	Forma
1	1	Serviço de Security Operations Center - SOC	24	Unidade (Mensal)	Contínuo
	2	Serviço de Tratamento e Resposta aos Incidentes Cibernéticos - CSIRT - Blue Team	24	Unidade (Mensal)	Contínuo
2	3	Serviço de Teste de Invasão - Red Team	827	Unidade (Alvos)	Sob demanda

6. **ESTIMATIVA DE CUSTO TOTAL DA CONTRATAÇÃO**

6.1. A estimativa de custo total da contratação é apresentada na tabela 18.

Tabela 18 - Estimativa de quantidades e custos

Grupo	Item	Descrição do item	Quantidade	Unidade	Valor Unitário	Valor Mensal máximo (R$)	Valor Total máximo (24 meses) (R$)
1	1	Serviço de Security Operations Center - SOC	24 meses	Unidade (Mensal)	R$ 168.156,00	R$ 168.156,00	R$ 4.035.744,00
	2	Serviço de Tratamento e Resposta aos Incidentes Cibernéticos - CSIRT - Blue Team	24 meses	Unidade (Mensal)	R$ 18.446,40	R$ 18.446,40	R$ 442.713,60
2	3	Serviço de Teste de Invasão - Red Team	827	Unidade (Alvos)	R$ 1.150,84	N/A	R$951.744,68
	Total					**R$ 186.602,40**	**R$ 5.430.202,28**

As valores de referência utilizados para compor a estimativa de custo são os mesmos presentes na tabela 10 - Custo estimado para o MJSP, baseadas no preço final homologado do Pregão 01/2020 do Conselho de Justiça Federal (CJF) que possui objeto similar a essa pretensa contratação.

6.2. A estimativa total da contratação para 24 meses é de R$ 5.430.202,28 (cinco milhões, quatrocentos e trinta mil duzentos e dois reais e vinte e oito centavos) e de R$ 13.575.505,70 (treze milhões, quinhentos e setenta e cinco mil quinhentos e cinco reais e setenta centavos) para cinco anos.

7. **AVALIAÇÃO DAS NECESSIDADES DE ADEQUAÇÃO DO AMBIENTE DO ÓRGÃO**

7.1. **Não** é necessário adequar o ambiente da infraestrutura física das instalações do Ministério para viabilizar a entrega ou a execução contratual.

7.2. **Não** é necessário adequar o ambiente da infraestrutura elétrica para viabilizar a entrega ou a execução contratual.

8. **RECURSOS HUMANOS**

8.1. Gestor do contrato– responsável pela gestão do contrato, no âmbito do Ministério;

8.2. Fiscal Técnico do contrato– responsável pela fiscalização do contrato, no âmbito da DTIC;

8.3. Fiscal Administrativo do contrato – responsável pela fiscalização do contrato, no âmbito da CGL;

8.4. Fiscal Requisitante do contrato - responsável pela fiscalização do contrato, no âmbito da Unidade Requisitante;

8.5. Equipe técnica– formada por servidores da equipe de CRS da DTIC responsáveis pelo acompanhamento de chamados técnicos, de execução de configurações e dos serviços contratado.

9. **RECURSOS MATERIAIS**

9.1. Será necessário disponibilizar mobiliário e computadores nas dependências do MJSP para prestação de serviços, quando a CONTRATA informar necessidade.

10. **DECLARAÇÃO DE VIABILIDADE DA CONTRATAÇÃO**

10.1. 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) (14424141), sendo descritas e tratadas como macro requisitos e necessidades de negócio como serviço para tal finalidade.

10.2. Foram avaliadas as soluções disponíveis no mercado quanto à viabilidade técnica e econômica para o atendimento das necessidades deste órgão.

10.3. 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.

11. **APROVAÇÃO E ASSINATURA**

11.1. A Equipe de Planejamento da Contratação foi instituída pela PORTARIA DE PESSOAL SAA/SE/MJSP Nº 1, DE 08 DE JANEIRO DE 2021 (13636809), alterado pela PORTARIA SAA/SE/MJSP Nº 57, DE 11 DE MAIO DE 2021 (14627967).

11.2. 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	INTEGRANTE REQUISITANTE
Cintia Mye Yonekawa Yamaguti **Matrícula/SIAPE:** 3201981	Ivanildo de Oliveira da Silva JR **Matrícula/SIAPE:** 2535600

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 **Cintia Mye Yonekawa Yamaguti**, **Integrante Técnico(a)**, em 14/10/2021, às 16:26, com fundamento no § 3º do art. 4º do Decreto nº 10.543, de 13 de novembro de 2020.

Documento assinado eletronicamente por **IVANILDO DE OLIVEIRA DA SILVA JUNIOR**, **Integrante Requisitante**, em 14/10/2021, às 17:03, com fundamento no § 3º do art. 4º do Decreto nº 10.543, de 13 de novembro de 2020.

Documento assinado eletronicamente por **Rodrigo Lange**, **Diretor(a) de Tecnologia da Informação e Comunicação**, em 15/10/2021, às 11:38, 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 **15854445** e o código CRC **4B9B4C8C**
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.

15854396 08006.000003/2021-38

MINISTÉRIO DA JUSTIÇA E SEGURANÇA PÚBLICA
Secretaria-Executiva
Coordenação de Riscos e Segurança de TIC

ANEXOS DA MINUTA DO TERMO DE REFERÊNCIA

ANEXO I-A

PROPOSTA DE PREÇOS
(EMITIR EM PAPEL TIMBRADO DA EMPRESA)

PROPOSTA DE PREÇOS

Objeto: Contratação de empresa especializada, para o fornecimento de **Serviço de Centro de Operações de Segurança - SCO (Security Operations Center - SOC) remoto com funcionamento e suporte de primeiro nível 24h por dia e 7 dias por semana, Serviço de tratamento e resposta aos incidentes cibernéticos - CSIRT - Blue Team e Serviço de teste de invasão - Red Team** e garantia dos serviços pelo período de 24(vinte e quatro) meses, renováveis até o limite de 60 (sessenta) meses, para o atendimento das necessidades da Diretoria de Tecnologia da Informação e Comunicação - DTIC do Ministério da Justiça e Segurança Pública - MJSP, de acordo com as especificações técnicas contidas neste Termo de Referência – TR 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 CATSER	Descrição do Bem ou Serviço	Quantidade	Métrica ou Unidade de medida	Valor Unitário (R$)	Valor Mensal (R$)	Valor Total (24 meses) (R$)
1	1	26000	Serviço de Security Operations Center - SOC	24	Unidade (Mensal)			
	2	26000	Serviço de Tratamento e Resposta aos Incidentes Cibernéticos - CSIRT - Blue Team	24	Unidade (Mensal)			
2	3	26000	Serviço de Teste de Invasão - Red Team: Sistemas Web	217	Unidade (Alvo)			
	4	26000	Serviço de Teste de Invasão - Red Team: Infraestrutura	610	Unidade (Alvo)			
Valor Global (Somatório do Valor Total 24 meses)								

Tabela 1 - Quantitativos a serem registrados

A empresa XXX apresenta a proposta no valor global de R$ YYYY (por extenso).

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

ORDEM DE SERVIÇO N°		DATA:	
		HORA:	
1. IDENTIFICAÇÃO DO SOLICITANTE			
Nome:	E-mail:		
Fone/Ramal:	Assinatura do Solicitante:		
2. SERVIÇO A EXECUTAR			
EMPRESA RESPONSÁVEL:			
LOCAL/REFERÊNCIA:			
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. MATERIAL EMPREGADO			
Item	Descrição	Unidade/Tipo	Quantidade
1			
2			
3			
4			
6. DATA E HORÁRIO DO INÍCIO E TÉRMINO DOS SERVIÇOS (desconsiderar intervalos)			
Data de início do serviço	Hora	Data de término do serviço	Hora
___/__/___	___:___ hs	___/__/___	___:___ hs
7. ACEITE DO SERVIÇO			
Declaro que o serviço acima solicitado, foi executado, considerando aceito o serviço			

Data ___/__/___	Hora ___:___ hs	Ass. e carimbo solicitante:

ANEXO I-C

RELATÓRIO DE CHAMADO TÉCNICO – RCTA

ORDEM DE SERVIÇO Nº:		***DATA:***	
		HORA:	

1. ***IDENTIFICAÇÃO DO SOLICITANTE***

Resp. Solicitante:		*CICC:*	
Nome:		*E-mail:*	
Fone/Ramal:		*Ass. e carimbo:*	_____

2. ***SERVIÇOS A EXECUTAR***

Severidade do evento:	*Não crítica*	*Baixa*	*Média*	*Alta*	*Grave*
Empresa Responsável:					
Nome do(a) atendente:					

1. ***HORÁRIO (SLA – ATENDIMENTO)***		***DATA ___ / ___ / ___***	
Início:		*Chegada:*	
Término:		*Saída:*	
Total de horas:		*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 o 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>* Matrícula: *<Matr.>*	_____ *<Nome>* *<Qualificação>*
Testemunhas	
Testemunha 1	**Testemunha 2**
_____ *<Nome>* *<Qualificação>*	_____ *<Nome>* *<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 2021.

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 08006.000003/2021-38, 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:								
Período:			Carga Horária:					
Instrutor:								
Aluno(a):								
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 **Assinale apenas uma das graduações, observando as correspondências.**								
Não se Aplica	**Ruim (R)**	**Bom (B)**	**Ótimo (O)**	**Excelente (E)**				
	O que é Ruim? "Algo considerado abaixo do padrão"	O que é Bom? Algo considerado "conforme", "de acordo", mas que pode melhorar; Algo que cumpre com as obrigações, porém sem superar as expectativas.	O que é Ótimo? Algo considerado "o melhor possível" dentro das condições em que se atua.	O que é Excelência? Algo que é superior na Qualidade; Algo que é Perfeito; Algo que é Magnífico.				
CONTEÚDO PROGRAMÁTICO				**0**	**1**	**2**	**3**	**4**
Material didático (apostilas, livros, exercícios, etc.)								
O conteúdo da matéria apresenta durante o curso								
Ordem e distribuição dos assuntos apresentados								
A duração (carga horária) do curso								
Recursos audiovisuais (quadro, retroprojetor, micros, RH, etc.)								
Condições de equipamentos utilizados (micros, retroprojetor, etc.)								
INSTRUTOR				**0**	**1**	**2**	**3**	**4**
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 do formador quanto ao cumprimento do horário								
Aproveitamento do tempo quanto ao cumprimento do programa								
AUTO AVALIAÇÃO				**0**	**1**	**2**	**3**	**4**
Interesse e participação das atividades em sala de aula								
Aplicabilidade do curso em rotina de trabalho								

Relacionamento com o instrutor					

1) Os conhecimentos adquiridos neste curso serão aplicáveis em sua atividade de trabalho? Como?
2) Comentários/Sugestões:

Assinatura: _____

CPF: _____

Brasília, ____/_____/_____

ANEXO I-L

TERMO DE RECEBIMENTO PROVISÓRIO

INTRODUÇÃO
O Termo de Recebimento Provisório declarará formalmente à Contratada que os serviços foram prestados ou que os bens foram recebidos para posterior análise das conformidades e qualidade, baseadas nos requisitos e nos critérios de aceitação definidos no Modelo de Gestão do Contrato. **Referência: Inciso XXI, Art. 2º, e alínea "a", inciso II, art. 33, da IN SGD/ME Nº 1/2019.**

1 – IDENTIFICAÇÃO

CONTRATO Nº	xx/aaaa		
CONTRATADA	<Nome da Contratada>	**CNPJ**	xxxxxxxxxxx
Nº DA OS/OFB	<xxxx/aaaa>		
DATA DA EMISSÃO	<dd/mm/aaaa>		

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

3 – RECEBIMENTO
Por este instrumento, atestamos, para fins de cumprimento do disposto no art. 33, inciso II, alínea "a", da IN SGD/ME nº 01/2019, atualizada pela IN SGD/ME nº 31/2021, que os <serviços / bens> correspondentes à <OS/OFB> acima identificada, conforme definido no Modelo de Execução do contrato supracitado, foram recebidos provisoriamente na presente data e serão objetos de avaliação por parte da **CONTRATANTE** quanto à adequação da entrega às condições contratuais, de acordo com os Critérios de Aceitação previamente definidos no Modelo de Gestão do contrato. Ressaltamos que o recebimento definitivo destes serviços ocorrerá após a verificação dos requisitos e demais condições contratuais, desde que não se observem inconformidades ou divergências quanto às especificações constantes do Termo de Referência e do Contrato acima identificado que ensejem correções por parte da **CONTRATADA**.

4 – ASSINATURAS

FISCAL TÉCNICO
_____ <Nome do Fiscal Técnico do Contrato> **Matrícula:** xxxxxx <Local>, <dia> de <mês> de <ano>.
PREPOSTO
_____ <Nome do Preposto do Contrato> **Matrícula**: xxxxxx <Local>, <dia> de <mês> de <ano>.

ANEXO I-M

TERMO DE RECEBIMENTO DEFINITIVO

INTRODUÇÃO

O Termo de Recebimento Definitivo declarará formalmente à Contratada que os serviços prestados ou que os bens fornecidos foram devidamente avaliados e atendem aos requisitos estabelecidos e aos critérios de aceitação.

Referência: Alínea "f", inciso II, e alínea "d", inciso III, do art. 33, da IN SGD/ME Nº 1/2019.

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

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

3 – ATESTE DE RECEBIMENTO

Por este instrumento atestamos, para fins de cumprimento do disposto na alínea "f", inciso II, e alínea "d", inciso III, do art. 33, da IN SGD/ME Nº 1/2019, alterada pela IN SGD/ME nº 31/2021, que os <serviços / bens> correspondentes à <OS/OFB> acima identificada foram <prestados/entregues> pela **CONTRATADA** e atendem às condições contratuais, de acordo com os Critérios de Aceitação previamente definidos no Modelo de Gestão do Termo de Referência do Contrato acima indicado.

4 – DESCONTOS EFETUADOS E VALOR A LIQUIDAR

De acordo com os critérios de aceitação e demais termos contratuais, <não> há incidência de descontos por desatendimento dos indicadores de níveis de serviços definidos.
<Não foram / Foram> identificadas inconformidades técnicas ou de negócio que ensejam indicação de glosas e sanções, <cuja instrução corre em processo administrativo próprio (nº do processo)>.
Por conseguinte, o valor a liquidar correspondente à <OS/OFB> acima identificada monta em R$ <valor> (<valor por extenso>).
Referência: <Relatório de Fiscalização nº xxxx ou Nota Técnica nº yyyy>.

5 – ASSINATURA	
FISCAL TÉCNICO	**FISCAL REQUISITANTE**
_____ <Nome do Fiscal Técnico> **Matrícula:** xxxxxxxx <Local>, <dia> de <mês> de <ano>.	_____ <Nome do Fiscal Requisitante> **Matrícula:** xxxxxxxx <Local>, <dia> de <mês> de <ano>.

A equipe de Planejamento da Contratação designada por intermédio da Portaria SAA nº 11, de 29 de abril de 2021, apresenta os Anexos do Termo de Referência para aprovação.

I - **Integrante Requisitante**: Ivanildo de Oliveira da Silva JR, SIAPE 2535600, CPF 031.033.324-59;

II - **Integrante Requisitante substituto:** Joédes Cardoso da Silva, SIAPE 3730955, CPF 523.656.891-91;

III - **Integrante Técnico**: Cintia Mye Yonekawa Yamaguti, SIAPE 3201981, CPF 619.425.371-15;

III - **Integrante Técnico**: Ivanildo de Oliveira da Silva JR, SIAPE 2535600, CPF 031.033.324-59; e

IV - **Integrante Administrativo**: Gustavo Henrique Corrêa de Paula Maciel, CPF nº 916.497.571-15.

Aprovo o presente Termo de Referência nos termos do Art. 11 da Portaria SE nº 1.008, de 25 de Abril de 2019.

Diretor de Tecnologia da Informação e Comunicação

RODRIGO LANGE

Matrícula: 1558579

Documento assinado eletronicamente por **Cintia Mye Yonekawa Yamaguti**, **Integrante Técnico(a)**, em 14/10/2021, às 17:03, com fundamento no § 3º do art. 4º do Decreto nº 10.543, de 13 de novembro de 2020.

Documento assinado eletronicamente por **IVANILDO DE OLIVEIRA DA SILVA JUNIOR**, **Integrante Requisitante**, em 14/10/2021, às 17:03, com fundamento no § 3º do art. 4º do Decreto nº 10.543, de 13 de novembro de 2020.

Documento assinado eletronicamente por **Gustavo Henrique Correa de Paula Maciel**, **Integrante Administrativo**, em 14/10/2021, às 18:21, com

fundamento no § 3º do art. 4º do Decreto nº 10.543, de 13 de novembro de 2020.

Documento assinado eletronicamente por **Rodrigo Lange**, **Diretor(a) de Tecnologia da Informação e Comunicação**, em 15/10/2021, às 11:38, 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 **15854396** e o código CRC **35FC9A1E**

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 08006.000003/2021-38 SEI nº 15854396

16826244 08006.000003/2021-38

MINISTÉRIO DA JUSTIÇA E SEGURANÇA PÚBLICA
Esplanada dos Ministérios, Bloco T, Anexo II, 6º Andar, Sala 621 - Bairro Zona Cívico Administrativa, Brasília/DF, CEP 70064-900
Telefone: (61) 2025-9301 e Fax: @fax_unidade@ - https://www.justica.gov.br

ANEXO DO TERMO DE REFERÊNCIA
PREGÃO ELETRÔNICO Nº **21/2021**
PROCESSO Nº 08006.000003/2021-38

MODELO DE DECLARAÇÃO DE INEXISTÊNCIA DE VÍNCULO FAMILIAR

A empresa _____ (razão social da empresa) inscrito no CNPJ nº xx.xxx.xxx/xxxx-xx com sede (endereço completo) por intermédio de ser representante legal _____ (***nome representante legal ou procurador***,) infra-assinado, portador da Carteira de Identidade nº XXXXXXX e CPF nº XXXXXXXX, para fins do presente processo licitatório em consonância com o artigo 7º do Decreto nº 7.203, de 04 de junho de 2010, **DECLARA**, sob as penas da lei, que não utilizará, na execução do contrato, mão-de-obra de cônjuge, companheiro ou parente em linha reta ou colateral, por consangüinidade 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.

(local e data)

(Assinatura do Representante Legal)
Nome do representante legal
(Número da Carteira de Identidade e CPF)

Observações:

1) Esta declaração deverá ser emitida em papel que identifique a licitante.

2) Esta declaração servirá apenas como modelo, o declarante deverá elaborar a sua contendo todos os dados constantes da presente.

Documento assinado eletronicamente por **Ariel Craveiro Noleto**, **Pregoeiro(a)**, em 29/12/2021, às 12:56, 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 **16826244** e o código CRC **7B405C17**
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 08006.000003/2021-38 SEI nº 16826244

16765671 08006.000003/2021-38

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 ... DO EDITAL
MINUTA DE CONTRATO

Minuta de Contrato Nº 9048696/2019-DICON/CCONT/CGL/SAA/SE

*** MINUTA DE DOCUMENTO**

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 E SEGURANÇA PÚBLICA, POR INTERMÉDIO DA DIRETORIA DE TECNOLOGIA DA INFORMAÇÃO E COMUNICAÇÃO E DA COORDENAÇÃO-GERAL DE LICITAÇÕES E CONTRATOS, E A EMPRESA xxxxxxxxxxxxxxxxxx.

PROCESSO Nº 08006.000003/2021-38

A União, representada pelo **MINISTÉRIO DA JUSTIÇA E SEGURANÇA PÚBLICA**, com sede à Esplanada dos Ministérios, CEP 70064-900, Brasília/DF, inscrito no CNPJ sob o n° 00.394.494/0013-70, neste ato representado pelo Diretor de Tecnologia da Informação e Comunicação, Senhor **RODRIGO LANGE**, brasileiro, casado, portador do RG nº 38542508 - SSP PR e CPF nº 017.698.019-95, nomeado por meio da Portaria n° 29 de 2 de janeiro de 2019, publicada no D.O.U de 2 de janeiro de 2019 - Edição Extra, e com delegação de competência fixada pela Portaria SE nº 77, de 17 de janeiro de 2020, publicada no D.O.U. de 20 de janeiro de 2020, e pela Coordenadora-Geral de Licitações e Contratos, Senhora **DÉBORA DE SOUZA JANUÁRIO,** brasileira, solteira, portadora do RG nº 3.558.79980–SSP/SP e do CPF nº 712.315.791-53, nomeada pela Portaria n°1.087, de 06 de novembro de 2015, publicada no D.O.U de 09 de 2015, com delegação de competência fixada pela Portaria SAA nº 37, de 10 de novembro de 2020, publicada no D.O.U de 11 de novembro de 2020, doravante denominada **CONTRATANTE**, e a Empresa **XXXXXXXXXXXXXXXXX.**, inscrita no CNPJ n° XXXXXXXXXX e inscrição estadual n° XXXXXXXX, estabelecida XXXXXXXXXXX - CEP XXXXXXX, neste ato representada pelo Senhor **xxxxxxx**, CPF n° xxxxxxx, RG n° xxxxxx, doravante denominada **CONTRATADA**, tendo em vista o que consta no Processo nº 08006.000003/2021-38, e em observância às disposições da Lei nº 8.666, de 21 de junho de 1993, da Lei nº 10.520, de 17 de julho de 2002, da Lei nº 8.248, de 22 de outubro de 1991, do Decreto nº 9.507, de 21 de setembro de 2018, do Decreto nº 7.174, de 12 de maio de 2010, da Instrução Normativa SGD/ME nº 1, de 4 de Abril de 2019 e da Instrução Normativa SEGES/MPDG nº 5, de 26 de maio de 2017 e suas alterações, resolvem celebrar o presente Termo de Contrato, decorrente do Pregão Eletrônico 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, para o fornecimento de **Serviço de Centro de Operações de Segurança (Security Operations Center - SOC) com funcionamento e suporte 24h por dia e 7 dias por semana, Serviço de tratamento e resposta aos incidentes cibernéticos - CSIRT - Blue Team e Serviço de teste de invasão - Red Team** e garantia dos serviços pelo período de 24(vinte e quatro) meses, renováveis até o limite de 60 (sessenta) meses, para o atendimento das necessidades da Diretoria de Tecnologia da Informação e Comunicação - DTIC do Ministério da Justiça e Segurança Pública - MJSP, 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	Código SIASG CATSER	Descrição do Bem ou Serviço	Quantidade	Métrica ou Unidade	Regime de operação	Forma	Valor Unitário	Valor Total
1	26000	Serviço de Security Operations Center - SOC	24	Unidade (Mensal)	24x7	contínuo		
2	26000	Serviço de Tratamento e Resposta aos Incidentes Cibernéticos - CSIRT - Blue Team	24	Unidade (Mensal)	24x7	contínuo		
3	26000	Serviço de Teste de Invasão - Red Team: Sistemas Web	217	Unidade (Alvo)	N/A	sob demanda		
4	26000	Serviço de Teste de Invasão - Red Team: Infraestrutura	610	Unidade (Alvo)	N/A	sob demanda		

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 60 (sessenta) meses, com base no artigo 57, inciso II, da Lei nº 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:

4.1.1. Programa de Trabalho:

4.1.2. Natureza da Despesa:

4.1.3. Plano Interno:

4.1.4. Ptres:

4.1.5. Fonte:

4.1.6. Ação:

4.1.7. PO:

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

5. **CLÁUSULA QUINTA – PAGAMENTO**

5.1. O prazo para pagamento à CONTRATADA e demais condições a ele referentes encontram-se definidos no Termo de Referência e no Anexo XI da IN SEGES/MP n. 5/2017.

6. **CLÁUSULA SEXTA – REAJUSTAMENTO DE PREÇOS EM SENTIDO AMPLO**

6.1. 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
Coordenadora-Geral de Licitações e Contratos
Ministério da Justiça e Segurança Pública

RODRIGO LANGE
Diretor de Tecnologia da Informação e Comunicação
Ministério da Justiça e Segurança Pública

xxxxxxxxxxxxxxxxxxxxxxx

Representante da Contratada

TESTEMUNHAS:

1. NOME:

CPF:

2. NOME:

CPF:

Documento assinado eletronicamente por **Katia Braga de Faria**, **Chefe da Divisão de Contratos**, em 21/12/2021, às 16:41, 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 **16765671** e o código CRC **B7B8A079**
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 08006.000003/2021-38 SEI nº 16765671