



17308596



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 nº 123, de 14 de dezembro de 2006, da Lei nº 11.488, de 15 de junho de 2007, do Decreto nº 8.538, de 06 de outubro de 2015, aplicando-se, subsidiariamente, a Lei nº 8.666, de 21 de junho de 1993 e as exigências estabelecidas neste Edital.

Data da sessão: 14/03/2022

Horário: 10:00

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 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 nº 7.203, de 04 de junho de 2010);

4.4. Nos termos do art. 7º do Decreto nº 7.203, de 2010, é vedada, ainda, a utilização, na execução dos serviços contratados, de empregado da futura Contratada que seja familiar de agente público ocupante de cargo em comissão ou função de confiança neste órgão contratante.

4.5. Conforme item 3.4.2.7.1 do Termo de Referência, é vedada a contratação de uma mesma empresa para dois ou mais serviços licitados, quando, por sua natureza, esses serviços exigirem a segregação de funções, tais como serviços de execução e de avaliação, mensuração ou apoio à fiscalização, assegurando a possibilidade de participação de todos licitantes em ambos os itens seguindo-se a ordem de adjudicação entre eles (ou lotes/grupos) indicada no subitem seguinte.

4.5.1. Será adjudicado primeiro o grupo 1 e posteriormente o grupo 2.

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

campo próprio do sistema eletrônico, relativo às seguintes declarações:

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

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

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

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

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

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

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

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

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

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

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

4.7. 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 §1º do artigo 57 da Lei n.º 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, §2º 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 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 5º e 8º do Decreto n.º 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 § 3º do artigo 43 da Lei nº 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 nº 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 Information 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) máquinas 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. 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;

9.11.3. 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.

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

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

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

9.11.7. 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 desclassificadas do certame;

9.11.8. Para fins de habilitação, serão aceitos atestados de capacidade técnica emitidos em nome de outra empresa da qual a licitante seja subsidiária integral, desde que na criação da subsidiária tenha havido transferência parcial de patrimônio e de pessoal da controladora. (Acórdão do TCU - 4936/2016)

9.11.9. 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.

9.11.10. 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.

9.11.10.1. 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 17239180)
- 22.13.1.1. ANEXO I - A - PROPOSTA DE PREÇOS (SEI nº 17075464)
- 22.13.1.2. ANEXO I - B - MODELO DE ORDEM DE SERVIÇO – O.S. (SEI nº 17075464)
- 22.13.1.3. ANEXO I - C - RELATÓRIO DE CHAMADO TÉCNICO – RCTA (SEI nº 17075464)
- 22.13.1.4. ANEXO I - D - MODELO DE DECLARAÇÃO DE VISTORIA (SEI nº 17075464)
- 22.13.1.5. ANEXO I - E - TERMO DE CIÊNCIA (SEI nº 17075464)
- 22.13.1.6. ANEXO I - F - TERMO DE COMPROMISSO (SEI nº 17075464)
- 22.13.1.7. ANEXO I - G - MODELO DE DECLARAÇÃO DE RENÚNCIA À VISTORIA (SEI nº 17075464)
- 22.13.1.8. ANEXO I - H - MODELO DE PLANO DE INSERÇÃO (SEI nº 17075464)
- 22.13.1.9. ANEXO I - I - MODELO DE PLANO DE FISCALIZAÇÃO (SEI nº 17075464)
- 22.13.1.10. ANEXO I - J - MODELO DE DECLARAÇÃO DE SUSTENTABILIDADE AMBIENTAL (SEI nº 17075464)
- 22.13.1.11. ANEXO I - K - TERMO DE RECEBIMENTO PROVISÓRIO (SEI nº 17075464)
- 22.13.1.12. ANEXO I - L - TERMO DE RECEBIMENTO DEFINITIVO (SEI nº 17075464)
- 22.13.1.13. ANEXO I - M - ESTUDO TÉCNICO PRELIMINAR (SEI nº 17166682)
- 22.13.1.14. ANEXO I - N - PORTARIA 513 MJSP (SEI nº 15854486)
- 22.13.2. ANEXO II – MINUTA DE TERMO DE CONTRATO (SEI nº 17243768)
- 22.13.3. ANEXO III - MODELO DE DECLARAÇÃO DE INEXISTÊNCIA DE VÍNCULO FAMILIAR (SEI nº 17309079)

EDUARDO DE OLIVEIRA DA ROSA

Pregoeiro



Documento assinado eletronicamente por **EDUARDO DE OLIVEIRA DA ROSA, Pregoeiro(a)**, em 22/02/2022, às 14:15, 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 **17308596** e o código CRC **D5E942C1**

O trâmite deste documento pode ser acompanhado pelo site

<http://www.justica.gov.br/acesso-a-sistemas/protocolo> e tem validade de prova de registro de protocolo no Ministério da Justiça e Segurança Pública.



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

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**, 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 a 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 completude de ativos". Já a disponibilidade é a "propriedade de estar acessível e utilizável sob demanda por uma entidade autorizada". Existem outros 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 prever, detectar e responder efetivamente as ameaças, conforme podemos visualizar na figura 1:

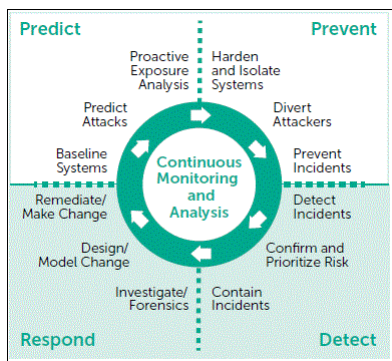


Figura 1 - Gartner, Designing an Adaptive Security Architecture for Protection From Advanced Attacks, February 2014. (retirado da brochura do Kaspersky for Security Operations Center)

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?mc=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, simplificarmente 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

3.1.17. Para a 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.

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. Os itens e os respectivos quantitativos referem-se às necessidades do MJSP, apresentados 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 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.**

3.4.2.7.1. Conforme entendimento da AGU, é vedada a contratação de uma mesma empresa para dois ou mais serviços licitados, quando, por sua natureza, esses serviços exigirem a segregação de funções, tais como serviços de execução e de avaliação, mensuração ou apoio à fiscalização, assegurando a possibilidade de participação de todos licitantes em ambos os itens seguindo-se a ordem de adjudicação entre eles (ou lotes/grupos) indicada no subitem seguinte.

3.4.2.7.2. Será adjudicado primeiro o grupo 1 e posteriormente o grupo 2.

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 controlá-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 responsabilidade 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 móveis;
- 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 12, do Estudo Técnico Preliminar, Anexo I-M, 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.

3.4.5. Justificativa para impedimento da empresa responsável pelo serviço de *service desk* e sustentação de infraestrutura de TI

3.4.5.1. O principal objetivo da empresa responsável pelo serviço de *service desk* e sustentação de infraestrutura do Ministério é manter o pleno funcionamento dos recursos e serviços do ambiente de TIC e melhorar a qualidade dos serviços prestados aos seus usuários, conforme consta no Termo de Referência do Contrato 40/2019. Assim, sua prioridade é garantir a disponibilidade de acordo com os níveis estabelecidos. Importante frisar que por meio desse contrato é disponibilizado um serviço de NOC.

3.4.5.2. Os serviços de SOC e NOC não se confundem em suas atribuições, uma vez que um SOC é responsável pela garantia da tríade de segurança: confidencialidade, integridade e disponibilidade. Por outro lado, a empresa responsável pelo serviço de *service desk* e sustentação de infraestrutura de TI (NOC), concentra-se apenas na disponibilidade, sem considerar os aspectos de segurança.

3.4.5.3. Na prática, a função do NOC é considerada operacional, enquanto o SOC possui impacto estratégico no negócio. Desta forma, a operação e gerenciamento de ambos os serviços são diferentes. Enquanto o NOC trabalha para impedir tempos de inatividade prolongados, que podem facilitar a infestação por *malwares* e monitora continuamente a funcionalidade da rede, evitando que os usuários experimentem lentidão no acesso a internet, por exemplo. Em comparação, o SOC tende a ser mais visível, sua função é prevenir e responder a incidentes de segurança cibernéticos. Por ser altamente especializado, um SOC deve se concentrar inteiramente no monitoramento e gerenciamento de estratégias de segurança.

3.4.5.4. Conforme explicitado anteriormente, os serviços do SOC e do NOC não são conflitantes, uma vez que o NOC foca na disponibilidade e o SOC além da disponibilidade foca também na confidencialidade e integridade. Desse modo, percebe-se que um complementa os serviços do outro. Portanto, não há impedimento da participação da empresa responsável pela empresa de serviço de *service desk* de sustentação de infraestrutura de TI de participar do certame no que se refere ao Grupo 1.

3.4.5.5. Por outro lado, a empresa prestadora de serviço atual de *service desk* e sustentação de infraestrutura de TI fica impedida de participar do Grupo 2 - serviço de Red Team, pois os objetivos são conflitantes. Enquanto o objetivo de uma empresa é manter a disponibilidade, o da outra é encontrar brechas e falhas segurança nos serviços prestados, softwares e hardwares configurados pela primeira. Nessa perspectiva, a ISO 27001 considera a segregação de funções como um controle a ser aplicado para reduzir o risco. Logo, observa-se, nesse caso, justificativa similar àquela descrita no item **Justificativa para divisão em grupos**.

3.4.5.6. Portanto, resta demonstrado, o impedimento da empresa prestadora de serviço atual de *service desk* e sustentação de infraestrutura de TI do Ministério de participar do presente pregão para o grupo 2.

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. Reduzindo os riscos relacionados a perda de dados, comprometimento dos sistemas, ativos críticos e imagem institucional do Ministério.
- 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 segurança, qualidade e eficiência.
- 4.1.4. Aprimorar mecanismos de gestão e de disseminação do conhecimento com foco em segurança da informação. Aumentando a maturidade em segurança da informação.
- 4.1.5. Aprimorar e integrar a gestão e a governança institucional com o fortalecimento das equipes de tratamento de incidentes de segurança e com a instituição de práticas de conformidade e auditoria de Segurança da informação e comunicação.
- 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>.

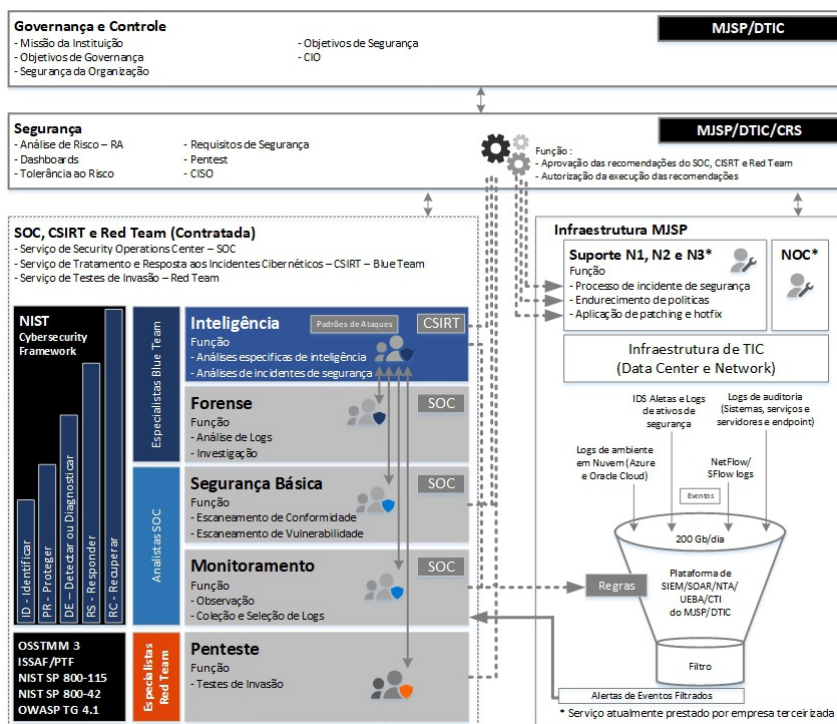


Figura 4 - Diagrama de relacionamento dos serviços e seus respectivos componentes com os demais serviços da DTIC.

4.1.8. Na Figura 4 é apresentado o diagrama de interação, para a presente contratação, 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 papéis:

- 4.1.8.3.1. Inteligência - através da equipe de especialistas Blue Team do CSIRT com as funções de Análise específicas 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 papéis 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 4 (quatro) 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: Sistemas WEB e Serviço de Teste de Invasão - Red Team: Infraestrutura, atendimento sob demanda;**

4.1.9.4. **O Serviço de Security Operations Center - SOCe o Serviço de Tratamento e Resposta aos Incidentes Cibernéticos - CSIRT - Blue Team** atuarão em conjunto e envolve os seguintes serviços, conforme *Information Technology Infrastructure 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.

4.1.9.4.12. 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 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.

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

4.1.9.4.14. 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.

4.1.9.4.15. 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.

4.1.9.4.16. 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.

4.1.9.4.17. 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.

4.1.9.4.18. Apoiar a CRS na divulgação de ações de segurança da informação (Alertas, Consentificação 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.

4.1.9.4.19. 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.

4.1.9.4.20. A CONTRATADA poderá utilizar as ferramentas de Vulnerabilidades em ativos de rede e aplicações Web disponíveis no Ministério. A CONTRATADA também poderá utilizar outras ferramentas de Vulnerabilidades, se julgar necessário, ou para

complementar as ferramentas disponíveis, desde que não tenha custos para a CONTRATANTE.

4.1.9.5. O **Serviço de Teste de Invasão - Red Team** envolve os seguintes serviços, conforme *Information Technology Infrastructure 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. Prover conhecimento de qualidade para a organização.

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

4.1.9.5.7. 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. Para os serviços de SOC e BLUE TEAM, 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. Para os serviços de RED TEAM, a CONTRATADA deverá disponibilizar ferramenta *on line* que permita o acompanhamento das Ordens de Serviço e de seus atendimentos, contendo os resultados detalhados dos serviços de teste de invasão.

4.1.9.6.1. As CONTRATADAS deverão fornecer licenças da ferramenta de ITSM e da ferramenta *on line* em número suficiente para o gerenciamento das demandas de TIC da CONTRATANTE.

4.1.9.6.2. Os eventuais custos de licenciamento dessas ferramentas ficarão ao encargo exclusivo da CONTRATADA.

4.1.9.6.3. Todo processo, base de dados, aprendizado e documento produzido em decorrência da prestação dos serviços será de propriedade da CONTRATANTE.

4.1.9.6.4. Caso a ferramenta seja proprietária, deverá ser fornecida a base de dados em formato aberto, de forma a ser possível efetuar a visualização dos chamados e dos históricos de atendimento.

4.1.9.6.5. Promover a transição contratual com transferência da base de dados de conhecimento, da tecnologia e das técnicas empregadas, sem perda de informações, capacitando ao término do contrato, se solicitado, os servidores da CONTRATANTE ou quem por ele for indicado.

4.1.9.6.6. Ao final do contrato, a CONTRATADA promoverá a transição contratual com transferência das 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 e capacitará ao término do contrato, se solicitado, os servidores da CONTRATANTE ou quem por ele for indicado.

4.1.9.7. 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.

4.1.9.8. 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					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	R/C/I	R/C/I	R/C/I	R/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	MUSP/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 (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 negócio 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
		Tempo para remediação da vulnerabilidade	tempo
	Vulnerabilidade	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
	Alerta	Tipos de casos (MITRE ATT&CK)	número
		Tempo por investigação de alerta	tempo
		Índice de geração de alerta	número/escala
	Incidente	Número de alertas que permanecem por analisar (em aberto)	número
		Criticidade de um alerta	escala
		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
	Resiliência	Custo por incidente	valor/texto
		Sucesso na mitigação	número/percentual
		Tempo médio gasto por ataque (MTTA)	tempo
		Eficiência defensiva	escala
		Repercussão do ataque	texto
Pessoas	Performance	Quantidade de interrupções	número e percentual
		Tempo de interrupções	tempo
Gerais	Performance	Número de incidentes encerrados em um turno	número
		Análise de escalção de caso	número
		Taxa de falso positivo	percentual
	Cobertura	Tempo médio de análise	tempo
		Nível de disponibilidade da infraestrutura de SOC	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. Comunicar tempestivamente a contratante medidas a serem tomadas para evitar ou conter incidente.

4.1.14.1.5. Atuar no sentido de interromper um incidente quando a equipe do NOC ou suporte N1, N2 e N3 estiver limitada contratualmente ou em sua capacidade operacional. 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, não definidos inicialmente nos protocolos do item anterior, 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 reuniões 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 poderá servir 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 MUSP.

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 MUSP.

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

4.1.15.1. O **CSIRT - 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 Controls for 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	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
				Quebra de	Informações proprietárias não classificadas, tais como informações de		

	negócio.			propriedade	infraestrutura crítica protegida (PCII), foram acessadas ou exfiltradas		adicionais
				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 essenciais e críticos a nenhum usuário e 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 dispora uma ação ou resposta legal que vai além dos serviços de monitoramento e respostas a incidentes.	Alto	A organização não é mais capaz de fornecer alguns serviços essenciais e críticos a nenhum usuário e 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	Não Recuperável	A recuperação do incidente não é possível (por exemplo, os dados sensíveis exfiltrados e postados publico); 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 Segurança da Informação e Comunicação, visando auxiliar o CONTRATANTE no desempenho de suas atividades tais como, mas não se limitando a estas: verificação 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, executando testes, 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, Exploitation / 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 táticas 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 Controls for 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. Virus, 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 propositalmente (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”.

4.1.16.21. Para a realização dos serviços a CONTRATADA deverá arcar com todos os custos diretos e indiretos inerentes a utilização de soluções tecnológicas e seus licenciamentos necessários.

4.1.16.21.1. Quando a realização dos serviços ocorrer nas instalações da Contratante, a utilização das soluções tecnológicas deverão ser previamente autorizadas pela Contratante.

4.2. **Requisitos de Capacitação**

4.2.1. Para os itens 1, 2, 3 e 4 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 - SISF 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 a 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. O Ministério da Justiça e Segurança Pública somente autorizará que a CONTRATADA faça inventários nos equipamentos/serviços/software quando solicitado formalmente.

4.4.2. A CONTRATADA deve assegurar que as soluções de hardware e software que disponibilizar em complemento as soluções disponíveis no CONTRATANTE, relacionados aos itens do objeto, permaneçam sempre atualizados.

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

4.4.4. 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.

4.5. **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. 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.

4.5.3. 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 serviços 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 o Plano de Implantação e Cronograma Detalhado conforme consta na seção Deveres e responsabilidades da CONTRATADA.

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 dos serviços contratados.

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;

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 como 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 análise forense, como análise 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 (ISC²) ou Certified Cloud Security Professional - CCSP (ISC²) - Pelo menos um profissional;

4.12.13.3.1.3. CompTIA Cybersecurity 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 análise forense, como análise 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 – GXP (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 de 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 deverá cumprir com as seguintes diretrizes:
- 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 utilize para a prestação de serviços somente serão acessados pelo CONTRATANTE e serão protegidos de acessos de outros clientes e de colaboradores da CONTRATADA;
 - 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.
- 4.15.8. Eventos e incidentes cibernéticos devem ser comunicados através de canais predefinidos de comunicação, disponibilizados pela CONTRATADA, de maneira rápida e eficiente e de acordo com os requisitos legais, regulatórios e contratuais.
- 4.15.9. Para os itens 1 e 2 da Tabela 1, a CONTRATADA 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 constar 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. No caso de a CONTRATADA adotar solução tecnológica complementar, para atender a completa execução dos serviços, objeto da presente contratação, 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: conforme definido no item Mecanismos Formais de Comunicação.

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 MISP 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 MISP.

6.1.4.3. A CONTRATADA deverá disponibilizar números de celular e escala do(s) profissional(is) 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 e 2 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	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 às 23h59 de segunda a domingo (24x7)
		Gerenciamento de Acesso		
		Central de Serviços		
		Gerenciamento de operações de TIC (Controle de Operações de Segurança da Informação)	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 às 23h59 sábado e domingo (24x7)
		Gerenciamento Técnico		
		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: Infraestrutura	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 CONTRATANTE de restabelecimento de equilíbrio econômico-financeiro, bem como, cobranças de horas-extras ou adicionais noturnos.

6.1.4.12. A contratação dos itens mencionados não exige mão de obra com dedicação exclusiva, mas a prestação do serviço dentro dos níveis mínimos de serviços exigidos e com o sigilo adequado, conforme termos e documentações previamente assinadas.

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 locais abrangidos por este contrato devem considerar as localidades remotas, nas quais exista um prolongamento da rede do MJSP, tais como CICCN e penitenciárias federais ligadas ao núcleo central do MJSP, não ensejando a prestação de serviços presenciais da Contratada.

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 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. **Críticas 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 reduções 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 alheios 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 equipamentos 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 cumpre o escopo ou os prazos especificados no Plano de Comunicação para serviços que apresentem 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. 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.
Quantidade de Ataques sofridos					

5	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.		0	
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 - Horas de Manutenção Preventiva - Horas Indisponíveis causadas por Terceiros - Horas Indisponíveis no Mês) / (Horas Totais no Período - 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 fórmula de cálculo 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 recepcionados 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 negócio Baixa -0,4% por impacto ao negócio 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.
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 negócio Baixa -0,5% por impacto ao negócio Média -1% por impacto ao negócio 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 hora.	Total de resposta a incidentes e ou requisições abertos em até 1 hora do recebimento / Total de chamados recebidos x 100%	%	>=80% -0,3% por impacto ao negócio Baixa -0,5% por impacto ao negócio Média -1% por impacto ao negócio 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 negócio Baixa -0,5% por impacto ao negócio Média -1% por impacto ao negócio 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 de 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 MSP 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 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)				
				Quando da ocorrência de atraso até 3 dias a Contratada será glosada conforme segue: -10% por dia de atraso;

14	Índice Ordens de Serviços Cumpridas Dentro do Prazo	Soma da quantidade de dias fora do prazo acordados.	Qt.	=0	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 críticas 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 crítico 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:

$$\begin{aligned} EM &= I \times N \times VP, \text{ sendo:} \\ EM &= \text{Encargos moratórios;} \\ N &= \text{Número de dias entre a data prevista para o pagamento e a do efetivo pagamento;} \\ VP &= \text{Valor da parcela a ser paga.} \\ I &= \text{Índice de compensação financeira} = 0,00016438, \text{ assim apurado:} \\ &\quad \left(\frac{6}{100} \right) \quad I = 0,00016438 \\ I &= (TX) \quad I = \frac{\quad}{365} \quad TX = \text{Percentual da taxa anual} = 6\% \end{aligned}$$

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 corridas 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 nº 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 máximo aceitável (R\$)	Valor Total máximo aceitável (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 Information 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) máquinas 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 desclassificadas do certame;

- 12.3.5. 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;

- 12.3.6. Para fins de habilitação, serão aceitos atestados de capacidade técnica emitidos em nome de outra empresa da qual a licitante seja subsidiária integral, desde que na criação da subsidiária tenha havido transferência parcial de patrimônio e de pessoal da controladora. (Acórdão do TCU - 4936/2016).

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:** Lorena Ayres Leal Lima, SIAPE 1710987.

Aprovo,

Autoridade Máxima da Área de TIC	
Nome	Rodrigo Lange
Cargo	Diretor de TIC
Matricula	1558579

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 - TERMO DE RECEBIMENTO PROVISÓRIO.

ANEXO I - L - TERMO DE RECEBIMENTO DEFINITIVO.

ANEXO I - M - ESTUDO TÉCNICO PRELIMINAR

ANEXO I - N - PORTARIA 513 MJSP



Documento assinado eletronicamente por **Gustavo Henrique Correa de Paula Maciel**, **Integrante Administrativo**, em 15/02/2022, às 14:04, com fundamento no § 3º do art. 4º do Decreto nº 10.543, de 13 de novembro de 2020.



Documento assinado eletronicamente por **Cintia Mye Yonekawa Yamaguti**, **Integrante Técnico(a)**, em 15/02/2022, às 14:11, 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 15/02/2022, às 16:07, 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 15/02/2022, às 16:23, 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 **17239180** e o código CRC **AFCD23B9**.
O trâmite deste documento pode ser acompanhado pelo site <http://www.justica.gov.br/aceso-a-sistemas/protocolo> e tem validade de prova de registro de protocolo no Ministério da Justiça e Segurança Pública.



17075464



08006.000003/2021-38

**MINISTÉRIO DA JUSTIÇA E SEGURANÇA PÚBLICA**

Secretaria-Executiva

Coordenação de Riscos e Segurança de TIC

ANEXOS 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 (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**, 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 do 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, § 3º 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 Nº		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):		
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 ___/202_, cujo objeto é _____,

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.>	

<Nome>
Matrícula: <Matr.>

<Nome>
Matrícula: <Matr.>

_____, _____ de _____ de 20__.

ANEXO I-F

TERMO DE COMPROMISSO

O <NOME DO ÓRGÃO>, sediado em <ENDEREÇO>, CNPJ nº <CNPJ>, doravante denominado CONTRATANTE, e, de outro lado, a <NOME DA EMPRESA>, sediada em <ENDEREÇO>, CNPJ nº <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 ____/202__, bem como seus anexos, pelo que aceitamos seus termos e comprometemo-nos a observá-los integralmente. Declaramos, outrossim, NÃO ter visitado o local dos serviços a serem executados, motivo esse que não poderei alegar o desconhecimento de fatos evidentes à época da vistoria para solicitar qualquer alteração do valor do contrato que vier a celebrar.

Empresa: _____

C.N.P.J.(MF): _____ Tel/Fax: _____

Endereço: _____

Nome do Representante: _____

Endereço Eletrônico (e-mail): _____

Brasília-DF, ...de.....de 202...

Representante da Empresa

Carteira de Identidade - Órgão Emissor

ANEXO I-H

MODELO DE PLANO DE INSERÇÃO

INTRODUÇÃO	
O Plano de Inserção descreverá as atividades de alocação de recursos e preparação das condições necessárias para a contratada iniciar o fornecimento da Solução de TI.	
1 – IDENTIFICAÇÃO	
Contratada	
Nº. do Contrato	
Área Requisitante da Solução	
Gestor do Contrato	
Fiscal Requisitante	
Fiscal Técnico	

Fiscal administrativo				
2 – VISÃO GERAL DO PROJETO				
Justificativa da Contratação				
Objetivos da Contratação				
3 – METODOLOGIA DE TRABALHO				
Forma de Comunicação				
Forma de Encaminhamento das Ordens de Serviço				
Modelo de execução do contrato				
4 – EXECUÇÃO DO CONTRATO				
Ferramentas de Controle				
Id	Ferramenta	Controles		
DOCUMENTAÇÃO MÍNIMA EXIGIDA				
Documento		Finalidade do documento		
PAPEIS E RESPONSABILIDADES				
Id	Papel	Responsabilidades		
PARTES INTERESSADAS				
Id	Área/Órgão/Setor	Impacto		
FATORES CRÍTICOS DE SUCESSO				
PREMISSAS DA CONTRATAÇÃO				
RESTRIÇÕES DA CONTRATAÇÃO				
ENTREGAS PLANEJADAS				
Id	Entrega	Marco	Duração	Data de Entrega
INFRAESTRUTURA A SER DISPONIBILIZADA À CONTRATADA				
Id	Recurso	Início	Fim	

CRITÉRIO DE ACEITAÇÃO – MÉTRICA E PERIODICIDADE		
Métrica 1		
Indicador de Qualidade		
Mínimo aceitável		
Métrica		
Ferramentas		
Periodicidade Aferição		
Métrica “N”		
Indicador de Qualidade		
Mínimo aceitável		
Métrica		
Ferramentas		
Periodicidade Aferição		
RESULTADOS ESPERADOS		
Id	Entrega	Benefícios
5 – INSTRUÇÕES COMPLEMENTARES		
6 - CIÊNCIA		
Fiscais do Contrato		
Fiscal Técnico	Fiscal Requisitante	Fiscal Administrativo
<Nome> Matrícula: <Matr.>	<Nome> Matrícula: <Matr.>	<Nome> Matrícula: <Matr.>
Gestor do Contrato		
<Nome> Matrícula: <Matr.>		
Contratada		
<Nome> CPF/CNPJ: <...>		
Brasília-DF, ...de.....de 202...		

ANEXO I-I

MODELO DE PLANO DE FISCALIZAÇÃO

INTRODUÇÃO
O Plano de Fiscalização descreverá as atividades de acompanhamento e fiscalização da execução do contrato de fornecimento da Solução de

TI		
1 – IDENTIFICAÇÃO DO CONTRATO		
Contrato nº:		
Contratante		
Área Requisitante da Solução		
Fiscal Requisitante		
Fiscal Técnico		
Fiscal Administrativo		
Gestor do Contrato		
Contratada		
CNPJ		
2 – PROCEDIMENTOS DE TESTE DE INSPEÇÃO		
CRITÉRIO DE ACEITAÇÃO – MÉTRICA E PERIODICIDADE		
Métrica 1		
Indicador de Qualidade		
Mínimo aceitável		
Métrica		
Ferramentas		
Periodicidade Aferição		
3 – CONFIGURAÇÃO/CRIAÇÃO DE FERRAMENTAS PARA IMPLANTAÇÃO E ACOMPANHAMENTO DE INDICADORES		
4 – ELABORAÇÃO/REFINAMENTO DAS LISTAS DE VERIFICAÇÃO E DOS ROTEIROS DE TESTE		
FISCAIS DO CONTRATO		
Fiscal Técnico	Fiscal Requisitante	Fiscal Administrativo
_____ <Nome> Matrícula: <Matr.>	_____ <Nome> Matrícula: <Matr.>	_____ <Nome> Matrícula: <Matr.>
GESTOR DO CONTRATO		
_____ <Nome> Matrícula: <Matr.>		
CONTRATADA		

<Nome>
CPF/CNPJ: <...>

Brasília-DF, ...de.....de 202__.

ANEXO I-J

MODELO DE DECLARAÇÃO DE SUSTENTABILIDADE AMBIENTAL

DECLARAÇÃO DE SUSTENTABILIDADE AMBIENTAL

(EMITIR EM PAPEL TIMBRADO DA EMPRESA)

Empresa: _____
C.N.P.J.(MF): _____ Tel/Fax: _____
Endereço: _____
Nome do Representante: _____
Endereço Eletrônico (e-mail): _____

Declaro, sob as penas da Lei nº 6.938/1981, na qualidade de proponente do procedimento licitatório, sob a modalidade Pregão Eletrônico nº _____, instaurado pelo Processo de nº 08006.000003/2021-38, 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

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	xxxxxxxxxxxxx
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-L

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	xxxxxxxxxxxxx
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 Requirante> Matrícula: xxxxxxxx <Local>, <dia> de <mês> de <ano>.

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).

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 Requirante: Ivanildo de Oliveira da Silva JR, SIAPE 2535600, CPF 031.033.324-59;

II - Integrante Requirante substituto: Joêdes 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;

IV - Integrante Técnico Substituto: Madson Luiz Magno da Silva, CPF 047.519.171-45;

V - Integrante Administrativo: Gustavo Henrique Corrêa de Paula Maciel, CPF nº 916.497.571-15 e

VI - Integrante Administrativo Substituto: Lorennay Ayres Leal Lima, SIAPE 1710987.

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 **IVANILDO DE OLIVEIRA DA SILVA JUNIOR, Integrante Requirante**, em 10/02/2022, às 19:53, com fundamento no § 3º do art. 4º do Decreto nº 10.543, de 13 de novembro de 2020.



Documento assinado eletronicamente por **Cintia Mye Yonekawa Yamaguti, Integrante Técnico(a)**, em 11/02/2022, às 08:18, 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 11/02/2022, às 09:30, 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 11/02/2022, às 10:00, 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 **17075464** e o código CRC **43EFE72D**.
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.

Estudo Técnico Preliminar 27/2021

1. Informações Básicas

[Este documento é sigiloso | Justificativa: Documento em validação interna. Não publicado.]

Número do processo: 08006.000003/2021-38

2. 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.

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, 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.

3. Descrição da necessidade

3.1 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.

3.2 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.

3.3 No que diz respeito a diversidade de Tecnologias, quantitativos consolidados, relação de sistemas e outras informações, foram levantadas e o resumo pode ser visualizado na tabela abaixo.

Tabela 1 - Resumo dos itens de infraestrutura

Itens	Descrição	Totais
1.	Equipamentos e tecnologias utilizadas no MJSP	728
2.	Total de estações de trabalho (SEI 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	2

6.	Total de chamados para janeiro e fevereiro 2021 - N3 - Segurança	219

Fonte: Relatório de relatório de informações sobre a infraestrutura

3.4 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.

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

3.5 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:

3.6 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

3.7 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.

3.8 Panorama no Brasil - Estatísticas de incidentes

3.8.1 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.

3.8.2 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.

3.8.3 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.

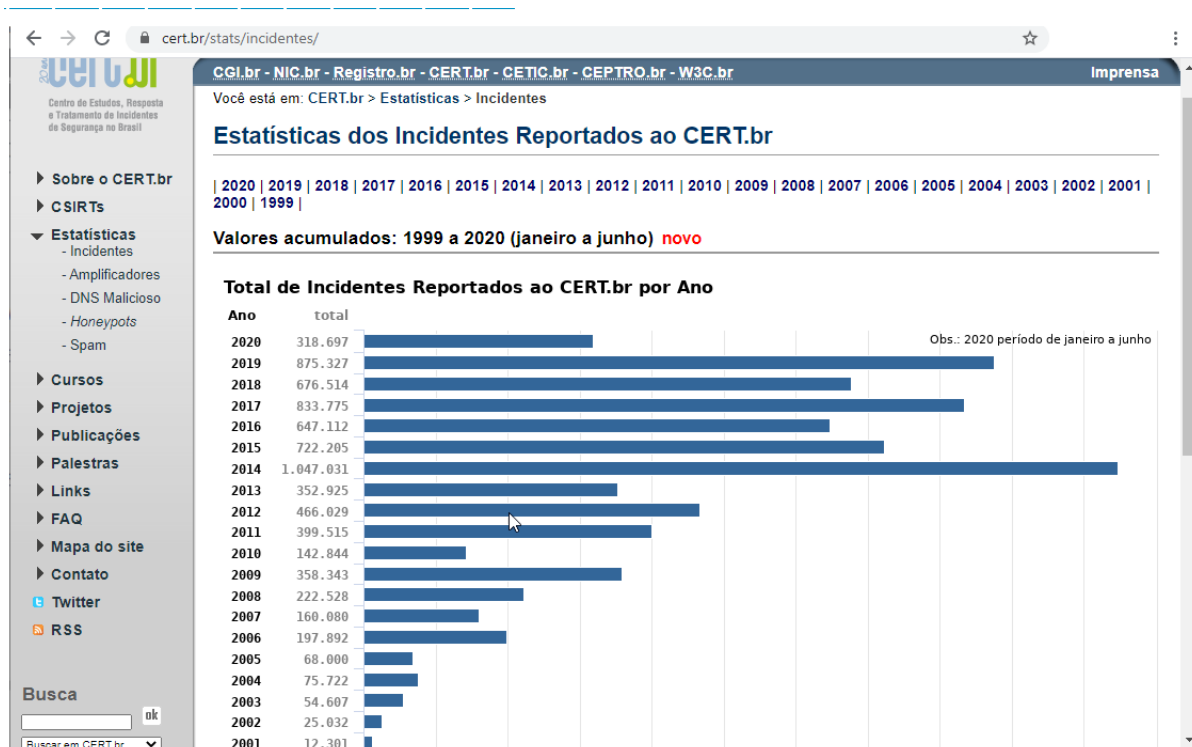


Figura 3 - Total de incidentes reportados, Fonte: CERT.br disponível em <https://www.cert.br/stats/incidentes/> acesso em 13/05/2021.

3.9 Incidentes Reportados ao CERT.br -- Janeiro a Junho de 2020

3.9.1 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	<u>worm</u> (%)		<u>dos</u> (%)		<u>invasão</u> (%)		<u>web</u> (%)		<u>scan</u> (%)		<u>fraude</u> (%)		outros (%)	
<u>jan</u>	35094	6703	19	3579	10	54	0	999	2	20704	59	2701	7	354	1
<u>fev</u>	40229	8215	20	7424	18	52	0	897	2	21184	52	2319	5	138	0
<u>mar</u>	63313	9316	14	16837	26	93	0	1045	1	31633	49	3111	4	1278	2
<u>abr</u>	55255	7680	13	6092	11	110	0	1458	2	36287	65	3537	6	91	0
<u>mai</u>	59820	10698	17	4815	8	122	0	2225	3	38389	64	3512	5	59	0
<u>jun</u>	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.

3.9.2 A figura 4 apresenta de forma gráfica os tipos de ataque.

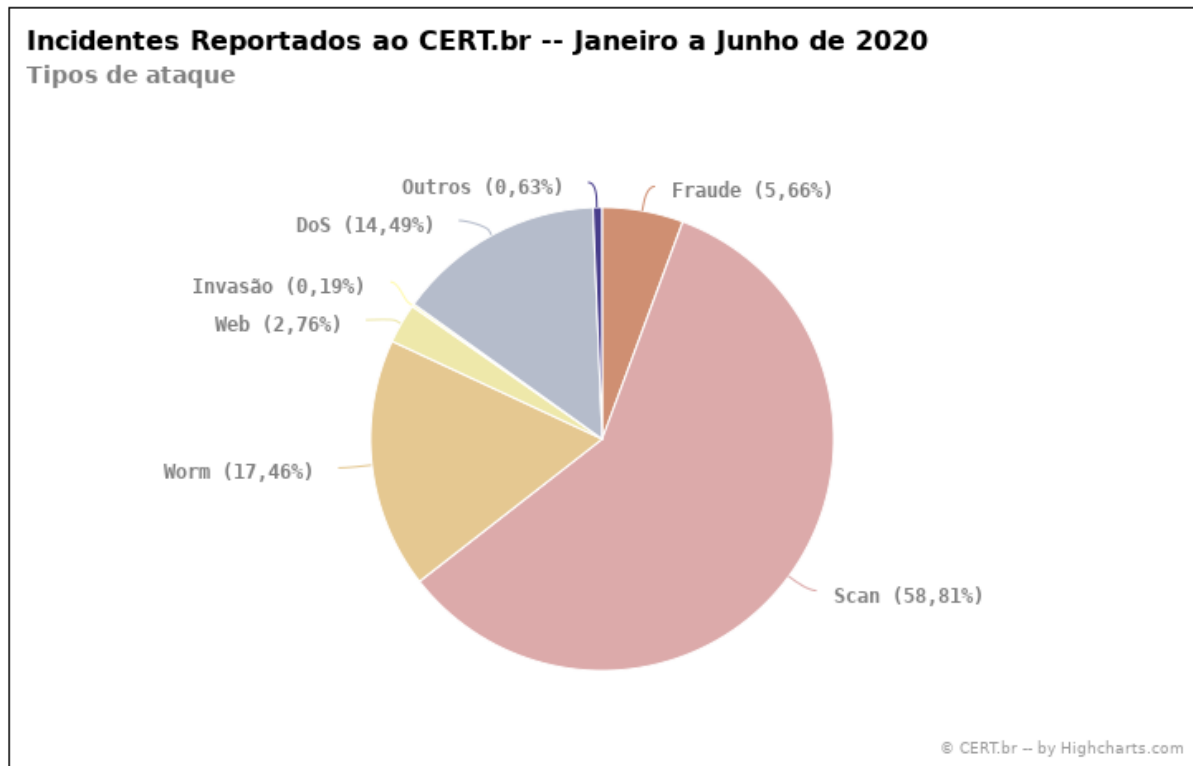


Figura 4 - Tipos de ataque - Fonte: CERT.br disponível em <https://www.cert.br/stats/incidentes/2020-jan-jun/tipos-ataque.html> acesso em 13/05/2021.

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.

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.

3.10 A figura 5 relaciona os scans reportados por porta .

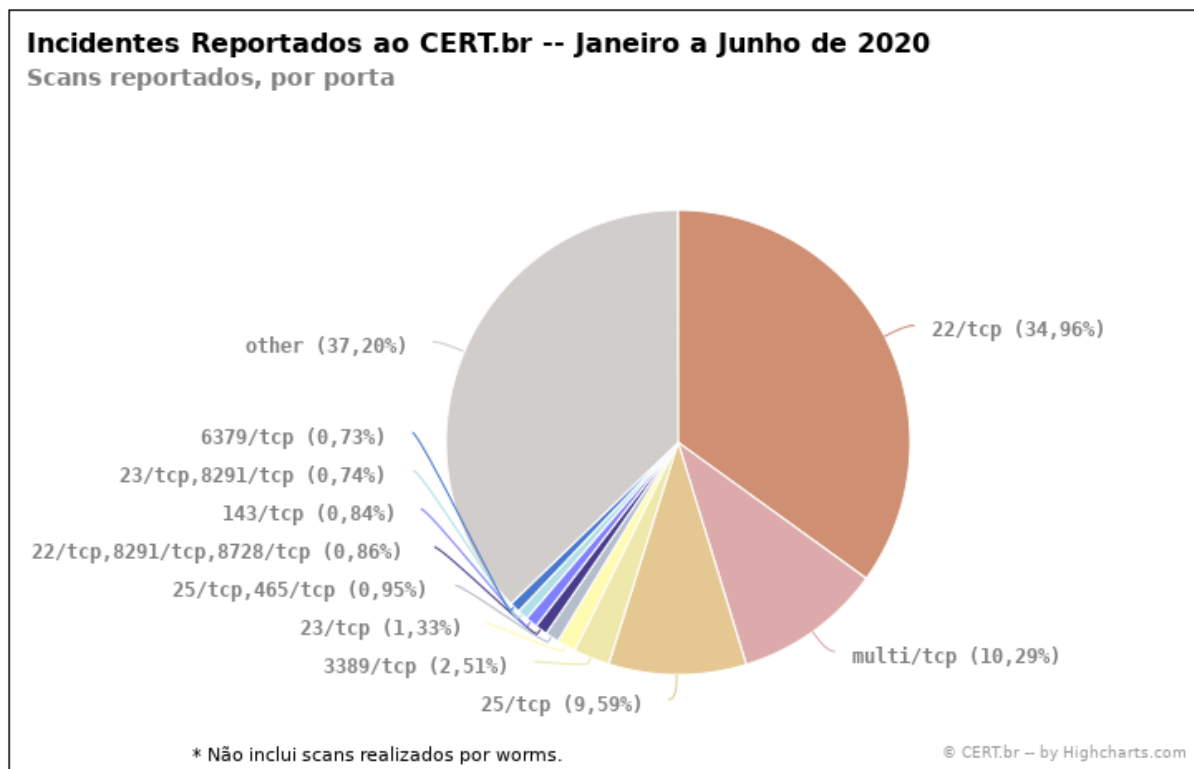


Figura 5 - Scans reportados, por porta - Fonte: CERT.br disponível em <https://www.cert.br/stats/incidentes/2020-jan-jun/scan-portas.html> acesso em 13/05/2021.

3.11 Na Figura 6 são apresentadas as Notificações sobre equipamentos participando em ataques DoS.

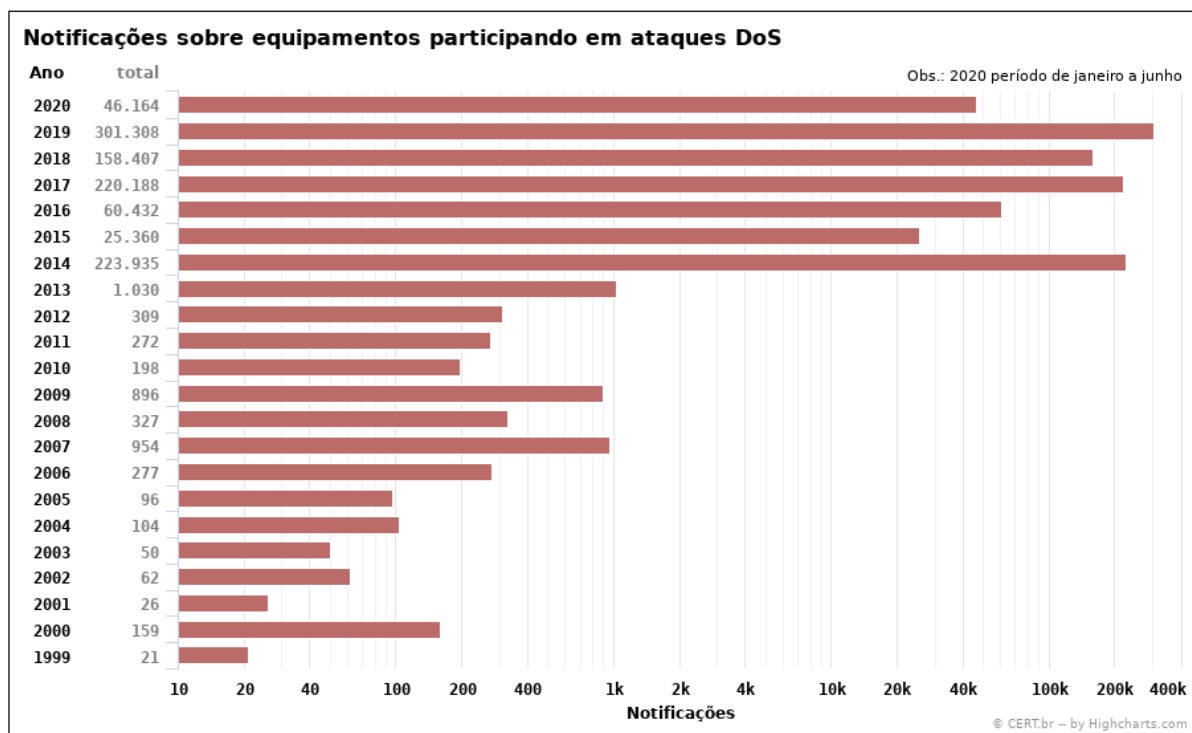


Figura 6 - Notificações sobre equipamentos participando em ataques DoS - Fonte: CERT.br disponível em <https://www.cert.br/stats/incidentes/2020-jan-jun/dos.html> acesso em 13/05/2021.

3.12 Na Figura 7 são apresentadas as Tentativas de Fraudes.

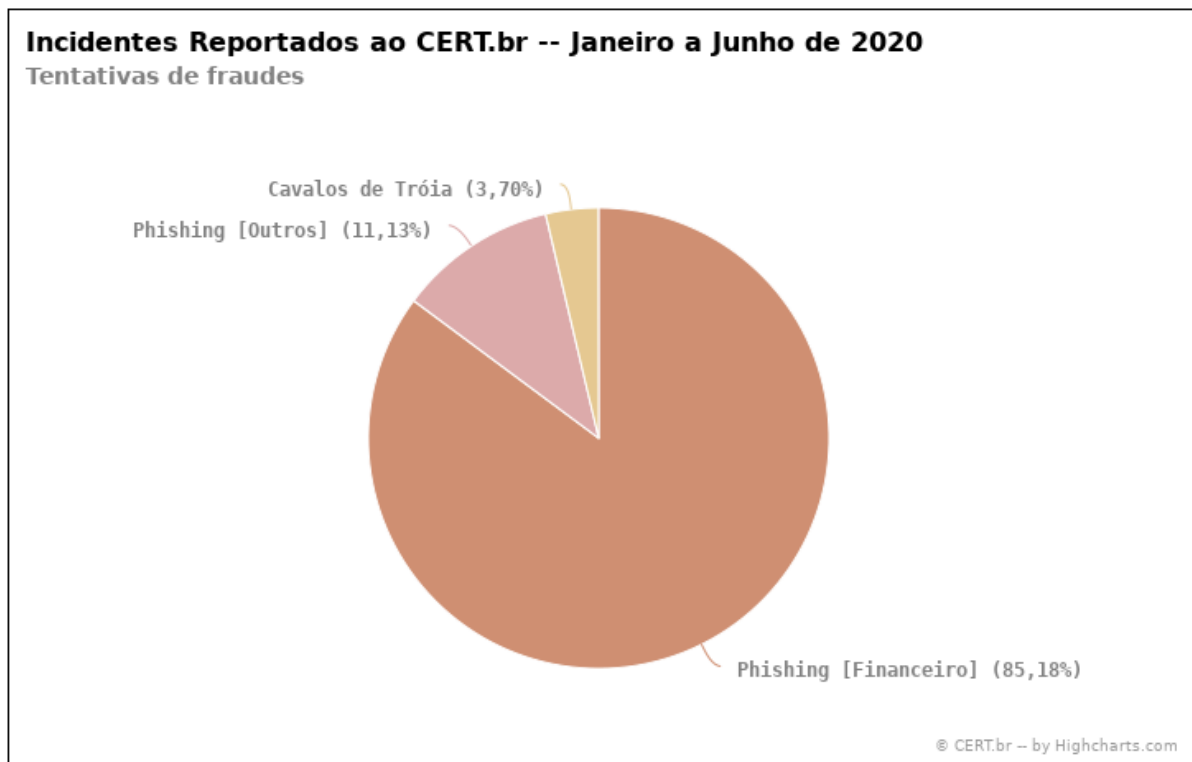


Figura 7 - Tentativas de fraudes - Fonte: CERT.br disponível em <https://www.cert.br/stats/incidentes/2020-jan-jun/fraude.html> acesso em 13/05/2021.

3.13 Na Figura 8 são apresentados os totais de incidentes reportados ao CERT.BR.

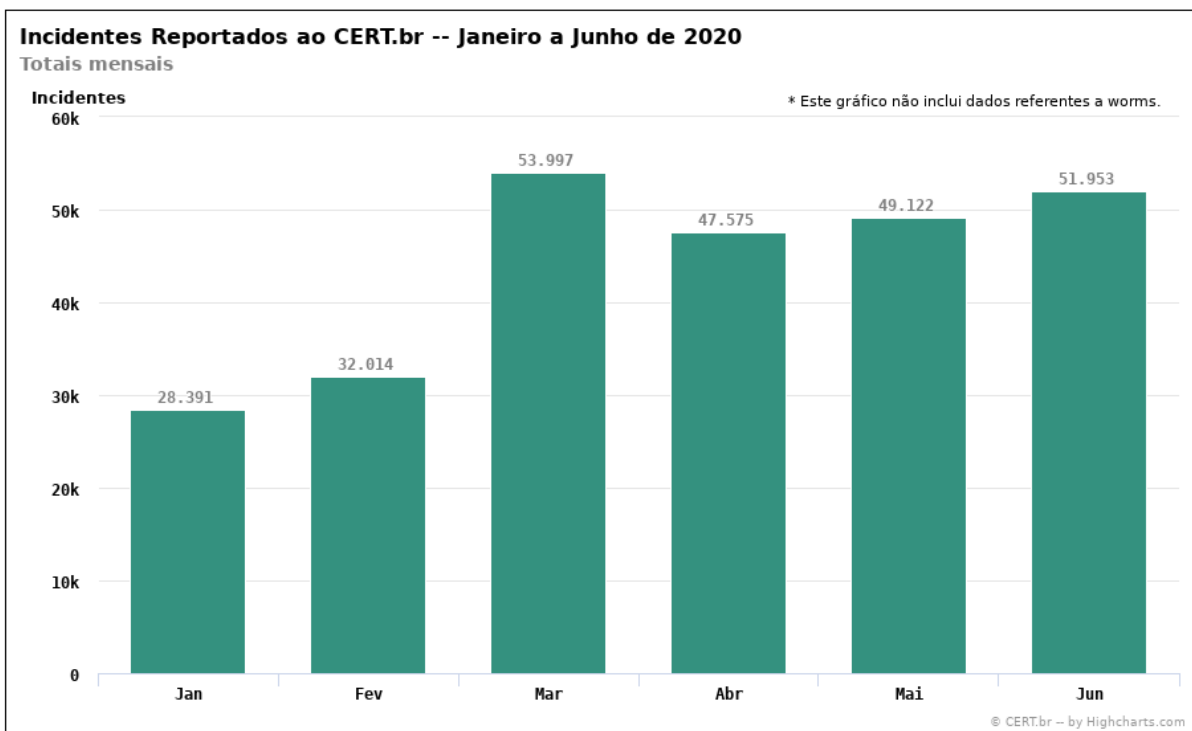


Figura 8 - Totais mensais - Fonte: CERT.br disponível em <https://www.cert.br/stats/incidentes/2020-jan-jun/total-mensal.html> acesso em 13/05/2021.

3.14 Na Figura 9 são apresentados os totais de incidentes reportados ao CERT.BR, considerando a origem do ataque.

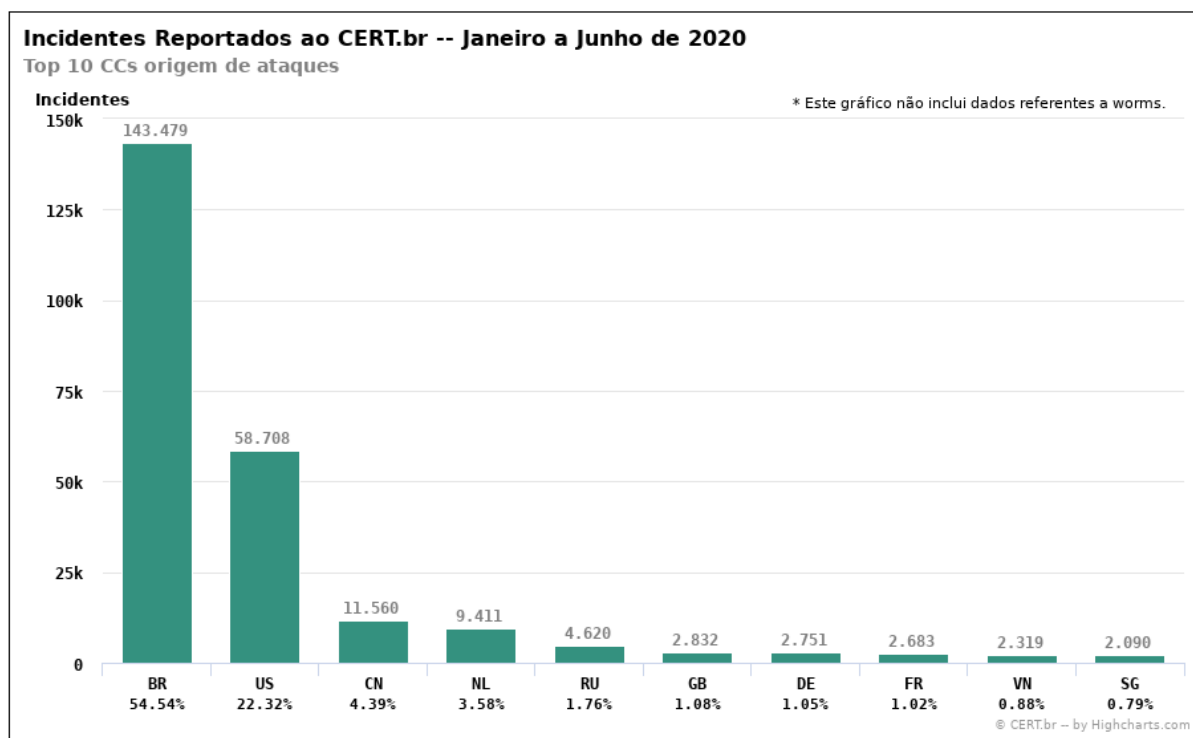


Figura 9 - Top 10 Country Codes origem de ataques - Fonte: CERT.br disponível em <https://www.cert.br/stats/incidentes/2020-jan-jun/top-cc.html> acesso em 13/05/2021.

3.15 Diante desse cenário complexo e misto, a contratação de uma equipe dedicada ao monitoramento, prevenção e reposta a incidentes de segurança se torna imprescindível.

3.16 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)

3.17 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.

3.18 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.

3.19 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.

3.20 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, conseqüentemente, eliminá-las.

3.21 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.

3.22 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.

3.23 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.

3.24 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."

3.25 A SANS - System Administration, Networking and Security é uma empresa especializada em segurança da informação e treinamento de cibersegurança. 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.

3.26 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.

3.27 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 prever, prevenir, detectar e responder efetivamente as ameaças, conforme podemos visualizar na figura 10 :

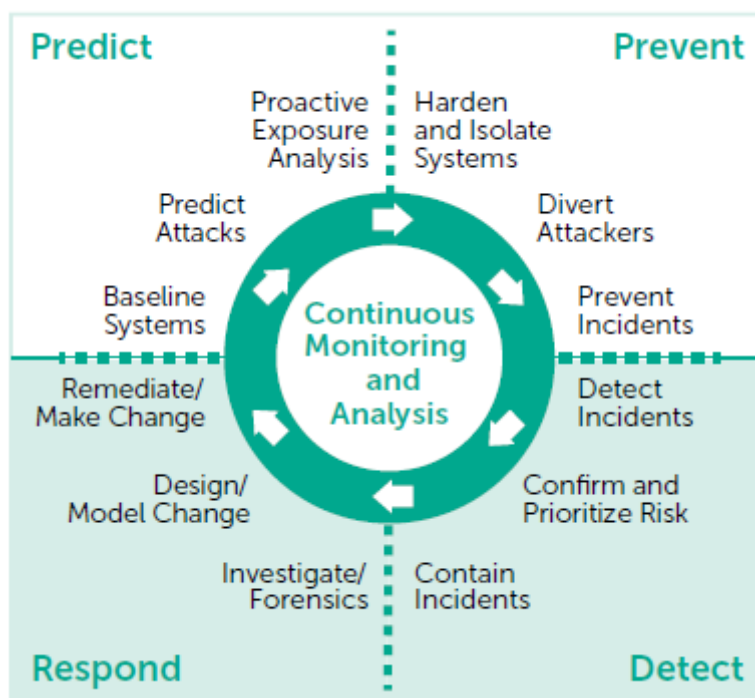


Figura 10 - Gartner, Designing an Adaptive Security Architecture for Protection From Advanced Attacks, February 2014. (retirado da brochura do Kaspersky for Security Operations Center)

3.27 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.

3.28 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.

4. Área requisitante

Área Requisitante	Responsável
Coordenação de Riscos e Segurança de TIC	Ivanildo de Oliveira da Silva JR

5. Necessidades de Negócio

5.1 Na tabela 3, são apresentadas as necessidades de negócio de acordo com o PDTIC 2021 (A0077 - Contratação de serviço de SOC).

Tabela - 3: Identificação das necessidades de negócio.

Identificação das necessidades de negócio	
1	Reduzir riscos associados a perda de dados, comprometimento dos sistemas, imagem institucional do ministério e do governo brasileiro
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

6. Necessidades Tecnológicas

6.1 Na tabela 4, são apresentadas as necessidades tecnológicas.

Tabela - 4: Identificação das necessidades tecnológicas

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

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

7.1 Na tabela 5, são apresentadas as demais necessidades da solução de TIC.

Tabela - 5: Identificação das demais necessidades da solução de TIC

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.

8. Estimativa da demanda - quantidade de bens e serviços

8.1 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:

- **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.

- **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.

- **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.

8.2 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>.

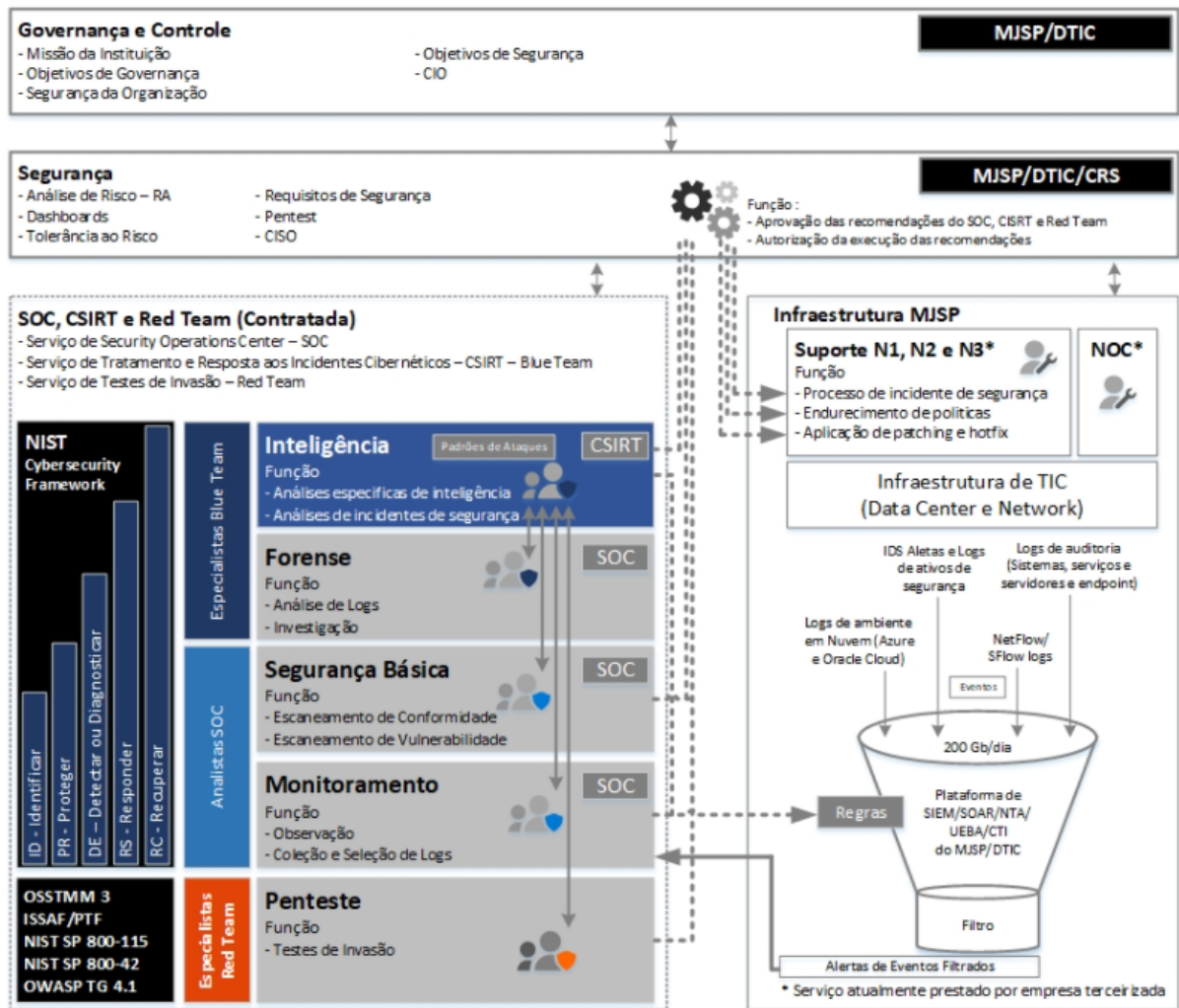


Figura 11 - Diagrama de relacionamento dos serviços e seus respectivos componentes com os demais serviços da DTIC.

8.3 Na Figura 11 é apresentado o diagrama de interação, para a presente contratação, 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.

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

- 8.3.1.1 Missão da Instituição;
- 8.3.1.2 Objetivos de Governança;
- 8.3.1.3 Segurança da Organização;
- 8.3.1.4 Objetivos de Segurança;
- 8.3.1.5 CIO (*Chief Information Officer*);

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

- 7.3.2.1 Análise de Risco;
- 7.3.2.2 Dashboards;
- 7.3.2.3 Tolerância ao Risco;
- 7.3.2.4 Requisitos de Segurança;
- 7.3.2.5 Pentest;

7.3.2.6 CISO (*Chief Information Security Officer*);

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

8.3.3 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:

8.3.3.1 Inteligência - através da equipe de especialistas Blue Team do CSIRT com as funções de Análise específicas de inteligência e de incidentes de segurança de acordo com os Padrões de Ataques;

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

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

8.3.3.4 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.

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

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

8.3.4.1 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.

8.3.4.2 NOC - através de equipe técnica (atualmente terceirizada) com a monitoramento da infraestrutura de TIC.

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

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

8.3.4.3.2 IDS Alertas e Logs de ativos de segurança;

8.3.4.3.3 NetFlow/ SFlow Logs;

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

8.4 Serviço de Security Operations Center - SOC

8.4.1 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:

8.4.1.1 Monitoramento contínuo e análise, predizendo, prevendo, detectando e respondendo efetivamente as ameaças de todos incidentes de segurança.

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

8.4.1.3 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.

8.4.1.4 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.

8.4.1.5 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.

8.4.1.6 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

8.4.1.7 Atuar em harmonia com o NOC do ministério.

8.4.1.8 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:

8.4.1.8.1 Camada de Automação:

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

8.4.1.8.1.2 Camada de Análise e Correlacionamento:

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

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

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

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

8.4.1.8.2 Camada de coleta:

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

8.4.1.9 Configurar, monitorar e operar a Plataforma de SIEM/SOAR/NTA/UEBA/CTI do Ministério.

8.4.1.10 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.

8.4.1.11 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.

8.4.1.12 Garantir a implementação do Modelo Adaptativo de Arquitetura de Segurança para Proteção de ataques avançados da Gartner exibido na figura 10.

8.4.2 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.

8.5 Serviço de Tratamento e Resposta aos Incidentes Cibernéticos - CSIRT - Blue Team

8.5.1 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.

8.5.2 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.

8.5.3 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.

8.5.4 Destacam-se algumas atividades que a equipe de especialistas Blue Team será responsável, não se restringindo somente a estas:

8.5.4.1 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.

8.5.4.2 Atuar como suporte de segundo nível em diante.

8.5.4.3 Defender o ministério nos incidentes de segurança.

8.5.4.4 Promover a melhoria da segurança da informação do Ministério.

8.5.4.5 Fazer cessar ou interromper os ataques à infraestrutura do Ministério.

8.5.4.6 Atuar em harmonia com o NOC do Ministério.

8.5.4.7 Atuar sob orientação do **CRS** quando de análises realizadas pelo **Red Team**.

8.5.4.8 Sugerir melhorias na segurança da informação do ministério a partir das melhores práticas internacionais.

8.5.4.9 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.

8.5.4.10 Implantar, configurar e suportar as tecnologias necessárias ao melhoramento da segurança da informação do Ministério.

8.5.4.11 Prover relatórios sob demanda.

8.5.4.12 Manter em funcionamento o painel de segurança da informação com as informações definidas de indicadores de performance e níveis de serviços acordados.

8.5.5 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.

8.5.6 Apoiar a CRS na avaliação, elaboração e revisão de relatórios segurança e privacidade.

8.6 Serviço de Teste de Invasão - Red Team

8.6.1 O **Red Team** funcionará sob demanda da CRS sem o conhecimento dos outros entes.

8.6.2 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.

8.6.3 Destacam-se algumas atividades que o **Red Team** será responsável, sob demanda, não se restringindo somente a estas:

8.6.3.1 Infligir ataques a infraestrutura de segurança interna e externa de rede e sistemas do ministério de modo não destrutivo.

8.6.3.2 Realizar tentativas de Data Exfiltration, Internal & External Reconnaissance, ShadowMap Scan, Vulnerability Assessment, Social Engineering, Exploitation, 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.

8.6.3.3 Gerar relatórios detalhado das tentativas.

8.6.3.4 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.

8.6.4 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.

8.7 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.

9. Levantamento de soluções

9.1 Foram identificadas 4 possíveis soluções, conforme relacionadas na tabela 6.

Tabela 6 - 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

10. Análise comparativa de soluções

10.1 Na tabela 7 é realizada uma análise comparativa de soluções, que foram mapeadas no MJSP.

Tabela 7 - 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
	Solução 1			X
	Solução 2			X

A Solução é composta por software livre ou software público? (quando se tratar de software)	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
Atuar de forma sincronizada com o Network Operations Center - NOC	Solução 1	X		
	Solução 2			X
	Solução 3			X
	Solução 4	X		
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	Solução 1		X	
	Solução 2		X	
	Solução 3			X

	Solução 4	X		
Prover equipe sob demanda da Coordenação de Riscos e Segurança da informação para atividades de SOC relacionadas a Red Team.	Solução 1		X	
	Solução 2		X	
	Solução 3			X
	Solução 4	X		

11. Registro de soluções consideradas inviáveis

11.1 Solução 1

11.1.1 **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.

11.1.2 **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.

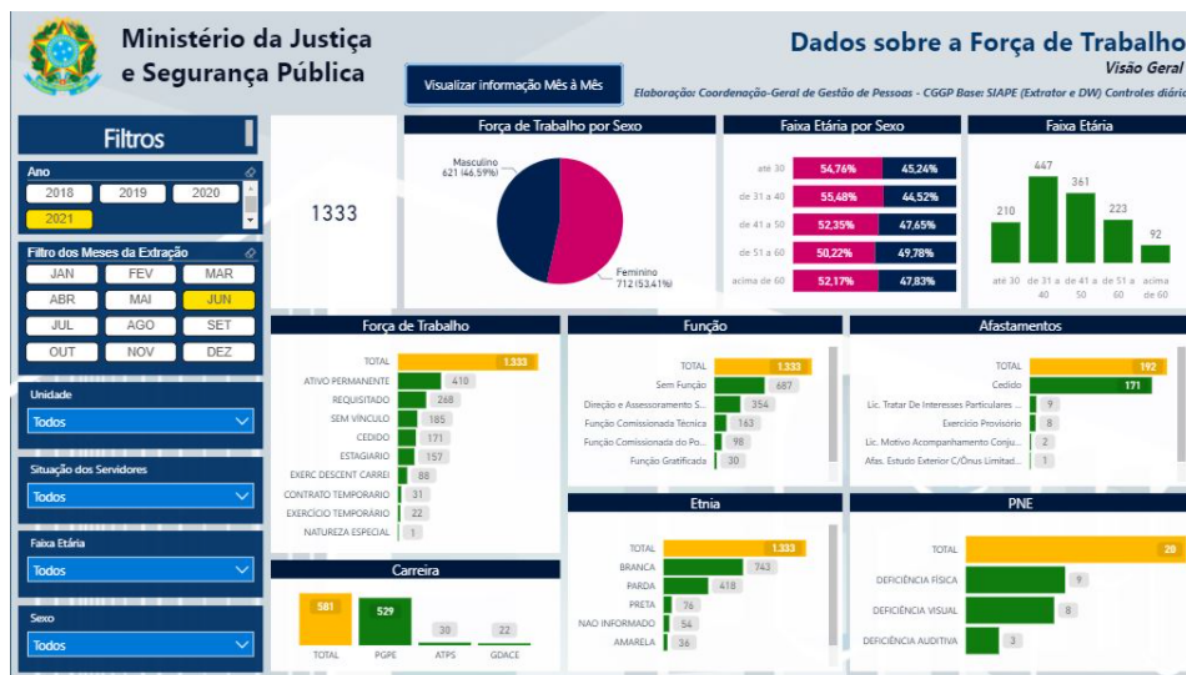


Figura 12 - Força de trabalho do MJSP, Fonte: Portal Gestão de Pessoas, disponível em <https://justicagovbr.sharepoint.com/sites/intra-CGGP/SitePages/For%C3%A7a-de-Trabalho.aspx>, acesso em 09/06/2021.

11.1.3 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.

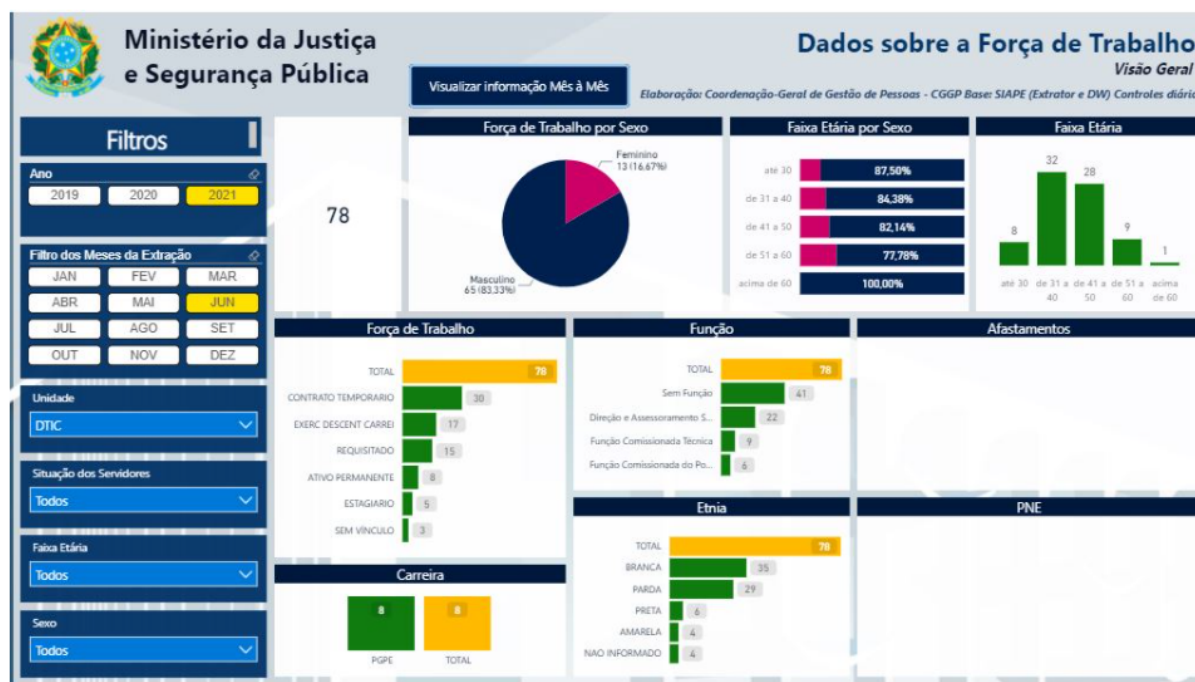


Figura 13 - Força de trabalho da DTIC, Fonte: Portal Gestão de Pessoas, disponível em <https://justicagovbr.sharepoint.com/sites/intra-CGGP/SitePages/For%C3%A7a-de-Trabalho.aspx>, acesso em 09/06/2021.

11.1.4 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."

11.1.5 Baseado nas recomendações da Gartner, considerando o quantitativo de pessoas do quadro de ativo permanente na Diretoria de Tecnologia e Comunicação, conforme item 11.1.3, e considerando o quantitativo de ativos instalados no MJSP, de acordo com Relatório sobre Informações da Infraestrutura do MJSP, a criação de um SOC com pessoal interno não seria viável.

11.1.6 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.

11.1.7 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.

11.1.8 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.

11.1.9 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 regime de escala de trabalho e/ou de plantão 24x7 para os seus servidores. Desta forma, essa solução é considerada inviável.

11.2 Solução 2

11.2.1 **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.

11.2.2 **Justificativa:** O Ministério da Justiça e Segurança Pública possui o Contrato nº 40/2019 (SEI 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.

11.2.3 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.

11.2.4 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.

11.2.5 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.

11.2.6 Outras funções do NOC incluem relatórios de desempenho e recomendações de melhoria, resposta à interrupção, planejamento de capacidade, alerta de acordo com procedimentos de escalção definidos e garantir a coordenação entre redes díspares.

11.2.7 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.

11.2.8 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.

11.2.9 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.

11.2.10 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 diferenças entre os conceitos de NOC e SOC.

Tabela 8 - 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.

11.2.11 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.

11.2.12 Isso posto, a possível solução de ampliar o Contrato nº 40/2019 (SEI 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.

11.2.13 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.

11.2.14 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.

11.3 Solução 3

11.3.1 **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.

11.3.2 **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.

11.3.3 Atualmente o Ministério da Justiça e Segurança Pública possui, como é possível observar no **relatório de informações sobre a infraestrutura**, 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.

11.3.4 Por isso, a simples aquisição de mais tecnologia apenas irá aumentar esse *pool*, não aumentando a segurança da informação do Ministério.

12. Análise comparativa de custos (TCO)

12.1 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-14), 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.

12.2 Das soluções apresentadas na tabela 6 - no item Levantamento de soluções, apenas a solução 4, 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 e Red Team será contratado. Os ativos, bens, sistemas, insumos necessários a execução dos 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.

12.3 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.

12.4 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.

12.5 O pregão do CJF considerou a contratação dos seguintes itens:

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 íntegro.

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.

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.

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.

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.

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.

12.6 O presente Estudo Técnico Preliminar visa a contratação, conforme exposto alhures, dos seguintes itens:

12.6.1 **Serviço de Security Operations Center - SOC:** conforme item 8.4 deste estudo.

12.6.2 **Serviço de Blue Team:** conforme item 8.5 deste estudo.

12.6.3 **Serviço de Red Team:** conforme item 8.6 deste estudo.

12.7 A tabela 9 apresenta a comparação dos serviços contratados pelo CJF com os serviços almejados pelo Ministério da Justiça e Segurança Pública chegamos as seguintes conclusões de equivalência, quando possível.

12.8 Cabe registrar que a ata do pregão do Conselho da Justiça Federal - CJF foi inserido no presente processo sob o número de documento (SEI 13624102). Foi inserido no presente processo o Edital do Conselho da Justiça Federal, sob o número de documento (SEI 13624084).

Tabela 9 - 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)

12.9 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 10.

Tabela 10 - 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	<table><tr><td colspan="2">Segunda-feira até Sexta-feira</td></tr><tr><td>Remoto</td><td>Presencial</td></tr><tr><td>9h até 20h = 11 horas</td><td>13h até 21h = 8h</td></tr></table>	Segunda-feira até Sexta-feira		Remoto	Presencial	9h até 20h = 11 horas	13h até 21h = 8h	Será dividido o valor dos itens pelas quantidades de horas contratadas e multiplicado pela necessidade do MJSP
Segunda-feira até Sexta-feira										
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.									

12.10 Considerando as tabelas 9 e 10 chegamos aos custos por hora e serviço para o CJF, apresentados na tabela 11:

Tabela 11 - 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_dtA

² Considerado um mês de 30 dias.

12.11 Diante das equivalências demonstradas pela Tabela 9, 10 e 11, podemos estimar o custo total de propriedade para a contratação dos serviços no MJSP. Conforme tabela 12. 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 12 - Custo estimado para o MJSP.

Custo Total de Propriedade – Memória de Cálculo				
Com o auxílio das tabelas 9, 10 e 11 chegamos a uma estimativa para o custo de uma possível contratação para o Ministério da Justiça e Segurança Pública, que é apresentado na tabela 12:				
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 Nível 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
			Sob demanda 217 Sistemas + 14 Appliance de Segurança + 110 Ativos de Rede + 68 Host Físico no Datacenter + 400 Sistemas Operacionais de Servidores	827 alvos x R\$ 1.150,84 = R\$ 951.744,68
		R\$ 1.150,84		

Serviço de Red Team	Serviço de testes de invasão (Red Team)	por alvo	+ 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)	/ 24 meses = 39.656,02 por mês
Total (sob demanda):				R\$ 951.744,68
Total 24 meses				R\$ 5.430.202,28

12.12 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.

12.13 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 12.

12.14 MAPA COMPARATIVO DOS CÁLCULOS TOTAIS DE PROPRIEDADE (TCO)

12.14.1 A tabela 13 apresenta a estimativa dos cálculos totais de propriedade para os próximos 5 anos, conforme memória de cálculo explicada no item 12.13 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 13 - 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 de Contratação
	Ano 1	Ano 2	Ano 3	Ano 4	Ano 5	
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

13. Descrição da solução de TIC a ser contratada

13.1 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.

13.2 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.

13.2.1 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:

13.2.1.1 **Serviço de Security Operations Center - SOC;**

13.2.1.2 **Serviço de Tratamento e Resposta aos Incidentes Cibernéticos - CSIRT - Blue Team;**

13.2.1.3 **Serviço de Testes de Invasão - Red Team;**

13.2.1.4 **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 Infrastructure Library – ITIL* e com as atividades dos processos do volume de **Transição de Serviços e Operação de Serviços;**

13.2.1.4.1 Gerenciamento de Configurações e de Ativo de Serviços;

13.2.1.4.2 Gerenciamento de Mudanças;

13.2.1.4.3 Gerenciamento de Liberações e Implantação;

13.2.1.4.4 Gerenciamento do Conhecimento;

13.2.1.4.5 Gerenciamento de Evento;

13.2.1.4.6 Gerenciamento de Incidente;

13.2.1.4.7 Gerenciamento de Problema;

13.2.1.4.8 Gerenciamento de Requisição;

13.2.1.4.9 Gerenciamento de Acesso;

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

13.2.1.4.10.1 Central de Serviços;

13.2.1.4.10.2 Gerenciamento de Operações de TI (Controle de Operações de Segurança da Informação);

13.2.1.4.10.3 Gerenciamento Técnico;

13.2.1.4.10.4 Gerenciamento de Aplicação;

13.2.1.4.11 Ambos os serviços desempenharão os seguintes objetivos e propósitos:

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

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

13.2.1.4.11.2 Prover conhecimento de qualidade para a organização.

13.2.1.4.11.3 Prover mecanismos de implementação eficientes e padronizados.

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

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

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

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

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

13.2.1.4.11.9 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 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.

13.2.1.4.11.10 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.

13.2.1.4.11.12 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.

13.2.1.4.11.13 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;

13.2.1.4.11.14 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.

13.2.1.4.11.15 Sugestão de ajustes de configuração dos dispositivos visando reduzir a probabilidade de ataques, sendo a execução desses ajustes de responsabilidade do NOC do ministério.

13.2.1.4.11.16 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.

13.2.1.4.11.17 Execução de serviços técnicos especializados, sob demanda e de maneira eventual.

13.2.1.4.11.18 Prestação remota dos serviços, sendo a presença física somente quando necessário ou mediante justificativa.

13.2.1.4.11.19 Utilização das ferramentas, soluções e equipamentos de segurança instalados no ministério.

13.2.1.4.11.20 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).

13.2.1.4.11.21 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.

13.2.1.4.11.22 Disponibilização de pessoal técnico qualificado mediante certificação oficial e experiência profissional em todos os itens da possível contratação.

13.2.1.4.11.23 Análise fim a fim dos incidentes e ataques.

13.2.1.4.11.24 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.

13.2.1.4.11.25 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.

13.2.1.4.11.26 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.

13.2.1.4.11.27 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.

13.2.1.4.11.28 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.

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

13.2.1.4.12 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:

13.2.1.4.12.1 NIST Cybersecurity Framework, Version 1.1 ou mais recente;

13.2.1.4.12.2 NIST Privacy Framework, Version 1.0 ou mais recente;

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

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

13.2.1.4.12.5 SANS Incident Handler's Handbook;

13.2.1.4.12.6 CIS Control, Version 7.1 ou mais recente;

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

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

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

13.2.1.4.13 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.

13.2.1.4.14 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.

13.2.1.5 O Serviço de Teste de Invasão - Red Team envolve os seguintes serviços, conforme *Information Technology Infrastructure Library* – ITIL e com das atividades dos processos do volume de **Transição de Serviços e Operação de Serviços**;

13.2.1.5.1 Gerenciamento do Conhecimento;

13.2.1.5.2 Gerenciamento de Incidente;

13.2.1.5.3 Gerenciamento de Problema;

13.2.1.5.4 Gerenciamento de Requisição;

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

13.2.1.5.5.1 Central de Serviços;

13.2.1.5.6 Serviços de Red Team desempenhará os seguintes objetivos e propósitos:

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

13.2.1.5.6.2 Prover conhecimento de qualidade para a organização.

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

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

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

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

13.2.1.5.6.7 Realização de testes de penetração.

13.2.1.5.6.8 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.

13.2.1.5.7 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 deverão ser entregues e permanecerão sob custódia exclusiva do Ministério;

13.2.1.5.8 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:

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

13.2.1.5.8.2 ISSAF/PTF (Information Systems Security Assessment Framework);

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

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

13.2.1.5.8.5 OWASP TESTING GUIDE 4.1 The Open Web Application Security Project.

13.2.1.5.9 Neste documento os termos “pentest”, teste de penetração, teste de intrusão e testes de invasão, são considerados sinônimos;

13.2.1.5.10 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;

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

13.2.1.5.12 Todas as fases dos “Testes de Invasão” serão acompanhadas e supervisionadas a critério do Ministério;

13.2.1.5.13 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;

13.2.1.5.14 O teste de invasão deverá obedecer às seguintes fases:

13.2.1.5.14.1 Planejamento;

13.2.1.5.14.2 Descoberta;

13.2.1.5.14.3 Ataque;

13.2.1.5.14.4 Relatório Teste de Invasão;

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

13.2.1.5.14.6 Reavaliação, novo teste pós remediação;

13.2.1.5.14.7 Relatório Final do Teste de Invasão.

13.2.1.5.15 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.

13.3 Matriz de Responsabilidade R.A.C.I

13.3.1 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 13 - 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 14 - 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								
Situação	Descrição	Processos				Processos				Funções				
		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 NDC	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	MISP/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.

13.4 Indicadores de performance do Serviço de Security Operation Center - SOC

13.4.1 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.

13.4.2 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.

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

13.4.4 Os indicadores de performance são flexíveis em quantidade e qualidade e estão descritos na tabela a seguir:

Tabela 15 - 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
	Ameaças	Nível de segurança	Classificação de cores
		Atribuição de ameaças a atores (usando inteligência de ameaças)	a definir
		Tempo para remediação da vulnerabilidade	tempo

Técnico	Vulnerabilidade	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 análise	tempo
		Nível de disponibilidade	percentual
	Cobertura	Quantidade de ativos monitorados	número
		Quantidade de ativos monitorados vs. Quantidade total de ativos	número e percentual

13.5 Dimensionamento da força de trabalho pela CONTRATADA.

13.5.1 Para o dimensionamento da força de trabalho da CONTRATADA, o fluxo de dados do Ministério a ser considerado de forma escalável, sob demanda, 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	-	-	-

13.6 Itens que compõe a pretensa contratação

13.6.1 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

14. Estimativa de custo total da contratação

Valor (R\$): 5.430.202,28

14.1 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

14.2 Os 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.

14.3 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.

15. Justificativa técnica da escolha da solução

15.1 Plataforma de SIEM/SOAR/NTA/UEBA/CTI do Ministério

15.1.1 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 19 - 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 Security Management Platform	LogRhythm's SmartResponse™	Splunk Phantom
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 Híbrido 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 Cibernéticas 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/UseCIMtonormalizeddataatsearchtime>

- 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

15.1.2 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.

15.1.3 A contratação da solução como serviço, conforme descrito em detalhe no item 13 - Descrição da solução de TIC a ser contratada, 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 e Red Team serão contratados.

15.1.4 Conforme está demonstrado neste estudo técnico preliminar, a contratação como serviço, sem aquisição da ferramenta de SIEM, utilizando a que está disponível no atual contrato junto a Microsoft, Azure Sentinel, se mostra mais vantajosa devido a economia no envio dos logs para análise da ferramenta.

16. Justificativa econômica da escolha da solução

16.1 Após a avaliação técnica, essa equipe de planejamento da contratação realizou uma comparação de preços entre as soluções comercializada no país 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 20 - 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/VIAMI
	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\$ 13.261,75 para 1Gbps (4)	R\$ 13.261,75	R\$ 4.681,28	R\$ 4.681,28	R\$ 8.777,42	R\$ 8.777,42
Endpoints	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 mensal 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.

16.2 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.

16.3 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 benefício para a administração bem como, a melhor estratégia da presente contratação.

17. Benefícios a serem alcançados com a contratação

17.1 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:

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

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

17.1.3 Redução dos riscos associados aos ativos críticos.

17.1.4 Aumento da maturidade de segurança da informação.

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

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

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

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

- 17.1.9 Implantar e fortalecer as equipes de tratamento de incidentes cibernéticos nas redes de computadores.
- 17.1.10 Implantar ações que promovam o envolvimento da alta administração do órgão em relação às diretrizes e ações de Segurança da Informação e Comunicação.
- 17.1.11 Definir e implantar mecanismos mais efetivos de responsabilização de colaboradores por eventos relacionados à Segurança da Informação e Comunicação.
- 17.1.12 Contribuir para o aumento da capacidade de resiliência dos ativos de informação e das infraestruturas críticas.
- 17.1.13 Instituir práticas de auditoria de Segurança da Informação e Comunicações.
- 17.1.14 Atualizar a Política de Segurança da Informação e Comunicações.
- 17.1.15 Manter uma equipe ininterrupta de resposta rápida e efetiva a ataques e incidentes cibernético .
- 17.1.16 Implantar o estado da arte em termos de segurança da informação.
- 17.1.17 Multiplicar o efetivo na área de segurança da informação.
- 17.1.18 Elevar o conhecimento técnico e a capacidade de gestão do corpo técnico próprio do Ministério da Justiça.
- 17.1.19 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.

18. Providências a serem Adotadas

18.1 AVALIAÇÃO DAS NECESSIDADES DE ADEQUAÇÃO DO AMBIENTE DO ÓRGÃO

18.1.1 **Não** é necessário adequar o ambiente da infraestrutura física das instalações do Ministério para viabilizar a entrega ou a execução contratual.

18.1.2 **Não** é necessário adequar o ambiente da infraestrutura elétrica para viabilizar a entrega ou a execução contratual.

18.2 RECURSOS MATERIAIS

18.2.1 Será necessário disponibilizar mobiliário e computadores nas dependências do MJSP para prestação de serviços, quando a CONTRATA informar necessidade.

19. Declaração de Viabilidade

Esta equipe de planejamento declara **viável** esta contratação.

19.1. Justificativa da Viabilidade

19.1 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.

19.2 Foram avaliadas as soluções disponíveis no mercado quanto à viabilidade técnica e econômica para o atendimento das necessidades deste órgão.

19.3 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.

20. Responsáveis

CINTIA MYE YONEKAWA YAMAGUTI
INTEGRANTE TÉCNICO

IVANILDO DE OLIVEIRA DA SILVA JR
INTEGRANTE REQUISITANTE

JOÉDES CARDOSO DA SILVA
INTEGRANTE REQUISITANTE SUBSTITUTO

MADSON LUIZ MAGNO DA SILVA
INTEGRANTE TÉCNICO SUBSTITUTO

Lista de Anexos

Atenção: Apenas arquivos nos formatos ".pdf", ".txt", ".jpg", ".jpeg", ".gif" e ".png" enumerados abaixo são anexados diretamente a este documento.

- Anexo I - SEI MJSP 14868691 - CentralIT_Quantidade De Estacoes De Trabalho.pdf (652.92 KB)
- Anexo II - SEI MJSP 10267604 - Contrato 40_2018.pdf (686.93 KB)
- Anexo III - SEI MJSP 13624084 - Edital_CJF.pdf (1.09 MB)
- Anexo IV - SEI MJSP 13624102 - Ata_do_pregao_CFJ.pdf (833.35 KB)
- Anexo V - SEI MJSP 14781049 - Despacho 333.pdf (455.95 KB)
- Anexo VI - SEI MJSP 14612910 - Despacho 80.pdf (1.36 MB)
- Anexo VII - SEI MJSP 14424141 - PDTIC_2021_2023.pdf (1.82 MB)
- Anexo VIII - SEI MJSP 13636809 - Portaria de Pessoal SAA 1.pdf (808.41 KB)
- Anexo IX - SEI MJSP 14627967 - Portaria SAA 57.pdf (753.02 KB)

Anexo I - SEI MJSP 14868691 - CentralIT_Quantidade De Estacoes De Trabalho.pdf

De: sati@mj.gov.br
Enviado em: quarta-feira, 9 de junho de 2021 17:05
Para: Cintia Mye Yonekawa Yamaguti
Assunto: Solicitação atendida SATI - 34691



Central de Serviços SATI

Prezado(a),

A Central de Serviços do Ministério da Justiça e Segurança Pública (MJSP) concluiu o atendimento da sua solicitação.

Nº do chamado: 34691

Serviço/Atividade: Levantar informações de objetos

Detalhamento do chamado: Solicito informar a QUANTIDADE TOTAL DE ESTAÇÕES DE TRABALHO EM TODO O AMBIENTE DO MJ. Esta informação será utilizada em uma das contratações de Serviços de Segurança do MJ. Portanto há necessidade de urgência e precisão na informação. Muito Obrigada.

Localidade: MJSP / PALÁCIO DA JUSTIÇA / EDIFÍCIO SEDE / ESPLANADA DOS MINISTÉRIOS

Nº andar: 3º Andar

Ramal: 3807

Sala: 314

Solução aplicada:

Atualmente a quantidade de maquinas ativas no parque MJ sao: 3125. Contando com desktops e notebooks. Esse levantamento foi tirado do AD.

Desejamos saber a sua opinião sobre os serviços prestados. Por gentileza, colabore conosco avaliando o nosso atendimento.

[Clique aqui para fazer a avaliação do Atendimento](#)

Acesse o [Portal de Serviços SATI](#) para solicitar atendimento e realizar o acompanhamento da sua solicitação.

Esta é uma mensagem automática. Por favor, não responda.

Atenciosamente,
SATI (Serviço de Atendimento a Tecnologia da Informação)
Tel: 2025-2200

Anexo II - SEI MJSP 10267604 - Contrato 40_2018.pdf

08006.000087/2019-95



10267604



08006.000087/2019-95

Boletim de Serviço em 21/11/2019
D.O.U. de 21/11/2019, seção 3, página 98



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

CONTRATO Nº 40/2019

CONTRATO QUE ENTRE SI CELEBRAM 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 CENTRAL IT TECNOLOGIA DA INFORMAÇÃO LTDA.

PROCESSO Nº 08006.000087/2019-95

A União, representada pelo **MINISTÉRIO DA JUSTIÇA E SEGURANÇA PÚBLICA**, com sede à Esplanada dos Ministérios, CEP 70064-900, Brasília/DF, inscrito no CNPJ 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 nº 29 de 2 de janeiro de 2019, publicada no D.O.U de 2 de janeiro de 2019 - Edição Extra, com delegação de competência fixada pela Portaria SE 1.008, de 25 de abril de 2019, publicada no D.O.U de 26 de abril de 2019 e a Coordenadora-Geral de Licitações e Contratos, **Sra. DÉBORA DE SOUZA JANUÁRIO**, brasileira, solteira, portadora do RG nº 3.558.79980 - SSP/SP e do CPF nº 712.315.791-53, nomeada por meio da Portaria nº 1.087, de 06 de novembro de 2015, publicada no D.O.U de 09 de novembro de 2015 e com delegação de competência fixada pela Portaria nº 23, de 26 de abril de 2019, publicada no D.O.U. de 30 de abril de 2019, doravante denominado **CONTRATANTE**, e a Empresa **CENTRAL IT TECNOLOGIA DA INFORMAÇÃO LTDA**, inscrita no CNPJ nº 07.171.299/0001-96, estabelecida SHN - Quadra 02 - Bloco F - Ed. Executive Office Tower - 17º Andar – Asa Norte, CEP: 70702-906 - Brasília/DF, neste ato representada pelo(a) **Sr. CARLOS ALBERTO FREITAS**, brasileiro, casado, portador do RG nº MG-2.158.316 - SSP/MG e do CPF 980.684.821-72, doravante denominada **CONTRATADA**, tendo em vista o que consta no Processo nº 08006.000087/2019-95 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 Instrução Normativa SITI/MPOG nº 4 de 11 de setembro de 2014 e da Instrução Normativa

Anexo III - SEI MJSP 13624084 - Edital_CJF.pdf



PODER JUDICIÁRIO
CONSELHO DA JUSTIÇA FEDERAL

UASG 090026

PROCESSO CJF – SEI 0001989-89.2019.4.90.8000

PREGÃO ELETRÔNICO N. 1/2020

O **CONSELHO DA JUSTIÇA FEDERAL**, por intermédio do pregoeiro, designado pela Portaria SEI n. 607, de 10 de novembro de 2019, nos termos das disposições contidas na Lei n. 10.520, de 17 de julho de 2002, regulamentada pelo Decreto n. 10.024 de 20 de setembro de 2019, na Lei Complementar n. 123, de 14 de dezembro de 2006, regulamentada pelo Decreto n. 8.538, de 6 de outubro de 2015, e legislação correlata, aplicando-se, subsidiariamente, no que couberem, a Lei n. 8.666, de 21 de junho de 1993 e alterações, e ainda a Lei n. 12.846, de 1º de agosto de 2013, fará realizar licitação na modalidade de **PREGÃO ELETRÔNICO**, do tipo **MENOR PREÇO GLOBAL**, para contratação de Serviços Gerenciados de Segurança da Informação para atender ao Conselho da Justiça Federal – CJF, conforme condições e especificações constantes das cláusulas abaixo e dos Módulos I a II, os quais fazem parte integrante do presente edital:

I – DA SESSÃO PÚBLICA DO PREGÃO ELETRÔNICO

II – DO OBJETO

III – DAS IMPUGNAÇÕES E PEDIDOS DE ESCLARECIMENTOS DO ATO CONVOCATÓRIO

IV – DO CREDENCIAMENTO

V – DAS CONDIÇÕES DE PARTICIPAÇÃO E DA CONCESSÃO DOS BENEFÍCIOS À ME/EPP

VI – DA PROPOSTA ELETRÔNICA DE PREÇO E DOS DOCUMENTOS DE HABILITAÇÃO

VII – DA ABERTURA DA SESSÃO E DA CLASSIFICAÇÃO DAS PROPOSTAS

VIII – DA FORMULAÇÃO DE LANCES E DO DESEMPATE

IX – DA NEGOCIAÇÃO E DO JULGAMENTO DAS PROPOSTAS

X – DA HABILITAÇÃO

XI – DA PROPOSTA DEFINITIVA DE PREÇO

XII – DOS RECURSOS

XIII – DA DOTAÇÃO ORÇAMENTÁRIA

XIV – DO PAGAMENTO

XV – DAS PENALIDADES

XVI – DO SISTEMA DE REGISTRO DE PREÇOS

XVII – DA ATA DE REGISTRO DE PREÇOS

XVIII – DO CONTRATO

XIX – DA REAPACTUAÇÃO E DO REAJUSTE

XX – DA GARANTIA

XXI – DA VISTORIA

XXII – DA ADJUDICAÇÃO E HOMOLOGAÇÃO

XXIII – DAS DISPOSIÇÕES FINAIS

MÓDULO I – TERMO DE REFERÊNCIA E SEUS ANEXOS

MÓDULO II – MINUTA DA ATA DE REGISTRO DE PREÇOS

MÓDULO – III – MINUTA DE CONTRATO

I – DA SESSÃO PÚBLICA DO PREGÃO ELETRÔNICO

1 – A abertura da presente licitação dar-se-á em sessão pública, dirigida pelo pregoeiro, a ser realizada conforme indicado abaixo, de acordo com a legislação mencionada no preâmbulo deste edital.

2 – No dia 5.2.2020, às 10:00 horas, será feita a abertura da sessão pública, exclusivamente por meio do sítio <http://www.comprasgovernamentais.gov.br/>



PODER JUDICIÁRIO
CONSELHO DA JUSTIÇA FEDERAL

3 – Todas as referências de tempo neste edital, no aviso de licitação e durante a sessão pública observarão obrigatoriamente o horário de Brasília – DF e, dessa forma, serão registradas no sistema eletrônico e na documentação relativa ao certame.

II – DO OBJETO

1 – A presente licitação tem por objeto a contratação de Serviços Gerenciados de Segurança da Informação para o Conselho da Justiça Federal – CJF, com as especificações técnicas contidas nos Módulos I – Termo de Referência e Anexos (I a V), II – Minuta de Ata de Registro de Preço e III- Minuta de Contrato, compreendendo os seguintes serviços:

- a) **Serviços de Operação e Atendimento à Requisições;**
- b) **Serviço de Gestão de Incidentes de Segurança (CSIRT - Blue Team);**
- c) **Serviço de Gestão de Vulnerabilidades;**
- d) **Serviço de Monitoramento e Visibilidade de Ataques Cibernéticos;**
- e) **Serviço de Orquestração, Automação e Resposta de Segurança (SOAR);**
- f) **Serviço de Testes de Invasão (Red Team).**

2 – **Em caso de discordância existente entre as especificações do objeto descritas no COMPRASNET e as especificações constantes deste edital, prevalecerão as últimas.**

III – DAS IMPUGNAÇÕES E PEDIDOS DE ESCLARECIMENTOS DO ATO CONVOCATÓRIO

1 – Qualquer pessoa poderá impugnar o presente edital, encaminhando o pedido até 3 (três) dias úteis antes da data fixada para abertura da sessão pública, por meio do correio eletrônico sei-selita@cjf.jus.br, cabendo ao pregoeiro, com auxílio do setor responsável pela elaboração do termo de referência (se for o caso), decidir a matéria no prazo de 02 (dois) dias, contados da data de recebimento da impugnação, nos termos dos §1º, do art. 24, do Decreto n. 10.024/2019.

2 – As impugnações deverão ser dirigidas ao pregoeiro por quem tenha poderes para representar a licitante ou por qualquer cidadão que pretenda impugnar o ato convocatório nesta qualidade.

3 – Acolhida a impugnação contra o ato convocatório que implique em sua modificação, será divulgada nova data para realização do certame, da mesma forma que se deu a divulgação do texto original, reabrindo-se o prazo inicialmente estabelecido, exceto quando, inquestionavelmente, a alteração não afetar a formulação das propostas.

4 – Os pedidos de esclarecimentos referentes ao processo licitatório deverão ser enviados ao pregoeiro, até 3 (três) dias úteis anteriores à data fixada para abertura da sessão pública, exclusivamente por meio do correio eletrônico sei-selita@cjf.jus.br.

4.1 - 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 módulos anexos, nos termos do §1º, do art. 23, do Decreto n. 10.024/2019.

4.2 - As respostas aos pedidos de esclarecimentos serão divulgadas pelo sistema e vincularão os participantes e a administração, nos termos do §2º, do art. 23, do Decreto n. 10.024/2019.



PODER JUDICIÁRIO
CONSELHO DA JUSTIÇA FEDERAL

5 – As respostas às impugnações e aos esclarecimentos solicitados serão disponibilizadas no endereço eletrônico <http://www.comprasgovernamentais.gov.br>, por meio do link *Acesso livre>Pregões>Agendados*, para conhecimento da sociedade em geral e dos fornecedores, cabendo aos interessados em participar do certame acessá-lo para obtenção das informações prestadas.

IV – DO CREDENCIAMENTO

1 – O credenciamento dar-se-á pela atribuição de chave de identificação e de senha, pessoal e intransferível, para acesso ao sistema eletrônico, no sítio <http://www.comprasgovernamentais.gov.br> (art. 9º, §1º, do Decreto n. 10.024/2019).

1.1 – O credenciamento da licitante ou de seu representante perante o provedor do sistema implicará responsabilidade legal pelos atos praticados e presunção de capacidade técnica para realização das transações inerentes ao pregão eletrônico;

2 – A licitante responsabilizar-se-á formalmente pelas transações efetuadas em seu nome, assumindo como firmes e verdadeiras suas propostas, seus documentos e seus lances, incluindo qualquer transação efetuada diretamente ou por seu representante, não cabendo ao provedor do sistema ou ao órgão promotor da licitação responsabilidade por eventuais danos decorrentes de uso indevido da senha, ainda que por terceiros (art. 19, inciso III, do Decreto n. 10.024/2019).

2.1 – A perda da senha ou a quebra de sigilo deverão ser comunicadas imediatamente ao provedor do sistema, para imediato bloqueio de acesso;

V – DAS CONDIÇÕES DE PARTICIPAÇÃO E DA CONCESSÃO DOS BENEFÍCIOS À ME/EPP

1 – Poderão participar deste PREGÃO ELETRÔNICO as empresas que:

1.1 – Atenderem a todas as exigências, inclusive quanto à documentação, constantes deste edital;

1.2 – Estejam previamente credenciadas perante o sistema eletrônico provido pelo Ministério da Economia, por meio do sítio <http://www.comprasgovernamentais.gov.br>.

1.3 – Estejam cadastradas no Sistema de Cadastramento Unificado de Fornecedores – SICAF, nos termos do art. 10 do Decreto n. 10.024/2019.

1.4 – Manifestarem, em campo próprio do sistema eletrônico, que cumprem plenamente os requisitos de habilitação e a conformidade de sua proposta com as exigências do edital.

1.5 – Quando da participação das microempresas e empresas de pequeno porte – ME/EPP serão adotados os critérios estabelecidos nos artigos 42 a 45 da Lei Complementar n. 123/2006 e no Decreto n. 8.538/2015.

1.5.1 – Para o enquadramento das ME/EPP, o fornecedor, no ato de envio de sua proposta e da documentação de habilitação, em campo próprio do sistema, deverá declarar que atende os requisitos do art. 3º da Lei Complementar n. 123/2006 para fazer jus aos benefícios da referida Lei;



PODER JUDICIÁRIO
CONSELHO DA JUSTIÇA FEDERAL

1.5.2 – Não poderão se beneficiar do regime diferenciado e favorecido as empresas que se enquadrem em qualquer das exclusões relacionadas no §4º, do art. 3º da Lei Complementar n. 123/2006.

2 – Não poderão participar deste certame:

2.1 - Não poderá participar do certame a empresa que preste os serviços técnicos especializados de **SUSTENTAÇÃO DA INFRAESTRUTURA DE TI** ou serviços técnicos especializados de desenvolvimento e sustentação de software, em regime de **FÁBRICA DE SOFTWARE** para o CJF, esta restrição objetiva atender ao princípio da segregação de funções previsto na Norma NBR ISO/IEC 27002:2005 e manutenção da qualidade dos serviços de Segurança da Informação, conforme exposto na justificativa do Módulo I - Termo de Referência.

2.2 – Empresas que estiverem sob a aplicação da penalidade referente ao art. 87, incisos III e IV da Lei n. 8.666/93, do art. 7º da Lei n. 10.520/2002 ou do art. 49 do Decreto n. 10.024/2019;

2.2.1 – A suspensão prevista no art. 87, inciso III, aplica-se apenas no âmbito do CJF;

2.2.2 – Para fins de participação nesta licitação, a penalidade imposta com base no art. 7º da Lei n. 10.520/2002 abrange os órgãos e entidades da Administração Pública direta e indireta da União, nos termos do inciso I, §3º, do art. 24, da IN 3/2018/MPOG.

2.3 – Servidor/membro/juiz de qualquer órgão ou entidade vinculada ao órgão promotor da licitação, bem assim a empresa da qual tal servidor/membro/juiz seja sócio, dirigente ou responsável técnico;

2.4 – Empresas que estejam reunidas em consórcio, qualquer que seja sua forma de constituição, sejam controladoras, coligadas ou subsidiárias entre si;

2.5 - Cooperativa de trabalho, associações e OSCIP's (Organização da Sociedade Civil de Interesse Público – acórdão TCU n. 746/2014 – Plenário – TC 021.605/2012-2);

2.6 – Empresa em processo de falência, sob concurso de credores, em dissolução ou em liquidação;

2.6.1. A empresa em recuperação judicial poderá participar do certame desde que apresente plano de recuperação aprovado e homologado judicialmente, com a recuperação já deferida.

2.6.2. A empresa em recuperação judicial que comprovar o disposto no Item 3.6.1 deverá demonstrar os demais requisitos de habilitação.

2.6.3. A regra é aplicável à empresa em recuperação extrajudicial, desde que preenchidos os requisitos dos itens 3.6.1 e 3.6.2.

2.7 – Empresas estrangeiras que não funcionam no país;

2.8 – Empresas que possuem em seu quadro societário pessoa detentora de mandato de deputado e/ou senador, desde sua diplomação, nos termos da alínea “a”, do inciso I, do artigo 54 da Constituição Federal;



PODER JUDICIÁRIO
CONSELHO DA JUSTIÇA FEDERAL

2.9 – Empresas que possuam registro de impedimento de contratação no Cadastro Nacional de Condenações Cíveis por ato de improbidade administrativa e inelegibilidade, disponível no portal do Conselho Nacional de Justiça;

2.10 – Empresas que possuam registros impeditivos de contratação, no Cadastro Nacional de Empresas Inidôneas e Suspensas/CGU, disponível no Portal da Transparência;

2.11 – Empresas cujo objeto social, expresso no estatuto ou contrato social, seja incompatível com o objeto da presente licitação.

VI – DA PROPOSTA ELETRÔNICA DE PREÇO E DOS DOCUMENTOS DE HABILITAÇÃO

1 – Após a divulgação deste edital no sítio <http://www.comprasgovernamentais.gov.br>, as licitantes deverão encaminhar, exclusivamente por meio do sistema eletrônico, concomitantemente com os documentos de habilitação exigidos no edital, proposta com a descrição do objeto ofertado e o preço (anexo II, do módulo I), com as características mínimas e quantidades estipuladas no termo de referência, até a data e hora marcadas para abertura da sessão quando, então, encerrar-se-á a fase de recebimento de propostas.

2 – A participação no pregão eletrônico dar-se-á por meio da digitação de senha privativa da licitante e subsequente encaminhamento da proposta eletrônica de preços, acompanhada dos documentos de habilitação exigidos no edital.

3 – A licitante deverá, na elaboração de sua proposta, obedecer ao descrito no Módulo I – Termo de Referência, preenchida na forma do do anexo II – Planilhas de formação de preços, em arquivo único.

4 – A proposta de preços deverá ser redigida em língua portuguesa, sem alternativas, opções, emendas, ressalvas, borrões, rasuras ou entrelinhas, e dela deverá constar declaração da licitante de ciência de que o CJF realizará o contingenciamento das obrigações trabalhistas, conforme previsto na Resolução CNJ n. 169/2013 e alterações, bem como na IN CJF nº 01/2016, nos termos estabelecidos na cláusula da minuta do contrato;

4.1 – Para o preenchimento exclusivo do anexo II, do Módulo I deste Edital (planilha de preços) a empresa deverá observar:

4.1.1- O contido na nota técnica CJF/SCI n. 01/2013, ressalvadas as alterações legislativas, haja vista que a referida Nota Técnica é do ano de 2013, e deverá constar a indicação de cada um dos componentes, expressos em reais, incluídos todos os custos relacionados com a remuneração e encargos sociais incidentes sobre a prestação dos serviços, bem como tributos e demais despesas diretas e indiretas.

4.1.2 - Qualquer valor diferente do estudo realizado na Nota Técnica – para MAIOR ou para MENOR, deverá ser devidamente justificado pela licitante, podendo ser realizada diligência para comprovar as informações prestadas.

4.1.3 - A nota técnica e a planilha formadora de custos são modelos referenciais orientadores, devendo a licitante preencher uma planilha para cada tipo de posto e efetuar as alterações que julgar necessárias, devidamente justificadas, uma vez que servirão para demonstrar possíveis variações de custo/insumo no curso da execução contratual, e serão



PODER JUDICIÁRIO
CONSELHO DA JUSTIÇA FEDERAL

utilizadas como base em eventuais repactuações de preços, sendo de responsabilidade exclusiva da empresa dimensionar e equacionar os componentes do preço ofertado, inclusive encargos trabalhistas, sociais e tributos incidentes, não podendo alegar, posteriormente, desconhecimento de fatos ou erros no preenchimento da planilha, com fundamento para solicitar reequilíbrio econômico-financeiro da proposta/contrato.

4.1.4 - No que concerne à taxa administrativa (custos indiretos), a mesma deve contemplar, no mínimo, as despesas elencadas no item **3.9 da Nota Técnica CJF/SCI n. 01/2013**.

4.2- A proposta de preço deverá conter, ainda, memória de cálculo detalhada que contenha a metodologia e fórmulas adotadas pela licitante para obtenção dos valores propostos para os encargos e demais componentes da planilha de composição de custos e formação de preços dos serviços envolvidos na contratação, caso a licitante apresente encargos distintos dos constantes no Anexo II do Módulo I;

4.3 - Caso sejam apresentadas propostas de preços consideradas inexequíveis, levando-se em conta os quantitativos dos serviços, a qualificação exigida, bem como os salários praticados no mercado de trabalho local, o CJF poderá realizar diligências junto à licitante, consultando a planilha de formação de preços, para verificar a capacidade de cumprir com a proposta de prestação de serviços apresentada.

4.4 - No que concerne às justificativas quanto à exequibilidade dos itens constantes da planilha de custos, não serão aceitas justificativas genéricas, que indiquem que o valor será suportado pelos demais contratos firmados pela empresa, sem a devida comprovação de despesa, haja vista que o contrato firmado com este Conselho deve ser autossuficiente.

4.5 - Não serão aceitos percentuais **zerados ou irrisórios** nas rubricas referentes à taxa administrativa ou lucro. Entendendo-se como irrisório qualquer valor inferior a 1% nas respectivas rubricas.

4.6 - Somente será pago 0,20% de INCRA mediante comprovação de recolhimento.

4.7 - Tendo em vista que o prazo de vigência da Lei Complementar nº 110/2001 expirou em dezembro de 2006, o adicional do FGTS de 0,5% não poderá ser incluído no total de encargos sociais.

4.8 – Não poderá constar da planilha de formação do custo percentual de reserva técnica de acordo com orientação TCU.

4.9 - No que concerne ao lucro, para o anexo II – Módulo I, as empresas deverão emitir declaração da opção de LUCRO REAL, PRESUMIDO ou SIMPLES.

4.10 - Os percentuais dos impostos consignados em sua proposta deverão ser comprovados com a apresentação do recibo de entrega da declaração de informações econômico-fiscais da pessoa jurídica, conforme tabela:

Regime de Tributação	ISS	PIS	COFINS
Simple Nacional <u>(alíquota máxima)</u>	5% sobre o faturamento	0,57% sobre o faturamento	2,63% sobre o faturamento
Lucro Presumido	5% sobre o faturamento	0,65% sobre o faturamento	3,0% sobre o faturamento



PODER JUDICIÁRIO
CONSELHO DA JUSTIÇA FEDERAL

Regime de Tributação	ISS	PIS	COFINS
Lucro Real	5% sobre o faturamento	1,65% sobre o faturamento	7,6% sobre o faturamento

4.11 - A empresa optante pelo SIMPLES NACIONAL que venha a ser contratada deverá apresentar cópia de ofício comunicando à Receita Federal a assinatura do contrato, abrindo mão da opção pelo referido regime tributário, ficando ciente de que não mais se beneficiará deste regime de tributação a partir do mês seguinte à contratação, conforme Acórdão 2798/2010, do Plenário do Tribunal de Contas da União.

4.11.1 – No prazo de até 90 (noventa) dias a empresa deverá apresentar documentação que comprove a desvinculação do regime do Simples.

4.12 - As licitantes somente poderão orientar os seus custos de acordo com a tributação pelo SIMPLES NACIONAL, justificadamente, comprovando não exercerem atividades impeditivas, inclusive as atividades objeto desta licitação, e atenderem aos requisitos de receita bruta, nos termos da Lei Complementar n. 123/2006;

4.13 - Caso a licitante seja beneficiária do regime substitutivo da Contribuição Previdenciária sobre a folha de pagamento, deverá apresentar declaração, conforme modelo do Anexo III da Instrução Normativa RFB n. 1.436/2013, bem como comprovante de recolhimento da DARF do mês de fevereiro do ano corrente, que comprove a opção do pagamento via CPRB. Não obstante, deverá incluir, dentre o módulo de tributação, percentual relativo à CONTRIBUIÇÃO PREVIDENCIÁRIA Sobre a Receita Bruta – a CPRB.

5 – No campo destinado à descrição detalhada do objeto ofertado, a licitante deverá informar os dados complementares e singulares que o caracterizam, quando for o caso, não se admitindo a mera cópia do descritivo indicado no termo de referência, ficando a licitante sujeita a desclassificação.

6 – Serão irrelevantes quaisquer ofertas que não se enquadrem nas especificações exigidas.

7 – Serão irrelevantes quaisquer ofertas que não se enquadrem nas especificações exigidas no Módulo I – Termo de Referência.

8 – O prazo de validade das propostas será de 90 (noventa) dias.

9 – Os preços deverão ser finais, acrescidos de todas as despesas e conter somente duas casas decimais, não sendo admitidos valores simbólicos, irrisórios ou de valor zero, incompatíveis com os preços dos insumos e salários de mercado, acrescidos dos respectivos encargos, conforme definido no §3º do art. 44 da Lei n. 8.666/93.

10 – Até a abertura da sessão, a licitante poderá retirar ou substituir a proposta e os documentos de habilitação anteriormente inseridos no sistema.

11 - Os documentos complementares à proposta e à habilitação, quando necessários à confirmação daqueles exigidos no edital e já apresentados, serão encaminhados pelo licitante melhor classificado após o encerramento do envio de lances, no prazo mínimo de 2 (duas) horas.

12 – Qualquer elemento que possa identificar a licitante importará na desclassificação imediata da proposta.



PODER JUDICIÁRIO
CONSELHO DA JUSTIÇA FEDERAL

13 - Na etapa de apresentação da proposta e dos documentos de habilitação pelo licitante não haverá ordem de classificação das propostas, o que ocorrerá somente após os procedimentos de julgamento das propostas, nos termos do §7º, do artigo 26, do Decreto n. 10.024/2019.

14 - 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.

VII – DA ABERTURA DA SESSÃO E CLASSIFICAÇÃO DAS PROPOSTAS

1 – O pregoeiro, por meio do sistema eletrônico, dará início à sessão pública, na data e horário previstos na Cláusula I deste edital, com a divulgação das propostas de preços recebidas no prazo estipulado, as quais deverão guardar perfeita consonância com as especificações e condições detalhadas no edital.

1.1 – A comunicação entre o pregoeiro e as licitantes ocorrerá mediante troca de mensagens, em campo próprio do sistema eletrônico.

2 – O pregoeiro procederá à análise das propostas quanto ao atendimento aos requisitos deste edital, efetuando a classificação ou desclassificação da proposta, após que dará início à fase competitiva, das propostas classificadas.

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

4 – Caberá à 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 qualquer mensagem emitida pelo sistema ou de sua desconexão.

VIII – DA FORMULAÇÃO DE LANCES E DO DESEMPATE

1 – O sistema ordenará, automaticamente, as propostas classificadas pelo pregoeiro, sendo que somente estas participarão da fase de lances.

2 – Classificadas as propostas, o pregoeiro dará início à fase competitiva, quando então as licitantes poderão encaminhar lances exclusivamente por meio do sistema eletrônico, sendo informadas do recebimento e do respectivo horário de registro e valor.

3 – As licitantes poderão oferecer lances sucessivos, observados o horário fixado para abertura da sessão e as regras estabelecidas neste edital.

3.1 - O licitante somente poderá oferecer valor inferior ao último lance por ele ofertado e registrado pelo sistema, observado o intervalo mínimo de 1 % entre os lances, que incidirá tanto em relação aos lances intermediários quanto em relação ao lance que cobrir a melhor oferta. (parágrafo único, do artigo 31 c/c com o §3º, do artigo 30, ambos do Decreto n. 10.024/2019).

3.2 - Não serão aceitos dois ou mais lances iguais e prevalecerá aquele que for recebido e registrado primeiro.



PODER JUDICIÁRIO
CONSELHO DA JUSTIÇA FEDERAL

4 – No transcurso da sessão pública, as licitantes serão informadas, em tempo real, do lance de menor valor registrado, vedada a identificação da detentora do lance.

5 – Os lances apresentados e levados em consideração para efeito de julgamento serão de exclusiva e total responsabilidade da licitante, não lhe cabendo o direito de pleitear qualquer alteração, seja para menos ou para mais.

6 – A etapa de lances da sessão pública **será aberta** e perdurará por 10 (dez) minutos. Quando houver lance ofertado nos últimos dois minutos do período de duração da sessão, o sistema prorrogará a fase automaticamente, nos termos do *caput*, do artigo 32, do Decreto n. 10.024/2019.

6.1 - A prorrogação automática da etapa de envio 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 quando se tratar de lances intermediários, nos termos do §1º, do artigo 32, do Decreto n. 10.024/2019.

6.2 - Na hipótese de não haver novos lances na forma estabelecida nos itens 6 e 6.1, a sessão pública será encerrada automaticamente.

7 - Encerrada a sessão pública sem prorrogação automática pelo sistema, nos termos do disposto no 6.1, o pregoeiro poderá, assessorado pela equipe de apoio, admitir o reinício da etapa de envio de lances, em prol da consecução do melhor preço, mediante justificativa. (Decreto n. 10.024/2019, art. 32, §3º).

8 – Do desempate:

8.1 Quando houver participação nesta licitação de microempresas ou empresas de pequeno porte, considerar-se-á empate quando a proposta dessas empresas for igual ou até **5% (cinco por cento)** superior à proposta classificada em primeiro lugar. Neste caso, e desde que a proposta classificada em primeiro lugar não tenha sido apresentada por microempresa ou empresa de pequeno porte, o sistema eletrônico procederá da seguinte forma:

a) classificação das propostas de microempresas ou empresas de pequeno porte que se enquadrem na situação prevista neste item 8.1;

b) convocação da microempresa ou empresa de pequeno porte que apresentou a menor proposta dentre as classificadas na forma da alínea “a” deste item para que, no prazo de 5 (cinco) minutos após o encerramento dos lances, sob pena de preclusão, apresente uma última oferta, obrigatoriamente inferior à da primeira colocada, para o desempate, situação em que será classificada em primeiro lugar;

c) não sendo apresentada proposta pela microempresa ou empresa de pequeno porte, na situação da alínea “b” deste item ou não ocorrendo a contratação, serão convocadas, na ordem e no mesmo prazo, as propostas remanescentes classificadas na forma da alínea “a” deste item, para o exercício do mesmo direito

d) caso a ME/EPP classificada em segundo lugar desista ou não se manifeste no prazo estabelecido, o sistema convocará as demais ME/EPP participantes na mesma condição, na ordem de classificação. Havendo êxito nesse procedimento, o sistema disponibilizará a nova classificação das licitantes para fins de aceitação;



PODER JUDICIÁRIO
CONSELHO DA JUSTIÇA FEDERAL

9 - Não havendo êxito, ou não existindo ME/EPP participante e havendo igualdade de condições, será utilizado como critério de desempate, a preferência critério estabelecida no §2º, do art. 3º da Lei n. 8.666, de 1993.

10 - Na hipótese de persistir o empate, a proposta vencedora será sorteada pelo sistema eletrônico dentre as propostas empatadas.

11 - Não poderá haver desistência dos lances efetuados, sujeitando-se a empresa licitante desistente às penalidades previstas neste edital.

12 - Caso ocorra desconexão do pregoeiro no decorrer da etapa de lances e se o sistema eletrônico permanecer acessível às licitantes, os lances continuarão sendo recebidos, sem prejuízo dos atos realizados.

13 - Quando a desconexão do pregoeiro persistir por tempo superior a 10 (dez) minutos, a sessão do pregão, na forma eletrônica, será suspensa e reiniciada somente decorridas 24 (vinte e quatro) horas após a comunicação do fato aos participantes no sítio <http://www.comprasgovernamentais.gov.br>.

IX – DA NEGOCIAÇÃO E JULGAMENTO DAS PROPOSTAS

1 - Apurada a melhor oferta no sistema, o pregoeiro iniciará a fase de negociação.

2 - O pregoeiro encaminhará contraproposta diretamente à licitante que tenha apresentado o lance mais vantajoso, para que seja obtida uma melhor proposta, observando o critério de julgamento, não se admitindo negociar condições diferentes daquelas previstas neste edital.

3 - Havendo negociação, a licitante terá o prazo no mínimo de 2 (duas) horas, contado da solicitação do pregoeiro no sistema, para envio da proposta negociada e, se necessário, dos documentos complementares, adequada à negociação.

4 - Encerrada a etapa de negociação de que trata o item anterior, o pregoeiro examinará a proposta classificada em primeiro lugar quanto à adequação ao objeto e à compatibilidade do preço, observado o disposto no parágrafo único do art. 7º e no § 9º do art. 26 do Decreto n. 10.204/2019, e verificará a habilitação do licitante conforme disposições do edital.

5 - Se a proposta não for aceitável ou se a licitante não atender às exigências habilitatórias, o pregoeiro examinará a proposta subsequente e, assim sucessivamente, na ordem de classificação, até a apuração de uma proposta que atenda ao edital.

6 - O critério de julgamento das propostas será o de **MENOR PREÇO GLOBAL**, desde que satisfeitos todos os termos estabelecidos neste ato convocatório.

7 - No julgamento das propostas, o pregoeiro poderá sanar erros ou falhas que não alterem a substância das propostas e sua validade jurídica, mediante despacho fundamentado, registrando em ata e acessível a todos, atribuindo-lhes validade e eficácia para fins de classificação.

7.1 - Na hipótese de necessidade de suspensão da sessão pública para a realização de diligências, com vistas ao saneamento de que trata o item anterior, a sessão pública



PODER JUDICIÁRIO
CONSELHO DA JUSTIÇA FEDERAL

somente poderá ser reiniciada mediante aviso prévio no sistema com, no mínimo, 24 (vinte e quatro) horas de antecedência, cuja ocorrência será registrada em ata.

X – DA HABILITAÇÃO

1. - Os documentos para habilitação encontram-se listados abaixo:

1.1 – Em se tratando de filial, os documentos de habilitação jurídica e regularidade fiscal deverão estar em nome da filial, exceto aqueles que são emitidos somente em nome da matriz

Habilitação jurídica

- a)** cédula de identidade;
- b)** registro comercial, no caso de empresário individual;
- c)** ato constitutivo, estatuto ou contrato social em vigor, devidamente registrado, em se tratando de sociedades comerciais, e, no caso de sociedades por ações, acompanhado de documentos de eleição de seus administradores e alterações ou da consolidação respectiva;
- d)** inscrição do ato constitutivo, no caso de sociedade civil, acompanhado da prova de diretoria em exercício;
- e)** decreto de autorização, em se tratando de empresa ou sociedade estrangeira em funcionamento no país, e ato de registro ou autorização para funcionamento expedido pelo órgão competente, quando a atividade assim o exigir;

Regularidade fiscal e trabalhista

- f)** comprovante de inscrição no Cadastro de Pessoas Físicas – CPF e comprovante de inscrição no Cadastro Nacional de Pessoa Jurídica - CNPJ do Ministério da Fazenda;
- g)** comprovante de inscrição no cadastro de contribuintes estadual ou municipal relativo à sede da licitante, pertinente ao seu ramo de atividade e compatível com o objeto contratual.
- h)** 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;
- i)** prova de regularidade para com as Fazendas Estadual ou Municipal do domicílio ou sede da licitante;
- j)** Certificado de Regularidade do FGTS – CRF, emitido pela Caixa Econômica Federal;
- k)** Certidão Negativa de Débitos Trabalhistas – CNDT, emitida pela Justiça do Trabalho;

Qualificação Técnica

- l)** É obrigatório às licitantes, apresentar atestado(s) ou certidão(ões) de capacidade técnico-operacional comprobatórios de que a empresa proponente tenha executado ou esteja executando, serviços de características técnicas semelhantes às do objeto do presente Edital;
- m)** Os Atestado(s) de Capacidade Técnica-Operacional deverá(ão) ser emitido(s) por entidade da Administração Federal, Estadual ou Municipal, direta ou indireta e/ou empresa privada que comprove ter a empresa licitante executado serviços de características técnicas semelhantes ao objeto desta contratação nos termos da Lei, comprovando:

m.1) Experiência na prestação de serviços de administração de solução de Gerenciamento Unificado de Ameaças - UTM;



PODER JUDICIÁRIO
CONSELHO DA JUSTIÇA FEDERAL

- m.2)** Experiência na prestação de serviços de administração de solução de anti-malware para estações de trabalho em ambiente computacional com, no mínimo, 250 (duzentos e cinquenta) estações de trabalho;
- m.3)** Experiência na prestação de serviços de administração de solução de anti-malware para ambiente de datacenter utilizando plataforma de virtualização de rede VMware NSX com, no mínimo, 200 (duzentos) servidores de rede;
- m.4)** Experiência na prestação de serviços de administração de solução de segurança para proteção de gateway de e-mail, contemplando proteção *anti-malware* e *anti-spam* em ambiente computacional com, no mínimo, 250 (duzentos e cinquenta) caixas postais;
- m.5)** Experiência na prestação de serviços de monitoramento proativo e resposta a incidentes de segurança da informação em ambientes com, no mínimo, 400 (quatrocentos) ativos;
- m.6)** Experiência na prestação de serviços de gestão de vulnerabilidades, incluindo o monitoramento e o tratamento das vulnerabilidades encontradas em ambientes com, no mínimo, 400 (quatrocentos) ativos;
- m.7)** Experiência na prestação de serviços de administração de solução de Gerenciamento e Correlação de Eventos de Segurança da Informação - SIEM, em ambientes com, no mínimo, 400 (quatrocentos) ativos;
- m.8)** Experiência na prestação de serviços de testes de invasão para exploração de vulnerabilidades de segurança da informação, em conformidade com boas práticas internacionais;
- n)** Entende-se por similar, soluções ou produtos (equipamentos ou softwares) com funcionalidades equivalentes, escalabilidade compatível e porte corporativo;
- o)** Deverão constar do(s) atestado(s) de capacidade técnica-operacional em destaque, os seguintes dados: identificação do emitente, especificação do fornecimento/serviço executado, prazo de vigência do contrato, local e data de expedição, data de início e término, quando for o caso, do contrato;
- p)** Será permitido o somatório de atestado(s) de capacidade técnica-operacional para efeito de comprovação de experiência na prestação dos serviços de características técnicas semelhantes ao objeto desta contratação;
- q)** O CONTRATANTE poderá diligenciar a pessoa jurídica indicada no Atestado de Capacidade Técnica-Operacional, visando validar ou esclarecer informações sobre o serviço prestado;

Qualificação Econômico-financeira

- r)** Certidão Negativa de Falência e Recuperações Judiciais, expedida pelo Distribuidor da sede da pessoa jurídica;
- r.1)** a certidão negativa de recuperação judicial é exigível por força do art. 31, II, da Lei 8.666, de 1993, porém a certidão positiva não implica a imediata inabilitação, cabendo ao CJF realizar diligências para avaliar a real situação de capacidade econômico-financeira, mediante a apresentação do plano de recuperação aprovado e homologado judicialmente,



PODER JUDICIÁRIO
CONSELHO DA JUSTIÇA FEDERAL

com a recuperação já deferida, nos termos do Item 3.6.1, da cláusula V – DAS CONDIÇÕES DE PARTICIPAÇÃO E DA CONCESSÃO DOS BENEFÍCIOS À ME/EPP.

s) Balanço Patrimonial do exercício social exigível na forma da lei e regulamentos na data de realização da licitação, vedada sua substituição por balancetes ou balanços provisórios, podendo ser atualizado por índices oficiais quando encerrados há mais de 3 (três) meses da data da apresentação da proposta;

t) demonstração do Resultado do Exercício (DRE) relativa ao último exercício social exigível, apresentado na forma da lei;

u) qualificação econômico-financeira válida no SICAF;

u.1) comprovação de patrimônio líquido não inferior a 10% (dez por cento) do valor estimado da contratação, quando qualquer dos índices Liquidez Geral, Liquidez Corrente e Solvência Geral, informados pelo SICAF, for igual ou inferior a 1, devendo a comprovação ser feita através do balanço exigido na alínea “m”;

u.2) Os índices serão obtidos a partir das seguintes fórmulas:

a) LG – Liquidez Geral;

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

b) LC – Liquidez Corrente;

$$\text{Liquidez Corrente} = \frac{\text{Ativo Circulante}}{\text{Passivo Circulante}}$$

c) SG – Solvência Geral;

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

v) os termos do art. 3º do Decreto n.º 8.538/2015, não será exigida da microempresa ou da empresa de pequeno porte a apresentação de balanço patrimonial do último exercício social e, por conseguinte, a comprovação de que trata esta condição.

2. Documentação Complementar:

a) Certidão Negativa de improbidade Administrativa e Inelegibilidade, do Cadastro Nacional de Condenações Cíveis por Ato de Improbidade Administrativa, disponível no Portal do Conselho Nacional de Justiça (CNJ) (www.cnj.jus.br), por meio do link *Sistemas e Serviços>outros>consulta requerido/Condenação:Retorna os requeridos cadastrados nos sistemas, podendo-se detalhar as suas respectivas condenações*;

b) como condição para habilitação será verificada a existência de registros impeditivos de contratação, no Cadastro Nacional de Empresas Inidôneas e Suspensas/CGU, disponível no Portal da Transparência (<http://portaltransparencia.gov.br>), em atendimento ao disposto no Acórdão n. 1793/2011, do Plenário do Tribunal de Contas da União;

c) As documentações indicadas nas letras "a" e "b" poderão ser substituídas pela Certidão/Consulta Consolidada de Pessoa Jurídica, do Tribunal de Contas da União (TCU), disponível através do link: <https://certidoes-apf.apps.tcu.gov.br/>.

3. Declarações exigidas:

a) Declaração de cumprimento do disposto no artigo 7º, XXXIII, da Constituição Federal/88, e artigo 27, inciso V, da Lei n. 8.666/93;

b) Declaração de inexistência de fato superveniente impeditivo de habilitação, na forma do artigo 32, §2º, da Lei n. 8.666/93.



PODER JUDICIÁRIO
CONSELHO DA JUSTIÇA FEDERAL

4. A documentação elencada no Item 3 desta Cláusula deverá ser formalizada em campo próprio no sistema.

5 As declarações extraídas do Sistema de Cadastramento Unificado de Fornecedores – SICAF substituirão os documentos relacionados nas alíneas ‘a’ a ‘k’ do item 1, para fins de habilitação da licitante cadastrada naquele sistema. Essas declarações somente serão válidas nas seguintes condições:

- a)** se as informações relativas àqueles documentos estiverem disponíveis para consulta na data da sessão de recebimento da proposta e da documentação; e
- b)** se estiverem dentro dos respectivos prazos de validade.

6 – Os documentos exigidos para habilitação que não estejam contemplados no SicaF serão enviados nos no prazo de apresentação das propostas.

7 - Caso conste na Consulta de Situação do Fornecedor a existência de Ocorrências Impeditivas Indiretas, o CJF irá diligenciar à licitante para verificar a possibilidade de fraude à licitação, mediante a checagem dos vínculos societários da empresa, linhas de fornecimentos similares, dentre outras formas admitidas, sendo assegurado o contraditório e a ampla defesa, nos termos do art. 29 da IN n. 03/2018 /MPOG.

8 - O descumprimento das exigências contidas nesta cláusula determinará a inabilitação da licitante.

9 – Para as ME/EPP a comprovação da regularidade fiscal somente será exigida para efeito de formalização do ajuste.

9.1 – As ME/EPP deverão apresentar toda a documentação arrolada nesta cláusula, ainda que apresentem alguma restrição.

9.2 – Havendo alguma restrição na comprovação da regularidade fiscal, será assegurado o prazo de 5 (cinco) dias úteis, cujo termo inicial corresponderá ao momento em que a licitante for declarada vencedora do certame, para a regularização da documentação, pagamento ou parcelamento do débito, e emissão de eventuais certidões negativas ou positivas com efeito de certidão negativa.

9.2.1 – O prazo que trata o subitem 9.2 poderá ser prorrogado, por igual prazo, a critério da administração, nos termos do decreto 8.538/2015 de 6 de outubro de 2015.

9.3 – A não-regularização da documentação, no prazo previsto nos subitens 9.2 e 9.2.1 desta cláusula, implicará decadência do direito à contratação, sem prejuízo da sanção prevista neste edital e em lei, sendo facultado à Administração convocar as licitantes remanescentes, na ordem de classificação, para a formalização da avença, ou revogar a licitação.

10 – Sempre que julgar necessário, o pregoeiro poderá solicitar a apresentação de originais dos documentos exigidos da licitante.

11 – Não serão aceitos “protocolos de entrega” ou “solicitações de documentos” em substituição aos comprovantes exigidos no presente edital.



PODER JUDICIÁRIO
CONSELHO DA JUSTIÇA FEDERAL

12 – No julgamento da habilitação, o pregoeiro poderá sanar erros ou falhas que não alterem a substância 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.

12.1 - Na hipótese de necessidade de suspensão da sessão pública para a realização de diligências, com vistas ao saneamento de que trata o item anterior a sessão pública somente poderá ser reiniciada mediante aviso prévio no sistema com, no mínimo, 24 (vinte e quatro) horas de antecedência, e a ocorrência será registrada em ata.

12.2 - Caso seja necessário o envio de documentos complementares, após o julgamento das propostas, quando necessários à confirmação daqueles exigidos no edital e já apresentados, a licitante deverá o encaminhá-los, em formato digital, via sistema, no prazo estipulado na cláusula IV deste Edital.

12.3 – No caso dos documentos que estejam disponíveis e que possam ser consultados pelo pregoeiro diretamente nos sistemas informatizados, os mesmos poderão ser consultados para comprovar a regularidade do licitante.

13 – Verificado o desatendimento de quaisquer dos requisitos de habilitação, o pregoeiro examinará a aceitabilidade da proposta e o preenchimento das exigências habilitatórias por parte da licitante classificada subsequente e, assim, sucessivamente, até a apuração de uma proposta que atenda as exigências do edital.

14 – A inabilitação será sempre fundamentada e registrada no sistema, com acompanhamento em tempo real por todos os participantes.

15 – Constatado o atendimento dos requisitos habilitatórios, o pregoeiro habilitará e declarará vencedora do certame a licitante correspondente.

XI – DA PROPOSTA DEFINITIVA DE PREÇO

1 – A licitante vencedora deverá enviar a proposta definitiva de preço, elaborada nos moldes do módulo II do edital, por meio do *link* “Enviar anexo/planilha atualizada”, no prazo máximo de 2 (duas) horas, a contar da solicitação do pregoeiro no sistema eletrônico, sob pena de ser considerada desistente, sujeitando-se às sanções previstas na cláusula XIV (Das Penalidades) deste edital.

1.1 – A critério do pregoeiro e por manifestação da licitante o prazo acima determinado poderá ser prorrogado.

2 – Para garantir a integridade da documentação e da proposta, recomenda-se que contenham índice e folhas numeradas e timbradas com o nome, logotipo ou logomarca da licitante.

3 – A proposta de preços deverá ser redigida em língua portuguesa, impressa, sem alternativas, opções, emendas, ressalvas, borrões, rasuras ou entrelinhas, e dela deverão constar:

3.1 – Razão social da empresa, CNPJ, endereço completo, telefone, correio eletrônico para contato e convocação para assinatura do contrato, banco, agência, praça de pagamento e conta corrente, assinatura e nome legível do representante legal da empresa responsável pela proposta.



PODER JUDICIÁRIO
CONSELHO DA JUSTIÇA FEDERAL

3.2 – O endereço e CNPJ informados deverão ser do estabelecimento que de fato emitirá a nota fiscal/fatura.

3.3 – Declaração da licitante de ciência de que o CJF realizará o contingenciamento das obrigações trabalhistas, conforme previsto na IN CJF nº 1/2016 e na Resolução CNJ n. 169/2013 e alterações, nos termos estabelecidos na Cláusula Oitava da minuta do contrato.

3.4 – Preço mensal e anual (com tributos, insumos e demais encargos da contratação), com exibição do valor em algarismos e por extenso, com duas casas decimais, conforme o lance final.

XII – DOS RECURSOS

1 – Declarada a vencedora, qualquer licitante poderá manifestar motivadamente, dentro do prazo de 30 (trinta) minutos, a intenção de recorrer durante a sessão pública, em campo próprio no sistema eletrônico. Não havendo intenção registrada, o pregoeiro adjudicará o objeto da licitação em favor da licitante julgada vencedora.

2 – A falta de manifestação imediata e motivada da licitante implicará decadência do direito de recurso.

3 – O pregoeiro fará juízo de admissibilidade da intenção de recurso manifestada, aceitando-a ou, motivadamente, rejeitando-a, em campo próprio do sistema.

4 – A recorrente que tiver sua intenção de recurso aceita deverá registrar as razões do recurso, em campo próprio do sistema, no prazo de 3 (três) dias, ficando as demais licitantes, desde logo, intimadas a apresentar contrarrazões em igual prazo, via sistema, que começará a correr do término do prazo da recorrente, sendo-lhes assegurada vista imediata dos elementos indispensáveis à defesa dos seus interesses.

5 – O acolhimento do recurso importará a invalidação apenas dos atos insuscetíveis de aproveitamento.

6 – Os autos do processo permanecerão com vista franqueada aos interessados.

7 – Decidido o recurso e constatada a regularidade dos atos procedimentais, a autoridade superior adjudicará o objeto à licitante vencedora e homologará o procedimento para determinar a contratação.

XIII – DA DOTAÇÃO ORÇAMENTÁRIA

1. A despesa decorrente desta licitação correrá à conta de recursos consignados ao Conselho da Justiça Federal no Orçamento Geral da União, Programa de Trabalho Resumido - PTRES: AI (Ações de Informática) 085322, Natureza de Despesa - ND: 33.90.40.11 (Suporte de Infraestrutura de TIC).

XIV – DO PAGAMENTO

1 – O pagamento será efetuado por ordem bancária, até o 10º dia útil, após o atesto firmado pela fiscalização da nota fiscal/fatura, cujo documento deverá estar em conformidade com as condições estabelecidas.



PODER JUDICIÁRIO
CONSELHO DA JUSTIÇA FEDERAL

1.1 - As notas fiscais deverão ser emitidas eletronicamente e encaminhadas ao gestor pelo e-mail: sutec@cjf.jus.br; ou outro à critério da administração ou enviadas pelo sistema eletrônico (sei.cjf.jus.br) e encaminhadas para SUTEC.

2 – O CJF descontará do valor devido as retenções previstas na legislação tributária vigente à época do pagamento.

XV – DAS PENALIDADES

1. a licitante, em caso de descumprimento às regras deste edital, e observado o regular processo administrativo, assegurado o contraditório e à ampla defesa, nos termos da lei, ficará sujeita às seguintes penalidades:

a) advertência;

b) multa compensatória:

b.1) 5%, calculada sobre o valor adjudicado, em caso de não regularização da documentação exigida para ME/ EPP, nos prazos previstos na Cláusula X;

b.2) 10%, calculada sobre o valor homologado, em caso de não assinatura da ata e/ou contrato;

c) declaração de inidoneidade, nos termos do art. 87, inciso IV, da Lei n. 8.666/1993;

1.1. As multas previstas nas alíneas b.1 e b.2 poderão cumular-se com as penalidades previstas nas alíneas a e c do Item acima.

1.2. O CJF, para aplicação da penalidade prevista no Item 1, adotará os critérios previstos nos art. 86 e 87 da Lei n. 8.666/1993.

2. Nos termos do art. 7º da Lei n. 10.520/2002, ficará impedido de licitar e contratar com a União e será descredenciado do SICAF, pelo prazo de até 5 (cinco) anos, sem prejuízo das multas previstas neste edital e das demais penalidades legais, aquele que:

a) não assinar a ata ou contrato nos prazos de 5 (cinco) dias, contados da efetiva convocação:

Pena - impedimento do direito de licitar e contratar com a União e descredenciamento do Sistema de Cadastramento Unificado de Fornecedores - SICAF pelo período de 4 (quatro) meses;

b) deixar de entregar documentação exigida para o certame:

Pena - impedimento do direito de licitar e contratar com a União e descredenciamento do SICAF pelo período de 2 (dois) meses;

c) fizer declaração falsa ou entregar documentação falsa:

Pena - impedimento do direito de licitar e contratar com a União e descredenciamento do SICAF pelo período de 24 (vinte e quatro) meses;

d) não manter a proposta:

Pena - impedimento do direito de licitar e contratar com a União e descredenciamento do SICAF pelo período de 4 (quatro) meses;

e) comportar-se de modo inidôneo:



PODER JUDICIÁRIO
CONSELHO DA JUSTIÇA FEDERAL

Pena - impedimento do direito de licitar e contratar com a União e descredenciamento do SICAF pelo período de 24 (vinte e quatro) meses;

f) cometer fraude fiscal:

Pena - impedimento do direito de licitar e contratar com a União e descredenciamento do SICAF pelo período de 40 (quarenta) meses.

2.1. O CJF, para aplicação da penalidade prevista no Item 2, adotará os critérios previstos na Instrução Normativa n. 1, de 13/10/2017, da Presidência da República, publicada no DOU, em 16/10/2017 (n. 198, Seção 1, pág. 5).

3. A aplicação de qualquer penalidade prevista nesta cláusula levará em consideração os critérios de razoabilidade e proporcionalidade, ficando a cargo do CJF decidir sobre a mais adequada ao caso concreto.

3.1. A critério da autoridade competente do CJF com fundamento nos Princípios da Proporcionalidade e Razoabilidade, as penalidades poderão ser relevadas ou atenuadas, em razão de circunstâncias fundamentadas, mediante comprovação dos fatos e, desde que formuladas por escrito, no prazo máximo de 5 (cinco) dias úteis, contados da data da notificação.

4. A aplicação das sanções previstas nesta cláusula será realizada mediante processo administrativo específico, mediante comunicação à licitante da penalidade, sendo assegurado, em todos os casos, o contraditório e a ampla defesa, no prazo de 5 (cinco) dias, contados do recebimento da comunicação.

5. Fica assegurado à licitante o uso dos recursos previstos em lei.

6. As penalidades previstas nesta cláusula referem-se ao descumprimento do certame licitatório, ficando as penalidades pelo descumprimento contratual previstas na minuta de contrato a qual é anexa a este edital.

XVI – DO SISTEMA DE REGISTRO DE PREÇOS

1 – O sistema de registro de preços regula-se pelas normas e procedimentos previstos no Decreto n. 7.892, de 23 de janeiro de 2013.

1.1 – A Sistema de Registro de Preços para a presente licitação se enquadra nas hipóteses previstas nos incisos II e III do artigo 3º do Decreto em referência.

2 – No âmbito do Sistema de Registro de Preços, a adjudicação significa tão somente o registro do preço ofertado.

3 – A existência do registro não obriga a Administração a efetivar as contratações por esse meio, ficando-lhe facultada a aquisição por outras modalidades, respeitada a legislação relativa às licitações, sendo assegurado à detentora da ata o direito de preferência em igualdade de condições.

4 – Na presente licitação **NÃO** serão permitidas adesões à ata (caronas), previstas no artigo 22 do Decreto n. 7.892 (de 23 janeiro 2013). (Acórdão TCU n. 1.297/2015 – Plenário, TC 003.377/2015-6, relator Ministro Bruno Dantas, 27.5.2015)



PODER JUDICIÁRIO
CONSELHO DA JUSTIÇA FEDERAL

XVII – DA ATA DE REGISTRO DE PREÇOS

1 – Encerrado o processo licitatório, o CJF, respeitada a ordem de classificação, convocará a adjudicatária e as interessadas remanescentes para, dentro do prazo de 5 (cinco) dias úteis, assinarem a ata, cuja minutas integram este edital e que, após publicados terão efeito de compromissos de fornecimento nas condições estabelecidas.

2 – Quando a empresa vencedora e as demais interessadas, ao serem convocadas, não assinarem a ata no prazo e condições estabelecidas, será facultado ao CJF, sem prejuízo de se aplicar as sanções previstas neste edital e em lei, convocar as licitantes seguintes, na ordem de classificação, para formalização do ajuste.

3 – Ao assinar a ata de registro de preços a licitante vencedora obriga-se a realizar o fornecimento/serviço a ela adjudicado, conforme especificações e condições contidas neste edital, em seus módulos e na proposta de preços apresentada, prevalecendo, no caso de divergência, as especificações e condições do edital.

4 – Por ocasião da assinatura da ata o CJF realizará consulta com vistas a comprovar a manutenção das condições de habilitação e qualificação exigidas na licitação, nos termos do art. 55, inciso XIII, da Lei n. 8.666/93.

5 – O representante da licitante vencedora deverá apresentar, ao CJF, os documentos pessoais (RG e CPF), e se for o caso, procuração particular, com firma reconhecida, ou pública, com poderes para assinar a ata, caso não tenham sido apresentados na fase de habilitação.

5.1 – Caso haja alguma alteração na documentação exigida no procedimento de habilitação, esta deverá ser apresentada na formalização dos ajustes.

5.2 – Os documentos deverão ser apresentados na forma de cópia autenticada por cartório competente ou, na forma original acompanhados de cópia, a qual será autenticada por servidor deste CJF.

6 – Farão parte integrante da ata todos os elementos apresentados pela empresa que tenham servido de base para o julgamento, bem como as condições estabelecidas neste edital.

7 – Formalizada a ata, durante sua vigência, a empresa estará obrigada ao seu cumprimento.

8 – A ata terá validade de 12 (doze) meses, a partir da data da assinatura.

9 – Nos termos do §1º do art. 12 do Decreto 7.892/2013, é vedado efetuar acréscimos nos quantitativos fixados nesta ata.

10 – Durante a vigência da ata a empresa fica obrigada a fornecer os itens de acordo com o preço registrado, nas quantidades indicadas em cada nota de empenho, respeitando-se as características do objeto constantes do termo de referência.

11 – O objeto será devolvido na hipótese de apresentar irregularidades, não corresponder às especificações da ata de registro de preços ou estar fora dos padrões determinados, devendo ser substituído pela empresa detentora da ata no prazo máximo de 48 (quarenta e oito) horas a contar da notificação, sob pena de aplicação das penalidades previstas na cláusula XVI deste edital.



PODER JUDICIÁRIO
CONSELHO DA JUSTIÇA FEDERAL

XVIII – DA CONTRATAÇÃO

1. Homologada a licitação, o CJF convocará a licitante vencedora, durante a validade da sua proposta, para assinatura, por meio eletrônico, do instrumento contratual, que se dará em até 5 (cinco) dias úteis, mediante uso do Sistema Eletrônico de Informações (SEI) do CJF, sem prejuízo das sanções previstas neste edital e no art. 81 da Lei n. 8.666/1993.

1.1. O prazo de convocação poderá ser prorrogado uma vez, por igual período, quando solicitado pela parte durante o seu transcurso e desde que ocorra motivo justificado aceito pela Administração.

2. Impreterivelmente dentro do prazo de 3 (três) dias úteis, contados da data da convocação, a licitante vencedora deverá requerer cadastramento no Sistema Eletrônico de Informações (SEI) do CJF.

3. É facultado à Administração, quando a adjudicatária não assinar o contrato, no prazo e nas condições estabelecidos, convocar outra licitante, obedecida a ordem de classificação, para assiná-lo, após comprovados os requisitos de habilitação, feita a negociação e aceita a proposta.

4. Por ocasião da assinatura do contrato, verificar-se-á por meio do SICAF e de outros meios se a adjudicatária mantém as condições de habilitação.

5. O CJF poderá requerer, no momento da assinatura do contrato, a documentação pessoal (RG e CPF) e a que confere poderes para a formalização do instrumento contratual.

6 – Farão parte integrante do Contrato todos os elementos apresentados pela empresa que tenham servido de base para o julgamento, bem como as condições estabelecidas neste edital.

7 – Formalizado o Contrato, a empresa estará obrigada ao seu cumprimento, durante sua vigência.

8 – O contrato terá vigência de 24 (vinte e quatro) meses, contados a partir da assinatura, podendo ser prorrogado por igual período ou fração, mediante termo aditivo, até o limite de 60 (sessenta) meses.

9 – Em cumprimento ao constante da Resolução n. 9, de 6 de dezembro de 2005, do Conselho Nacional de Justiça, é vedada a manutenção, aditamento ou prorrogação de contrato de prestação de serviços com empresa que venha a contratar empregados que sejam cônjuges, companheiros ou parentes em linha reta, colateral ou por afinidade, até o terceiro grau, inclusive, de ocupantes de cargos de direção e de assessoramento, de membros ou juízes vinculados a este CJF.

XIX – DA REPACTUAÇÃO E DO REAJUSTE

1 – A repactuação e o reajuste serão devidos de acordo com a Cláusula Décima Segunda – Da Repactuação e do Reajuste, Minuta de Contrato, Módulo II deste Edital.

XX – DA GARANTIA

1 – Para o integral cumprimento de todas as obrigações contratuais assumidas, inclusive indenização a terceiros e multas eventualmente aplicadas, será exigida garantia correspondente a 3% (três por cento) do valor total contratado, em uma das modalidades do art. 56, §1º da Lei n. 8.666/93, nos termos constantes da Cláusula Décima Sexta da Minuta de Contrato (Módulo II).



PODER JUDICIÁRIO
CONSELHO DA JUSTIÇA FEDERAL

2 – Não serão aceitos instrumentos de garantia que contenham cláusulas conflitantes com dispositivos contratuais ao até mesmo restrinjam-lhe a cobertura ou a sua eficácia.

XXI – DA VISTORIA

1 – A empresa licitante caso julgue conveniente para o correto dimensionamento e cumprimento das obrigações, poderá realizar uma vistoria nas instalações do CONTRATANTE para tomar conhecimento dos serviços a serem realizados. Não serão admitidas, em hipótese alguma, alegações posteriores de desconhecimento dos serviços e de dificuldades técnicas não previstas.

1.1 – A vistoria deverá ocorrer por horário marcado, e será agendada, por meio dos telefones (61) 3022-7400/7403.

1.2 – O agendamento de vistoria poderá ocorrer até 48 (quarenta e oito) horas antes da data e horário de abertura do processo licitatório.

1.3 – A vistoria técnica deverá ser realizada em até, no máximo, 24 (vinte e quatro) horas da abertura do processo licitatório.

XXII - DA ADJUDICAÇÃO E HOMOLOGAÇÃO

1. O objeto deste pregão será adjudicado pelo pregoeiro, salvo quando houver recurso, hipótese em que a adjudicação caberá à autoridade competente para homologação.

XXIII – DAS DISPOSIÇÕES FINAIS

1 – Estabelece-se que a simples apresentação de proposta pelas licitantes implicará a aceitação de todas as disposições do presente edital.

2 – Assegura-se a este Conselho o direito de:

2.1 – Promover, em qualquer fase da licitação, diligência destinada a esclarecer ou a complementar a instrução do processo (art. 43, §3º, da Lei n. 8.666/93), fixando as licitantes, prazos para atendimento, vedada a inclusão posterior de informação que deveria constar originalmente da proposta;

2.2 – Caso entenda necessário examinar mais detidamente a conformidade das propostas com os requisitos estabelecidos neste edital, bem como o preenchimento das exigências habilitatórias, poderá o Pregoeiro, a seu exclusivo critério, suspender a sessão respectiva, hipótese em que comunicará às licitantes, desde logo, a data e horário em que o resultado do julgamento será divulgado no sistema eletrônico;

2.2.1 – A sessão pública somente poderá ser reiniciada mediante aviso prévio no sistema com, no mínimo, 24 (vinte e quatro) horas de antecedência, cuja ocorrência será registrada em ata.

2.3 – O pregoeiro ou a autoridade superior poderão subsidiar-se em pareceres emitidos por técnicos ou especialistas no assunto objeto desta licitação;



PODER JUDICIÁRIO
CONSELHO DA JUSTIÇA FEDERAL

2.4 – Revogar a presente licitação por razões de interesse público (art. 49, caput, da Lei n. 8.666/93), decorrente de fato superveniente devidamente comprovado;

2.5 – Adiar a data da sessão pública;

3 – As empresas licitantes serão responsáveis pela fidelidade e legitimidade das informações e dos documentos apresentados, em qualquer época ou fase do processo licitatório.

4 – O desatendimento de exigências formais e não essenciais, não importará o afastamento da licitante, desde que seja possível a aferição da sua qualificação e a exata compreensão da sua proposta durante a realização da sessão pública do pregão.

5 – As normas que disciplinam este pregão serão sempre interpretadas em favor da ampliação da disputa, desde que não comprometam o interesse da Administração e a segurança da contratação.

6 – Nenhuma indenização será devida às licitantes pela elaboração e/ou apresentação de documentos relativos à presente licitação.

7 – Os documentos originais ou cópias autenticadas, caso sejam solicitados, deverão ser encaminhados ao endereço constante no item 8, abaixo.

8 – O edital estará à disposição dos interessados, em meio digital, na Comissão Permanente de Licitação, localizada no 1º andar, sala 105, na Sede do CJF, situada no Setor de Clubes Esportivos Sul – SCES, Trecho III, Polo 8, Lote 9, Brasília/DF, CEP 70.200-003, telefones 3022-7510 e 7511, nos dias úteis, de 13h às 18h, e na internet para *download*, nos endereços eletrônicos www.comprasgovernamentais.gov.br e www.cjf.jus.br.

Brasília-DF, 22 de janeiro de 2020.

ANTONIO ANTUNES DE OLIVEIRA
Pregoeiro



PODER JUDICIÁRIO
CONSELHO DA JUSTIÇA FEDERAL

MÓDULO I DO EDITAL 1/2020

TERMO DE REFERÊNCIA

SECRETARIA DE TECNOLOGIA DA INFORMAÇÃO

1. OBJETO

Contratação de Serviços Gerenciados de Segurança da Informação, através de Sistema de Registro de Preços, para atendimento às necessidades do Conselho de Justiça Federal – CJF, de acordo com as especificações técnicas contidas neste Termo de Referência – TR e seus anexos.

2. DETALHAMENTO DO OBJETO

2.1 Os Serviços Gerenciados de Segurança da Informação envolvem a prestação dos seguintes serviços, que poderão ser solicitados **sob demanda**, mediante emissão de Ordem de Serviço - OS:

2.1.1 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 íntegro.

2.1.2 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.

2.1.3 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.

2.1.4 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,



PODER JUDICIÁRIO
CONSELHO DA JUSTIÇA FEDERAL

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.

2.1.5 Serviço de orquestração, automação e resposta de segurança (SOAR), com o objetivo de automatizar os processos e fluxos de trabalho, a aplicação de atividades rotineiras ou de difícil execução e a orquestração das diversas ferramentas de segurança, sem necessidade de atuação humana.

2.1.6 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.

2.2 Todos os serviços descritos pertencem a um único objeto e bloco de contratação denominado SERVIÇOS GERENCIADOS DE SEGURANÇA.

2.3 Os serviços serão solicitados **SOB DEMANDA**, mediante emissão de Ordem de Serviço (OS), em períodos múltiplos de 12 (doze) meses, **SEM GARANTIA DE CONSUMO MÍNIMO DE MESES**.

3. FUNDAMENTAÇÃO DA CONTRATAÇÃO

Objetivo da Contratação

Na sociedade da informação, ao mesmo tempo em que as informações são consideradas o principal patrimônio de uma organização, estão estas sob constante risco e necessitam ser adequadamente protegidas. Com isso, a Segurança da Informação tornou-se um ponto crucial para a sobrevivência das instituições.

A Segurança da Informação pode ser caracterizada pela aplicação adequada de controles sobre um conjunto de informações ou um ativo de informação com o objetivo de proteger e preservar o valor, tangível ou não, que este possui para as organizações. Entende-se por informação todo e qualquer conhecimento inscrito, gravado ou codificado em um meio de armazenamento.

Desta forma, a Segurança da Informação busca fundamentalmente garantir a confidencialidade, a integridade e a disponibilidade dos ativos de informação. Por ativo



PODER JUDICIÁRIO
CONSELHO DA JUSTIÇA FEDERAL

entende-se qualquer componente — seja físico, humano, lógico ou tecnológico — que possua valor e sustente processos de negócio de uma unidade ou da organização.

Neste sentido, o CJF conta com um contrato de prestação de serviços técnicos especializados de segurança (CJF n. 010/2015) com a empresa ISH, que dentre os serviços prestados, inclui serviços de sustentação das soluções de segurança do CJF, monitoramento de serviços e o tratamento de incidentes de segurança do Conselho de Justiça Federal – CJF. Observando o princípio da segregação de funções, previsto na Norma NBR ISO/IEC 27002:2005, este contrato implantou um novo um novo modelo de gestão de segurança da informação. Tal modelo buscou reduzir a possibilidade de uma “única pessoa (ou empresa) acessar, modificar ou usar ativos sem a devida autorização ou detecção”, segregando a sustentação de segurança da sustentação dos demais serviços que infraestrutura. Tal princípio reduziu os riscos de modificações acidentais ou deliberadas que impactem na segurança de ativos críticos, assegurando que a sustentação dos produtos de segurança não fique a cargo, por exemplo, de uma mesma empresa, que na ânsia de atender um nível de serviço de infraestrutura pode acabar não observando as melhores práticas de segurança da informação. Desta forma, é fundamental cumprir esta diretriz e manter os serviços gerenciados de segurança por meio da contratação, em separado, dos serviços de sustentação à segurança da informação dos serviços de operação do ambiente de infraestrutura.

Ademais, o CJF tem buscado constantemente a evolução da Segurança da Informação, aprimorando a Governança, Gestão e Operação de Segurança, por meio da atualização da Política de Segurança Informação - PSI, da normatização dos documentos acessórios da Política de Segurança da Informação, pela constante revisão das soluções de gerenciamento de ameaças - UTM, de firewall de aplicações web – WAF, de proteção de endpoint, de datacenter, de serviço de e-mail e pela utilização de ferramentas de detecção de novas ameaças.

No entanto, considerando a importância vital que os sistemas e serviços de TI adquiriram para as organizações e que se observa a constante diversificação e desenvolvimento de novas ameaças cibernéticas, são mandatórios a constante evolução, o aprimoramento dos mecanismos de segurança, bem como o desenvolvimento de equipes e de métodos de segurança cada vez mais complexos. Portanto, verifica-se que o atual modelo de contratações, por meio da compra de produtos e contratação de serviços de operação, não é suficiente para fazer frente à velocidade com surgem novos tipos de ameaças, e principalmente a velocidade com que o mercado de segurança evolui e lança novos produtos. Para endereçar tais desafios desenvolveu-se internacionalmente (Gartner) o conceito de *Managed Security Services* – MSS. Neste modelo empresas especialistas de segurança,



PODER JUDICIÁRIO
CONSELHO DA JUSTIÇA FEDERAL

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.

Ademais, é primordial aprimorar a atuação preventiva, elevar o grau de detecção de comportamentos anômalos e desenvolver o processo de gestão de incidentes de segurança, agilizar a resposta a incidentes de segurança e melhorar a percepção de segurança perante os usuários do CJF e a sociedade. Estes objetivos serão perseguidos nesta contratação pela criação e revisão dos níveis de serviço, para que estes estejam condizentes com a importância que a segurança da informação possui para a instituição.

Neste sentido, foram incluídos no escopo da contratação os seguintes serviços com os seus respectivos objetivos:

- 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 íntegro.
- 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.
- 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.
- 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



PODER JUDICIÁRIO
CONSELHO DA JUSTIÇA FEDERAL

analisados, podendo estes serem transformados em um incidente de segurança da informação.

- Serviço de orquestração, automação e resposta de segurança (SOAR), com o objetivo de automatizar os processos e fluxos de trabalho, a aplicação de atividades rotineiras ou de difícil execução e a orquestração das diversas ferramentas de segurança, sem necessidade de atuação humana.
- 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.

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 pelo DL 200/67, em seu Art. 10, par. 7º, quando determina que “A execução das atividades da Administração Pública Federal deverá ser amplamente descentralizada,” de forma a permitir ao servidor “[...] para melhor desempenhar das tarefas de planejamento, coordenação, supervisão e controle e com o objetivo de impedir o crescimento desmesurado da máquina administrativa, a Administração procurará desobrigar-se da realização material de tarefas executivas, recorrendo, sempre que possível, à execução indireta, mediante contrato, desde que exista, na área, iniciativa privada suficientemente desenvolvida e capacitada a desempenhar os encargos de execução”.

Para a nova contratação, ficou definida a vigência inicial de 24 (vinte e quatro) meses, contados a partir do início da prestação dos serviços, podendo ser prorrogado até o limite de 60 (sessenta) meses.

Este prazo foi definido em estrito cumprimento ao inciso II do art. 57 da Lei nº 8.666/93, que determina que a prestação de serviços a serem executados de forma contínua, poderão ter a sua duração prorrogada por iguais e sucessivos períodos com vistas à obtenção de preços e condições mais vantajosas para a administração, limitada a sessenta meses.

Um fator ponderado é que diante da complexidade do ambiente computacional do CJF devido à grande diversidade de tecnologias integradas, e dada a criticidade dos sistemas e serviços de TI para o funcionamento do CJF, existe um tempo razoável de



PODER JUDICIÁRIO
CONSELHO DA JUSTIÇA FEDERAL

absorção dos conhecimentos pela empresa prestadora no início da prestação dos serviços, bem como também é demandado um tempo de preparação para a desativação e transição dos serviços para outro contrato. Desta forma, caso a vigência fosse menor, tão logo se estabilizasse o serviço, já deveria ser dispendido tempo para as ações de encerramento e a transição, o que poderia gerar perturbação e intercorrências no ambiente computacional do CJF.

Esta Subsecretaria tem por competência buscar a segurança do ambiente tecnológico que atende ao Conselho, prestar serviço de atendimento as demandas das demais áreas da TI, bem como desenvolver as atividades de gestão, inovação e absorção de soluções de segurança de TI, provendo a devida proteção do parque de TI. Esta unidade é responsável ainda pela gestão de segurança, avaliação das atividades de outras unidades no que tange à segurança de TI, proposição de políticas e normativos de segurança, apoiar o Comitê de Segurança Informação da Justiça Federal – CSI-Jus, apoiar o Comitê de Resposta a Incidentes de Segurança da Informação da Justiça Federal – CRI-JUS, ambos com atuação nacional, apoiar à Comissão Local de Segurança da Informação – CLSI-CJF e coordenar a Comissão Local de Resposta a Incidentes de Segurança da Informação – CLRI-CJF.

Por outro lado, o volume das atribuições conferidas à SUSTI é flagrantemente desproporcional ao quadro de servidores da subsecretaria. Para suprir esse déficit operacional é necessária a terceirização dos serviços operacionais, permanecendo sob responsabilidade do quadro de servidores, apenas as funções de gestão e de planejamento, intransferíveis para empresas terceirizadas.

Considerando que não há concursos públicos vigentes do Poder Judiciário para a especialidade de segurança da informação, mesmo que recebêssemos novos servidores de TI, demandaria um longo período de capacitação, para que estes se tornassem especialistas na área de segurança informação. Ademais, 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. O que atualmente não é permitido no âmbito do órgão.

Cabe ressaltar que todos os serviços serão solicitados sob demanda, mediante emissão de Ordem de Serviço, conforme disponibilidade orçamentária, e poderão ser suspensos no futuro, caso tenhamos novos servidores de TI qualificados e em número suficiente para a sustentação das soluções de segurança. Além disso, esta contratação prevê, em alguns casos, o fornecimento de serviços na modalidade “Software as a Service – SaaS”, onde o software necessário para a proteção do ambiente é fornecido e operado pela empresa, que garantirá a aplicação contínua das melhores práticas. Tal modelo evidencia-se mais efetivo e possibilita a utilização de produtos de segurança por um menor custo, haja vista a possibilidade de utilização



PODER JUDICIÁRIO
CONSELHO DA JUSTIÇA FEDERAL

de licenças mais baratas, por serem compradas em grande quantidade pelo fornecedor para atender a diversos clientes. Neste caso, a quantidade de servidores não interfere na contratação.

Portanto, considerando a importância dos serviços de segurança de TI para a proteção dos diversos serviços e sistemas do CJF, aliado à inexistência de profissionais especializados nos quadros do CJF, em quantitativo e qualificação necessários ao atendimento dessa demanda, torna-se essencial para a adequada proteção do ambiente tecnológico a contratação de serviços gerenciados de segurança da informação.

Do alinhamento estratégico:

Esta contratação está alinhada aos objetivos estratégicos traçados no Plano Estratégico de Tecnologia da Informação da Justiça Federal (PETI-JF 2015/2020) e metas definidas no Plano Diretor de Tecnologia da Informação do CJF (PDTI 2018-2020) conforme apresentado a seguir:

Conforme PETI-JF 2015/2020, essa contratação está alinhada ao Macrodesafio do Poder Judiciário “Melhoria da Infraestrutura e governança de TIC” e com os seguintes temas estratégicos:

Objetivos estratégicos:

- Assegurar efetividade dos serviços de TI para a Justiça Federal;
- Aperfeiçoar a governança de TI na Justiça Federal;
- Assegurar a atuação sistêmica da TI na Justiça Federal.

Missão:

- Garantir soluções tecnológicas efetivas para o cumprimento da função institucional da Justiça Federal.

Visão:

- Consolidar-se como área estratégica da Justiça Federal e ser reconhecida pela excelência e inovação de suas soluções.

Conforme PDTI-CJF 2018/2020, essa contratação está alinhada às seguintes diretrizes e iniciativas estratégicas:

Diretrizes:

- Padrões metodológicos para o desenvolvimento de softwares, gestão de projetos e governança de TI dentre outros;



PODER JUDICIÁRIO
CONSELHO DA JUSTIÇA FEDERAL

- Economicidade, uniformidade, compatibilidade e interoperabilidade mediante a adoção de procedimentos comuns e colaborativos entre os órgãos integrantes do Sistema de Tecnologia da Informação da Justiça Federal - SIJUS, para aquisição e instalação de hardwares e redes de comunicação de dados, desenvolvimento e instalação de softwares e quaisquer outras ações de TI;
- Inovar na busca de soluções visando racionalizar o uso de recursos orçamentários, otimizar esforços e maximizar a entrega de sistemas e serviços;
- Política de investimentos em relação aos hardwares, redes de comunicação de dados e softwares, observada a segurança da informação, a uniformidade, a compatibilidade e a interoperabilidade em toda a Justiça Federal.

Iniciativas:

- Prover solução de gerenciamento de infraestrutura de TI;
- Modernizar e nivelar a infraestrutura de TI.

Fundamentação Legal

O presente Termo de Referência foi elaborado em conformidade com os seguintes regramentos:

- Lei no 8.666, de 21 de julho de 1993, como peça integrante e indissociável de um processo licitatório;
- Decreto Lei no. 200, de 25 de fevereiro de 1967;
- Lei no 10.520, de 17 de julho de 2002, que instituiu a modalidade de pregão para aquisição de bens e serviços comuns;
- Decreto no 3.555, de 08 de agosto de 2000;
- Decreto no 10.024, de 20 de setembro de 2019, pela regulamentação do sistema de pregão para bens e serviços comuns;
- Instrução Normativa CJF-INN-2016/00001 do Conselho da Justiça Federal;
- Resolução no 169, de 31 de janeiro de 2013 do Conselho Nacional de Justiça;
- Resolução n. 182, de 17 de outubro de 2013, que dispõe sobre diretrizes para as contratações de Solução de Tecnologia da Informação pelos órgãos do Poder Judiciário;
- Instrução Normativa n. 07, de 20 de setembro de 2018, altera a IN n. 05/2017, que dispõe sobre as regras e diretrizes do procedimento de contratação de serviços sob o regime de execução indireta no âmbito da Administração Pública federal direta, autárquica e fundacional; Determinações do TCU como do Acórdão no. 667/2005, quanto à insuficiência de servidores do quadro para execução dos serviços;



PODER JUDICIÁRIO
CONSELHO DA JUSTIÇA FEDERAL

- Manual de Contratação de Serviços de Tecnologia da Informação da Justiça Federal – MCTI-JF v2.0.

Do Serviço Comum

O objeto da presente contratação pode ser objetivamente especificado por meio de padrões usuais de mercado. Desta forma, entendemos que o objeto pode ser classificado como serviço comum, para fins do disposto no parágrafo único, art. 1º da Lei 10.520, de 17 de julho de 2002, podendo, portanto, ser contratado por meio de processo licitatório na modalidade pregão, preferencialmente na forma eletrônica. Os serviços aqui tratados possuem natureza de serviço comum para fins do disposto no Art. 4º do Decreto nº 10.024/2019.

Benefícios Diretos e Indiretos que Resultarão da Contratação

O CJF espera obter os seguintes benefícios e resultados:

- Assegurar os níveis de serviço adequados ao CJF no tocante a Segurança da Tecnologia da Informação;
- Aumento do grau de satisfação dos usuários com os produtos e serviços fornecidos pela área de SI;
- Redução dos riscos de interrupção dos serviços e sistemas em decorrência de ataques cibernéticos;
- Melhoria da entrega dos serviços de SI aos usuários em decorrência da utilização de boas práticas dos processos de gerenciamento de serviços de TI;
- Implantar processo estruturado e instrumentalizado de gerenciamento de incidentes de segurança da informação, em que as etapas de triagem, classificação, análise, resposta e comunicação sigam as melhores práticas de internacionais;
- Criar bases históricas e estatísticas de incidentes, permitindo traçar tendências ou pontos que necessitam de aprimoramento;
- Permitir a análise crítica dos logs de segurança de forma automatizada, tendo em vista a incapacidade humana de visualizar todas as centenas de eventos de segurança que ocorrem a cada segundo e em diferentes soluções;
- Implantar processo de análise de lacunas de segurança (gap analysis) utilizando as mais modernas metodologias utilizadas internacionalmente;
- Responder mais rapidamente aos ataques cibernéticos;
- Possuir capacidade de identificação preventiva de ameaças emergentes e de eventuais vazamentos antes da divulgação pública;



PODER JUDICIÁRIO
CONSELHO DA JUSTIÇA FEDERAL

- Redução do tempo de restauração da operação normal dos serviços com o mínimo de impacto nos processos de negócios da CONTRATANTE, dentro dos Níveis Mínimos de Serviço (NMS) e prioridades acordados;
- Melhoria da percepção do adequado gerenciamento de segurança de SI por parte da alta administração e dos usuários internos e externos, deixando transparente que há efetivo gerenciamento dos incidentes de segurança de tecnologia da informação;
- Melhoria da disseminação de informações relacionadas à Segurança da Informação nos diversos níveis organizacionais;
- Definição clara dos objetivos, produtos, prazos, custos, padrões de qualidade, responsabilidades das partes, além de indicadores de desempenho;
- Incremento de qualidade no tratamento dos eventos de segurança;
- Melhoria na identificação e tratamento de vulnerabilidades de segurança do ambiente de TI;
- Investir no desenvolvimento de processos de trabalho seguros, ao invés de apenas investir em tecnologia;
- Desenvolver resiliência e melhorar a capacidade da TI de enfrentar eventos adversos relacionados a cibersegurança.

Dos Critérios de Agrupamento de Itens em Lote Único

Um ponto fundamental para se garantir a viabilidade técnico-administrativa de tal aquisição é o de que o conjunto dos serviços gerenciados de segurança sejam licitados em lote único, portanto com adjudicação para um único licitante vencedor. Os principais balizadores desta definição estão descritos a seguir:

- A definição pela contratação dos serviços em lote único levou em consideração o prejuízo de ordem técnica que poderiam ocorrer casos os serviços fossem prestados por diferentes empresas, uma vez que os serviços a serem contratados guardam estreita relação entre si e dependem de forte integração para sejam efetivos e alcancem os resultados pretendidos com a contratação.
- O agrupamento de itens em um único lote, na realização dos pregões eletrônicos, é orientação constante do Acórdão nº 861/2013 - Plenário, do Tribunal de Contas da União: "São lícitos os agrupamentos em lotes de itens a serem adquiridos por meio de pregão, desde que possuam mesma natureza e que guardem relação entre si".
- Destaca-se que a contratação de forma global, garante tanto a unicidade dos processos, aferição dos níveis de serviços, como a otimização dos recursos necessários à gerência e fiscalização do contrato.
- A contratação global também evita o risco de contratações conflituosas entre si, pois os serviços especificados dependem também do fornecimento de



PODER JUDICIÁRIO
CONSELHO DA JUSTIÇA FEDERAL

equipamentos e softwares que necessitarão de total integração, evitando-se que os produtos apresentem problemas de incompatibilidade.

- As contratações em separado apresentariam também o alto risco de ocorrer, no decorrer da vigência do contrato, situações de “empura-empurra”. Em que as contratadas atribuam culpa a terceiros por descumprimentos de suas responsabilidades.
- As equipes de ataque (RED TEAM) e defesa (BLUE TEAM) devem interagir e funcionar de maneira integrada. A equipe de ataque deve compartilhar seu conhecimento no sentido de indicar soluções para vulnerabilidades encontradas e a equipe de defesa deve possuir conhecimento das táticas e técnicas de ataque para que, por meio da atuação conjunta (PURPLE TEAM), aumente-se a efetividade da proteção do ambiente. Considerando a possibilidade de contratação dos serviços em separado, conforme disponibilidade orçamentária e consequente emissão de Ordem de Serviço, os serviços foram nomeados em separado, no entanto, objetiva-se que, quando os dois serviços forem demandados, as equipes RED TEAM e BLUE TEAM atuem integradas, tornando-se de fato em uma equipe PURPLE TEAM.

Motivação do Registro de Preço

A adoção do Sistema de Registro de Preços é justificada com base no art. 3º do Decreto nº 7.892/13, em seus incisos I e II. A parte final do inciso I alude ao cabimento de Registro de Preços quando houver necessidade de contratações frequentes. Já o inciso II trata da hipótese de cabimento do Registro de Preço quando for conveniente a contratação de serviços remunerados em regime de tarefa.

Considerando que o objeto da contratação se trata de Serviços Gerenciados de Segurança da Informação, constituído por 06 grandes serviços, torna-se impossível definir previamente o volume de serviços a ser demandado. Desta forma, entende-se haver plena compatibilidade entre tais fatos e as hipóteses previstas no art. 3º do Decreto nº 7.892/13, que regulamenta o Sistema de Registro de Preços, previsto no art. 15 da Lei nº 8.666/1993.

4. OBRIGAÇÕES DA CONTRATADA

Para fins de execução do contrato, a CONTRATADA deverá observar os seguintes requisitos:

REQUISITOS INTERNOS



PODER JUDICIÁRIO
CONSELHO DA JUSTIÇA FEDERAL

- 4.1** A CONTRATADA deverá atender aos Níveis Mínimos de Serviço estabelecidos pelos indicadores contidos no Anexo I deste Termo de Referência;
- 4.2** Excepcionalmente, os serviços poderão ser executados nas dependências da Gráfica, nos casos em que o CJF entender como conveniente;
- 4.3** Cumprir os normativos e os procedimentos definidos pelo CONTRATANTE;
- 4.4** Deverá primar pelo bom planejamento das atividades, utilizar as boas práticas técnicas e de governança, avaliar previamente a viabilidade técnica, os riscos e os impactos de suas ações, planejar e documentar adequadamente as mudanças de configuração dos ativos de Segurança da Informação – SI;
- 4.5** Criar documentação técnica, operacional e de análise e controle, execução de rotinas pró-ativas e reativas, análise de desempenho, monitoramento e operação dos serviços;
- 4.6** Efetuar a transferência de conhecimento para a equipe técnica do CONTRATANTE, de todos os novos serviços implantados ou modificados, mediante documentação técnica em repositório adotado pelo CJF para esse fim;
- 4.7** Executar todos os serviços, tarefas e atividades demandadas pelo CONTRATANTE dentro do prazo contratado, atendendo o padrão de qualidade exigido;
- 4.8** Apresentar no 1º (primeiro) dia útil de cada mês a relação dos profissionais que prestarão os serviços no mês corrente;
- 4.9** Formalizar ao CONTRATANTE a substituição de profissional, antes de sua efetiva substituição;
- 4.10** É admissível a fusão, cisão ou incorporação da contratada com/em outra pessoa jurídica, desde que sejam observados pela nova pessoa jurídica todos os requisitos de habilitação exigidos na licitação original; sejam mantidas as demais cláusulas e condições do contrato; não haja prejuízo à execução do objeto pactuado e haja a anuência expressa da Administração à continuidade do contrato;
- 4.11** Os serviços deverão ser realizadas em conformidade com os horários e períodos determinados pelo CONTRATANTE;
- 4.12** As atividades que não possuam rotinas e procedimentos definidos deverão ser documentados após a sua realização como condição para a aceitação do serviço;
- 4.13** Elaborar relatório gerencial de serviços, apresentando-o ao CONTRATANTE, até o terceiro dia útil do mês subsequente ao da prestação dos serviços, devendo constar dentre outras informações:



PODER JUDICIÁRIO
CONSELHO DA JUSTIÇA FEDERAL

- 4.13.1** Os indicadores e níveis de serviços alcançados em relação ao previsto no Anexo I deste Termo de Referência;
 - 4.13.2** Relatório de análise e diagnóstico das causas (causa raiz) dos incidentes e problemas ocorridos;
 - 4.13.3** Manutenções evolutivas e corretivas realizadas;
 - 4.13.4** Erros operacionais;
 - 4.13.5** Sugestões de melhorias;
 - 4.13.6** Painel de volumetria de chamados (requisições de serviço, incidentes, problemas etc.) divididos por grupos solucionadores e responsáveis, demonstrando graficamente a evolução destas informações;
 - 4.13.7** Indicadores de aferição da qualidade de novos produtos e/ou serviços que venham a ser implantados no decorrer da vigência contratual;
 - 4.13.8** Demais informações relevantes para as atividades demandadas nas Ordens de Serviços.
 - 4.13.9** Estatísticas de tratamento de e-mails suspeitos, *spam* etc.;
 - 4.13.10** Estatísticas de tratamento de *malware* (vírus, *worms*, *trojan horses*, *spyware* etc.);
 - 4.13.11** Relatório de resultados obtidos em testes de invasão;
 - 4.13.12** Relatório de vulnerabilidades de segurança nos sistemas de informação, aplicativos e serviços de TI;
 - 4.13.13** Sugestões de mitigação das vulnerabilidades de segurança encontradas;
 - 4.13.14** Eventos de segurança;
 - 4.13.15** Ações tomadas em reação aos eventos de segurança;
 - 4.13.16** Sugestões de mitigação de riscos.
- 4.14** Submeter seus profissionais aos regulamentos de segurança e disciplina instituídos pelo CONTRATANTE, durante o tempo de permanência nas suas dependências;
- 4.15** Responsabilizar-se por solicitar o credenciamento e descredenciamento de acesso físico e lógico às dependências do CONTRATANTE bem como assumir quaisquer prejuízos porventura causados por seus profissionais;
- 4.16** Promover o afastamento, no prazo máximo de 24 (vinte e quatro) horas, após a notificação de que qualquer dos seus profissionais que não estejam realizando



PODER JUDICIÁRIO
CONSELHO DA JUSTIÇA FEDERAL

as atividades com a devida competência técnica e/ou postura profissional exigidos para a prestação dos serviços no CONTRATANTE;

- 4.17** Os serviços deverão ser prestados de forma ininterrupta, portanto o afastamento mencionado no subitem 4.16 não poderá prejudicar a qualidade dos serviços e nem descumprir quaisquer cláusulas contratuais;
- 4.18** Comunicar às unidades do CONTRATANTE responsáveis pela fiscalização do contrato, por escrito, qualquer anormalidade, bem como atender prontamente o que lhe for solicitado e exigido;
- 4.19** Manter um Diário de Ocorrências que conste nos registros as eventuais ocorrências diárias relativas à execução dos trabalhos;
- 4.20** Selecionar e treinar adequadamente os profissionais alocados para prestação dos serviços, observando a boa conduta e a idoneidade moral destes;
- 4.21** Manter os seus profissionais atualizados tecnologicamente, promovendo treinamentos e participação em eventos de caráter técnico que permitam a boa execução dos serviços, sem qualquer ônus para o CONTRATANTE, com carga horária mínima de 20 (vinte) horas anuais. O CONTRATANTE poderá indicar áreas de conhecimento em que os serviços necessitem de aperfeiçoamento;
- 4.22** Manter os seus profissionais qualificados nas ferramentas, metodologias, processos e tecnologias utilizados pelo CONTRATANTE durante toda a vigência do contrato;
- 4.23** Durante toda a vigência do contrato, os serviços deverão ser realizados por profissionais com as competências e certificações exigidas nas descrições dos serviços, bem como capacitados nas tecnologias que eventualmente venham a ser utilizadas durante sua execução. Tal qualificação sempre que exigida pelo CJF, deverá ser comprovada por currículos e certificados oficiais;
- 4.24** A seleção, a designação e a manutenção do quadro de profissionais alocados ao contrato são de exclusiva responsabilidade da CONTRATADA;
- 4.25** Fiscalizar regularmente os seus profissionais designados para a prestação dos serviços verificando as condições em que as atividades estão sendo realizadas;
- 4.26** Refazer todos os serviços que, a juízo do representante do CONTRATANTE, não forem considerados satisfatórios, sem que caiba qualquer acréscimo no custo contratado, independentemente das penalidades previstas neste Termo de Referência;



PODER JUDICIÁRIO
CONSELHO DA JUSTIÇA FEDERAL

- 4.27** A CONTRATADA e seus profissionais deverão assinar o Termo de Responsabilidade conforme modelo Anexo IV e manter em caráter confidencial, mesmo após o término do prazo de vigência ou rescisão do contrato, as informações relativas:
- 4.27.1** As políticas e procedimentos de segurança da informação adotados pelo CONTRATANTE;
 - 4.27.2** As configurações de hardwares, de softwares, produtos, ferramentas e equipamentos;
 - 4.27.3** Aos processos internos do CONTRATANTE;
 - 4.27.4** As vulnerabilidades dos ativos de informação do CJF;
 - 4.27.5** Mecanismos de criptografia e autenticação.
- 4.28** A CONTRATADA e seus profissionais que prestarão os serviços deverão assinar o Termo de Responsabilidade e se responsabilizar pelos atos de seus profissionais que estiverem prestando serviço no CONTRATANTE, conforme modelo do Anexo IV;
- 4.29** Acatar as determinações feitas pela fiscalização do CONTRATANTE no que tange ao cumprimento do objeto deste contrato;
- 4.30** Prestar, de imediato, todos os esclarecimentos solicitados pela fiscalização do CONTRATANTE no que diz respeito a execução do objeto contratado;
- 4.31** Responder por escrito, no prazo máximo de 48 (quarenta e oito) horas, a quaisquer esclarecimentos de ordem técnica pertinentes à execução dos serviços que venham porventura a ser solicitados pelo CONTRATANTE;
- 4.32** Permitir auditoria pelo CONTRATANTE, ou terceiro por ela designado, inclusive com a possibilidade dos atendimentos serem monitorados para verificação de procedimentos;
- 4.33** A CONTRATADA deverá seguir as melhores práticas preconizadas pelo *framework* ITIL v3, garantindo a aplicação dos processos de Gerenciamento da Configuração e de Ativo de Serviço, Gerenciamento de Requisição, Gerenciamento de Incidente, Gerenciamento de Problema, Gerenciamento de Mudança, Gerenciamento do Conhecimento e o Gerenciamento de Níveis de Serviço, Gerenciamento da Disponibilidade, Gerenciamento do Catálogo de Serviço e o Gerenciamento de liberação e Implantação, garantindo a manutenção de uma base de dados de configuração e mudanças;
- 4.34** A realização dos processos ITIL significa seguir os processos descritos naquela metodologia, manter equipe capacitada para aplicar os conceitos, utilizar as



PODER JUDICIÁRIO
CONSELHO DA JUSTIÇA FEDERAL

ferramentas que implementem o ITIL e gerar relatórios com as informações pertinentes à metodologia;

- 4.35** É de responsabilidade da CONTRATADA manter atualizada a Base de Dados de Gerenciamento de Configuração dos ativos que fazem parte do objeto do seu contrato;
- 4.36** Participar, dentro do período compreendido entre a assinatura do contrato e o início da prestação dos serviços, de reunião de alinhamento de expectativas contratuais com uma equipe de técnicos da STI;
- 4.37** Indicar formalmente, quando da assinatura do contrato, PREPOSTO que tenha capacidade gerencial para tratar de todos os assuntos previstos no instrumento contratual e coordenação da equipe para a execução dos serviços contratados. O preposto deverá, entre outras atividades, promover os contatos com o gestor do contrato bem como deverá prestar atendimento aos profissionais em serviço, tais como:
- 4.37.1** Executar os procedimentos administrativos referentes aos profissionais alocados para execução dos serviços contratados, tais como: entregar-lhes contracheques, auxílio-transporte e auxílio-alimentação, acompanhar e controlar a apuração do ponto;
 - 4.37.2** Assegurar de que as determinações do CJF sejam disseminadas junto aos profissionais alocados com vistas à execução dos serviços contratados;
 - 4.37.3** Informar ao gestor do contrato sobre problemas de qualquer natureza que possam impedir o bom andamento dos serviços contratados;
 - 4.37.4** Desenvolver outras atividades administrativas de responsabilidade da CONTRATADA, principalmente quanto ao controle de informações relativas ao seu faturamento mensal e apresentação de documentos quando solicitado;
 - 4.37.5** O preposto não poderá ser contabilizado como profissional para execução dos serviços contratados.
 - 4.37.6** Após a assinatura do contrato, conhecer o parque tecnológico e as atividades em andamento, visando à preparação da equipe que irá prestar os serviços, conhecer os modelos de serviços realizados, as normas internas, procedimentos de segurança e a definição dos requisitos necessários;
 - 4.37.7** Deverá estar disponível, de segunda a sexta-feira, das 09 (nove) às 19 (dezenove) horas, e acessível por contato telefônico em qualquer outro horário;



PODER JUDICIÁRIO
CONSELHO DA JUSTIÇA FEDERAL

- 4.37.8** A CONTRATADA deverá indicar um substituto eventual para substituir o PREPOSTO nos casos de afastamento imprevisto, tais como por motivo de saúde, limitado a 5 (cinco) dias corridos;
- 4.37.9** A CONTRATADA deverá indicar um substituto com, no mínimo 10 (dez) dias corridos de antecedência, nos casos previsíveis de ausência do PREPOSTO, tais como por férias, treinamentos etc.;
- 4.38** Os profissionais deverão atender as exigências de vestimenta feitas aos servidores do CJF e portar crachá de identificação durante toda a prestação do serviço;
- 4.39** A CONTRATADA deverá manter o serviço de suporte técnico das soluções ofertadas com a finalidade de garantir a plena utilização dos produtos durante toda a vigência do contrato;
- 4.40** A CONTRATADA será responsável pelos serviços de implantação das novas versões, patches, releases, e service packs relativos a esses produtos de segurança utilizados no ambiente. Quando houver contrato de suporte técnico com terceiro, deverá ser aberto chamado de suporte técnico para a execução coordenada destes serviços;
- 4.41** A CONTRATADA deverá auxiliar o CONTRATANTE na comunicação junto aos fabricantes dos produtos utilizados pelo CONTRATANTE;

REQUISITOS EXTERNOS

- 4.42** Manter sigilo, sob pena de responsabilidade civil, penal e administrativa, sobre todo e qualquer assunto de interesse do CONTRATANTE ou de terceiros de que tomar conhecimento em razão da execução do objeto deste contrato, devendo orientar seus profissionais nesse sentido; Observar o cumprimento das normas relacionadas com a segurança e higiene no trabalho;
- 4.43** Responsabilizar-se pela manutenção da limpeza e conservação dos ambientes onde desempenhe seus serviços;
- 4.44** Responsabilizar-se pelos materiais, produtos, ferramentas e equipamentos disponibilizados para a execução dos serviços, inclusive por perdas decorrentes de roubo, furto ou outros fatos que possam vir a ocorrer;
- 4.45** Prestar os serviços dentro dos parâmetros e rotinas estabelecidos pelo CONTRATANTE, com observância às recomendações aceitas pela boa técnica, normas e legislação, bem como observar conduta adequada na utilização dos materiais, equipamentos, ferramentas e utensílios;



PODER JUDICIÁRIO
CONSELHO DA JUSTIÇA FEDERAL

- 4.46** Responsabilizar-se por danos causados ao patrimônio do CONTRATANTE, ou de terceiros, ocasionados por seus profissionais, em virtude de dolo ou culpa, durante a execução do objeto contratado;
- 4.47** Manter durante todo o período de vigência do ajuste todas as condições, inclusive de habilitação, que ensejaram sua contratação;
- 4.48** Prestar os serviços de forma ininterrupta, em conformidade com o demandado pelas Ordens de Serviço;
- 4.49** Assumir todas as despesas relativas à execução dos serviços, tais como taxas, emolumentos, encargos sociais;
- 4.50** Arcar com as despesas decorrentes de qualquer infração cometida por seus profissionais, inclusive com as glosas previstas, quando da execução dos serviços especificados nas Ordens de Serviço;
- 4.51** Responder por todo e qualquer dano ou prejuízo eventualmente causado ao CONTRATANTE como consequência de atos e fatos imputáveis a seus profissionais;
- 4.52** Cumprir às suas próprias expensas todas as cláusulas contratuais que definam suas obrigações;
- 4.53** A CONTRATADA e seus profissionais que prestarão os serviços deverão assinar declaração de não nepotismo, conforme modelo do Anexo IV;
- 4.54** Responsabilizar-se por todos os encargos previdenciários e obrigações sociais previstas na legislação social e trabalhista em vigor, obrigando-se a saldá-las na época própria, vez que os seus profissionais não manterão nenhum vínculo empregatício com o CONTRATANTE;
- 4.55** Responsabilizar-se por todas as providências e obrigações estabelecidas na legislação específica de acidentes de trabalho, quando, em ocorrência da espécie, forem vítimas os seus profissionais durante a execução deste contrato, ainda que acontecido em dependência do CONTRATANTE;
- 4.56** Responsabilizar-se por todos os encargos de possível demanda trabalhista, civil ou penal, relacionada à execução deste contrato, originariamente ou vinculada por prevenção, conexão ou continência;
- 4.57** Responsabilizar-se por todos os encargos fiscais e comerciais resultantes desta contratação;
- 4.58** Responsabilizar-se pelo pagamento de eventuais multas aplicadas por quaisquer autoridades federais, estaduais e municipais, em consequência de fato a ela imputável e relacionada com a execução do objeto do contrato;



PODER JUDICIÁRIO
CONSELHO DA JUSTIÇA FEDERAL

- 4.59** Responsabilizar-se por todos os prejuízos advindos de perdas e danos, incluindo despesas judiciais e honorários advocatícios, resultantes de ações judiciais a que o CONTRATANTE for compelido a responder por força desta contratação.

5. OBRIGAÇÕES DO CONTRATANTE

- 5.1** O CJF deverá nomear um gestor e equipe de fiscais técnicos para acompanhar a execução do contrato, que se tornará responsável pelo fiel cumprimento do mesmo e seus elementos integrantes;
- 5.2** Suas obrigações são receber e atestar as notas fiscais de faturamento dos serviços prestados, bem como, verificar a qualidade dos serviços por meio de relatórios que comprovem o cumprimento dos níveis mínimos de serviço estabelecidos. O gestor será também responsável por encaminhar as notas fiscais para pagamento segundo os procedimentos internos do CJF;
- 5.3** O CJF deverá nomear um Fiscal Administrativo do contrato que irá fiscalizar periodicamente os recolhimentos do FGTS, por empregado, o fornecimento de vale transporte e auxílio alimentação, o pagamento de 13º salário, a concessão de férias e o correspondente pagamento do adicional de 1/3, a realização de exames admissionais e demissionais e periódicos, os eventuais cursos de treinamento e reciclagem, a comprovação de encaminhamento ao Ministério do Trabalho e Emprego da RAIS e CAGED, do cumprimento das convenções, acordos e dissídios coletivos, e do efetivo pagamento dos valores salariais lançados na proposta da CONTRATADA, mediante a verificação das folhas de pagamento referentes aos meses de realização dos serviços, de cópias de carteiras de trabalho dos empregados, dos recibos e dos respectivos documentos bancários, entre outros meios de fiscalização cabíveis;
- 5.4** Solicitar a substituição do profissional que tenha infringido às normas do CJF, ainda que em parte, dos itens indicados no item 4 - "Obrigações da CONTRATADA";
- 5.5** Permitir acesso dos prestadores de serviço da CONTRATADA às suas dependências, aos equipamentos, softwares e sistemas de informação para a execução dos serviços contratados;
- 5.6** Prestar as informações e os esclarecimentos pertinentes que venham a ser solicitados pelos prestadores de serviço da CONTRATADA ou por seu preposto;
- 5.7** Efetuar o pagamento mensal devido pela execução dos serviços, desde que cumpridas as formalidades e exigências do contrato;
- 5.8** Exercer a fiscalização dos serviços prestados;



PODER JUDICIÁRIO
CONSELHO DA JUSTIÇA FEDERAL

- 5.9 Comunicar oficialmente à CONTRATADA, quaisquer falhas verificadas no cumprimento do contrato;
- 5.10 Avaliar mensalmente o relatório gerencial de serviços, observando os indicadores e metas de níveis de serviço alcançados;
- 5.11 Observar o cumprimento dos requisitos de qualificação profissional exigidos no edital e seus módulos, solicitando à CONTRATADA as substituições e os treinamentos que se verificarem necessários;
- 5.12 Fornecer as normas, rotinas, procedimentos e processos desenvolvidos pelo CJF para que a CONTRATADA promova os devidos ajustes e implementações adicionais;

6. DOS SERVIÇOS GERENCIADOS DE SEGURANÇA

- 6.1 O Serviço de Operação e Atendimento de Requisições deverá ser prestado no período das 09:00 às 22:00, de segunda-feira a sexta-feira, e **presencialmente**, nas dependências do CONTRATANTE (sede do CJF), das 13:00 às 21:00;
- 6.2 O Serviço de Gestão de Incidentes de Segurança deverá ser prestado em período integral (24x7) para o tratamento de incidentes de segurança da informação e **presencialmente**, nas dependências do CONTRATANTE (sede do CJF), em caso de ocorrência de grave incidente de segurança que implique em comprometimento de disponibilidade, integridade ou confidencialidade das informações do CJF;
- 6.3 A CONTRATADA, como parte da execução do Serviço de Operação e Atendimento de Requisições, deverá realizar, nos primeiros 60 (sessenta) dias de execução deste serviço, uma avaliação completa do ambiente do ambiente do contratante com o objetivo identificar lacunas ou oportunidades de melhoria (Gap Analysis) com o objetivo de avaliar a maturidade dos controles de segurança do CONTRATANTE.
 - 6.3.1 A análise dos controles de segurança deverá ser realizada 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.
 - 6.3.2 Esta análise deverá ser repetida anualmente durante a vigência do contrato.
 - 6.3.3 A análise deverá ser conduzida por profissional com certificação CISSP – Certified Information Systems Security, que será responsável pela



PODER JUDICIÁRIO
CONSELHO DA JUSTIÇA FEDERAL

apresentação dos resultados da análise ao gestor, fiscais do contrato e gestores de TI do CJF.

- 6.4** A CONTRATADA deverá seguir o processo de mudança estabelecido pelo CONTRATANTE. Sempre que solicitado, a CONTRATADA deverá estar disponível para participar das reuniões com o Comitê de Mudanças, para prestar informações sobre os ambientes e serviços por elas executados. Mudanças que impliquem em um conjunto de procedimentos complexos, que envolvam várias equipes ou empresas CONTRATADAS e que impliquem em riscos de paralisação de quaisquer serviços considerados prioritários, deverão ser tratadas como um Projeto. A CONTRATADA deverá apresentar ao Comitê de Mudanças do CJF a proposta de todas as mudanças no ambiente, conforme níveis de controle estabelecidos. Para todas as mudanças apresentadas, será necessário acompanhar dentre outras informações, as análises de risco relativas às mudanças, descrevendo o impacto da sua realização;
- 6.5** Fará parte do trabalho da CONTRATADA o teste e a emissão de parecer a respeito de qualquer novo Item de Configuração que suporte os serviços de segurança adotados pelo CJF, devendo emitir nota técnica avaliando os riscos deste novo IC para o ambiente tecnológico. Com base na nota técnica elaborada o CJF irá aprovar a Liberação do IC no ambiente. Se o processo de liberação do IC implicar em riscos de paralisação de quaisquer serviços considerados prioritários, deverá ser tratado como um Projeto;
- 6.6** A CONTRATADA deverá monitorar permanente e avaliar criticamente os serviços, traçando curvas de comportamento, definindo a volumetria média de acessos e identificando comportamentos não usuais, visando antecipar a identificação de incidentes de segurança, antes mesmo de impacto nos serviços;
- 6.7** As manutenções preventivas e/ou corretivas, que representem risco de interrupção do(s) serviço(s), deverão ser agendadas e realizadas fora do horário regular, salvo quando expressamente autorizado;
- 6.8** As manutenções programadas, que impliquem em extensiva parada do ambiente serão realizadas durante um final de semana. Tais atividades realizadas fora do horário regular não ensejarão qualquer pagamento adicional em relação ao estabelecido no contrato, portanto a CONTRATADA deverá prever esta situação em sua composição de custos;
- 6.9** Todos os serviços de manutenção corretiva e preventiva são considerados de natureza contínua e deverão minimizar a necessidade de parada do ambiente em produção;
- 6.10** Testar todos os serviços após a realização de manutenções preventivas e/ou corretivas, ficando sua aceitação final dependente da área demandante e/ou de



PODER JUDICIÁRIO
CONSELHO DA JUSTIÇA FEDERAL

fiscalização do CONTRATANTE, que avaliará as características esperadas para o serviço;

- 6.11** Todos os serviços deverão ser executados em conformidade com as rotinas, processos, procedimentos e preceitos do ITILv3 definidos pelo CONTRATANTE;
- 6.12** Monitorar o padrão de acessos ao ambiente e definir, com o aval do CONTRATANTE, os limites (*thresholds*) a partir do qual caracterizarão incidente de Segurança da Informação;
- 6.13** Os serviços deverão ser executados por profissionais habilitados, com base em programas de formação e/ ou certificações oficiais, conforme os requisitos específicos para o perfil profissional;
- 6.14** A CONTRATADA deverá produzir mensalmente informações a cerca da utilização e capacidade dos itens de configuração - IC que façam parte de seus serviços e o desempenho destes quando do cumprimento de níveis de serviço;
- 6.15** As equipes de ataque (RED TEAM) e defesa (BLUE TEAM) devem interagir e funcionar de maneira integrada. A equipe de ataque deve compartilhar seu conhecimento no sentido de indicar soluções para vulnerabilidades encontradas e a equipe de defesa deve possuir conhecimento das táticas e técnicas de ataque para que, por meio da atuação conjunta (PURPLE TEAM), aumente-se a efetividade da proteção do ambiente.
- 6.16** A CONTRATADA deverá elaborar e manter atualizados os Planos de Capacidade, de Gerenciamento de Incidentes, de Disponibilidade, de Continuidade e de Recuperação de Desastres para os serviços objeto deste Termo;
- 6.17** Será de responsabilidade da CONTRATADA o monitoramento constante dos acessos e dos IC's que suportem os serviços de segurança, gerando uma base histórica de monitoramento destes Itens;
- 6.18** A CONTRATADA deverá participar e colaborar com a manutenção/evolução dos seguintes processos do ITIL – Gerenciamento de Incidente, Cumprimento de Requisição, Gerenciamento de Problema, Gerenciamento da Configuração e de Ativo de Serviço, Gerenciamento de Mudança, Gerenciamento de Liberação e Implantação, Gerenciamento da Disponibilidade, Gerenciamento do Conhecimento, Gerenciamento de Níveis de Serviço, Gerenciamento do Catálogo de Serviço;
- 6.19** Os serviços devem ser executados de acordo com normas, procedimentos e técnicas adotadas pelo CJF;



PODER JUDICIÁRIO
CONSELHO DA JUSTIÇA FEDERAL

- 6.20** Deverá ser fornecido ao CONTRATANTE acesso à console dos produtos ofertados para que seja possível o acompanhamento, auditoria e direcionamento de ações no ambiente;
- 6.21** Os Serviços Gerenciados de Segurança que não forem presenciais, deverão ser prestados por meio de estrutura de SOC's - *Security Operation Center* redundantes, obrigatoriamente no Brasil. Um dos centros deverá ser provido em ambiente físico próprio da CONTRATADA e um segundo poderá provido em ambiente físico terceirizado, desde que os serviços sejam comprovadamente prestados por funcionários da empresa.
- 6.22** Os SOC's devem estar ativos e deverão atender aos seguintes requisitos mínimos:
- 6.22.1** Utilizar sistema de gerenciamento de CFTV, que viabilizem o rastreamento de pessoas dentro do ambiente da CONTRATADA e cujas imagens possam ser recuperadas;
 - 6.22.2** Filmar toda a área, mantendo as imagens armazenadas por no mínimo 90 (noventa) dias;
 - 6.22.3** Efetuar registro de entrada e saída dos visitantes, com identificação individual, em todos os acessos ao SOC por no mínimo 90 dias;
 - 6.22.4** Possuir solução de monitoramento de disponibilidade e desempenho;
 - 6.22.5** O perímetro deve protegido contra intrusão e acesso indevido;
 - 6.22.6** Ser vigiado de forma ininterrupta por segurança especializada em regime de 24x7x365;
 - 6.22.7** Ter controle de acesso físico com pelo menos 2 (dois) fatores de autenticação;
 - 6.22.8** Ser configurado de forma que a falha de um dos equipamentos isoladamente NÃO interrompa a prestação dos serviços;
 - 6.22.9** 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;
 - 6.22.10** Ter componentes de segurança necessários para garantir a preservação dos dados em casos de incêndio e execução de plano de recuperação de catástrofes;
 - 6.22.11** Deverá possuir processos implementados que garantam a segurança das informações do CONTRATANTE, em conformidade com a norma ABNT NBR ISO/IEC 27001.



PODER JUDICIÁRIO
CONSELHO DA JUSTIÇA FEDERAL

- 6.23** A CONTRATADA deverá fornecer link de comunicação dedicado cuja utilização não deverá ultrapassar 90% (noventa por cento) de sua capacidade. Podendo ser utilizado VPN via internet como redundância.
- 6.24** A CONTRATADA será responsável pela aplicação de controles de segurança adequados (criptografia) para garantir a confidencialidade de qualquer dado ou informação do CONTRATANTE que receber em seu ambiente ou em terceiro contratado.
- 6.25** A CONTRATADA deverá comunicar formalmente o CONTRATANTE sempre que identificar algum serviço com falhas de implementação e que tornem o ambiente vulnerável a indisponibilidade.
- 6.26** As equipes de ataque (RED TEAM) e defesa (BLUE TEAM) devem interagir e funcionar de maneira integrada. A equipe de ataque deve compartilhar seu conhecimento no sentido de indicar soluções para vulnerabilidades encontradas e a equipe de defesa deve possuir conhecimento das táticas e técnicas de ataque para que, por meio da atuação conjunta (PURPLE TEAM), aumente-se a efetividade da proteção do ambiente. Considerando a possibilidade de contratação dos serviços em separado, conforme disponibilidade orçamentária e consequente emissão de Ordem de Serviço, os serviços foram nomeados em separado, no entanto, objetiva-se que, quando os dois serviços forem demandados, as equipes RED TEAM e BLUE TEAM atuem integradas, tornando-se de fato em uma equipe PURPLE TEAM.

7. SERVIÇO DE OPERAÇÃO E ATENDIMENTO A REQUISIÇÕES

- 7.1** Tem por objetivo sustentar e operar todas as soluções e produtos de segurança do CJF, bem como a realização permanente de ações proativas voltadas para a segurança do parque computacional do CJF, descritas no ANEXO III – PLATAFORMA DE SEGURANÇA a fim de e mantê-lo estável, disponível e íntegro.
- 7.2** A CONTRATADA deverá realizar avaliação completa do ambiente do contratante com o objetivo identificar lacunas ou oportunidades de melhoria (Gap Analysis) com o objetivo de avaliar a maturidade dos controles de segurança do CONTRATANTE.
- 7.2.1** A análise dos controles de segurança deverá ser realizada 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.



PODER JUDICIÁRIO
CONSELHO DA JUSTIÇA FEDERAL

7.2.2 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 CJF.

7.3 Principais atividades a serem executadas de forma contínua pela CONTRATADA:

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

7.3.2 Priorizar os atendimentos críticos, conforme definição do CONTRATANTE;

7.3.3 Monitorar permanente e avaliar criticamente os produtos e serviços de segurança do CONTRATANTE;

7.3.4 Traçar curvas de comportamento, definir a volumetria média de acessos e identificar comportamentos não usuais, visando antecipar a identificação de incidentes de segurança, antes mesmo de impacto nos serviços;

7.3.5 Atuar proativamente na antecipação e identificação de incidentes de segurança, antes mesmo do impacto nos serviços;

7.3.6 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;

7.3.7 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.

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

7.3.9 Supervisionar sua equipe na execução dos serviços de SI;

7.3.10 Elaborar e propor plano de execução dos serviços;

7.3.11 Organizar a alocação de turnos e de profissionais de sua equipe;

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

7.3.13 Executar outros serviços correlatos à supervisão dos profissionais na execução dos Serviços Gerenciados de Segurança;

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



PODER JUDICIÁRIO
CONSELHO DA JUSTIÇA FEDERAL

- 7.3.15** Fornecer sugestões e auxiliar na construção e manutenção contínua, com o apoio e aprovação do CJF, de procedimentos sistematizados e da base de conhecimento, contemplando todas as soluções de problemas resolvidos com respostas padronizadas;
- 7.3.16** Receber as demandas dos serviços relativas à área de segurança da informação e providenciar a execução e alocação de recursos de trabalho;
- 7.3.17** Consolidar os relatórios de atividades mensais (mês calendário), referente aos Serviços Gerenciados de Segurança, provendo informações gerenciais ao CONTRATANTE;
- 7.3.18** Supervisionar sua equipe de profissionais na execução das ações conjuntas com a área de infraestrutura, cumprindo a política de segurança da informação do CJF e aplicando as melhores práticas de segurança;
- 7.3.19** Consolidar em manuais de procedimentos e em base de conhecimento todas as soluções adotadas na execução das atividades;
- 7.3.20** Elaborar mensalmente relatórios de desempenho, auditoria e operação dos ativos sob sua administração;
- 7.3.21** Implantar as melhorias solicitadas pelos servidores do CONTRATANTE através das aberturas de chamados no sistema de gestão de serviços de TI;
- 7.3.22** Sugerir novas tecnologias para modernizar o ambiente tecnológico, buscando subsidiar a equipe do CONTRATANTE na gestão de segurança da informação;
- 7.3.23** Aplicar os seguintes processos do ITIL: Gerenciamento de Incidente, Cumprimento de Requisição, Gerenciamento de Problema, Gerenciamento da Configuração e de Ativo de Serviço, Gerenciamento de Mudança, Gerenciamento de Liberação e Implantação, Gerenciamento da Disponibilidade, Gerenciamento do Conhecimento, Gerenciamento de Níveis de Serviço, Gerenciamento do Catálogo de Serviço.
- 7.3.24** Manter atualizado o *Configuration Management Database* (CMDB) na ferramenta de Gerenciamento de Serviços de TI (ServiceNow) utilizada pelo CONTRATANTE;
- 7.3.25** Consolidar as sugestões de melhoria;
- 7.3.26** Executar as tarefas de implantação, substituição e atualização de soluções destinadas à área de segurança da informação, prevendo



PODER JUDICIÁRIO
CONSELHO DA JUSTIÇA FEDERAL

prazos, custos, recursos, qualidade conforme as práticas de Gerenciamento de Projetos – PMI;

- 7.3.27** Administrar a solução de proteção de gateway de e-mail, contemplando proteção *antimalware* e AntiSpam, filtragem de conteúdo e prevenção contra perda de dados;
- 7.3.28** Administrar a solução de antivírus para servidores de rede, *storage*, ambiente virtualizado e estações de trabalho;
- 7.3.29** Elaborar relatório detalhado das funcionalidades necessárias de equipamentos e softwares a serem adquiridos, conforme demandado pelo CONTRATANTE;
- 7.3.30** Levantar preliminarmente custos de hardware e softwares, conforme demanda;
- 7.3.31** Subsidiar tecnicamente, quando demandado, os processos de aquisição;
- 7.3.32** Subsidiar os servidores do CONTRATANTE quanto ao dimensionamento da capacidade de hardware e configuração dos ativos de segurança;
- 7.3.33** Abrir chamados técnicos na língua inglesa para os serviços de suporte técnico remoto das soluções de hardware e software de TI do CONTRATANTE;
- 7.3.34** 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.
- 7.3.35** Instalar e customizar softwares aplicativos e equipamentos relacionados à segurança homologados para uso no CJF, por solicitação do CONTRATANTE;
- 7.3.36** Receber as diretrizes relacionadas à área de Segurança da Informação e providenciar a execução e alocação de recursos de trabalho;
- 7.3.37** Apoiar e participar na implementação dos processos bem como na mensuração dos indicadores de objetivos instituídos pelo CONTRATANTE;
- 7.3.38** Realizar as atividades em estrita observância na Política de Segurança da Informação (PSI) e demais normas estipuladas pelo CONTRATANTE;



PODER JUDICIÁRIO
CONSELHO DA JUSTIÇA FEDERAL

- 7.3.39** Gerar e consolidar os relatórios de ataques, atualização de ativos, atualização de softwares (aplicação de *patches* e *fix*), sistemas de proteção – antivírus de *gateway* e de *endpoint*, IPS, firewall, Proxy etc. – para apresentação ao CONTRATANTE, constando as medidas tomadas e sugestões;
- 7.3.40** Implantar e configurar os túneis de VPN para intercomunicação com outros órgãos e parceiros via rede Wan e Internet e acessos remotos de usuários;
- 7.3.41** Consolidar em manuais e *scripts* todos os serviços e soluções adotadas sejam eles novos ou já implantados no CONTRATANTE;
- 7.3.42** Auxiliar na elaboração dos procedimentos e metodologias, e verificar e reportar o cumprimento dos mesmos pelas demais áreas de TI;
- 7.3.43** Apoiar o CONTRATANTE na análise e definição das regras de uso dos recursos computacionais do CONTRATANTE;
- 7.3.44** Implantar as melhorias solicitadas pelos servidores do CONTRATANTE através das ordens de serviço;
- 7.3.45** Monitorar e propor soluções aos projetos/atividades em andamento otimizando-os quanto aos requisitos de Segurança da Informação;
- 7.3.46** 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;
- 7.3.47** Participar da implantação de projetos/soluções, substituição e atualização de soluções destinadas à Segurança da Infraestrutura de rede;
- 7.3.48** Elaborar relatório detalhado das funcionalidades necessárias de equipamentos e softwares a serem adquiridos, destinados à Segurança da Informação;
- 7.3.49** Implantar e configurar regras de firewall, IDS, IPS, antivírus, *proxy*, *AntiSpam*;
- 7.3.50** Auxiliar na homologação das soluções destinadas à Segurança da Informação;
- 7.3.51** Realizar análise de tentativas de invasão a sistemas e equipamentos;
- 7.3.52** Auxiliar o CONTRATANTE nos projetos de Segurança da Informação;
- 7.3.53** Propor procedimentos de Segurança da Informação;



PODER JUDICIÁRIO
CONSELHO DA JUSTIÇA FEDERAL

- 7.3.54** 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;
- 7.3.55** Implantar serviço de disseminação de alertas relacionados à Segurança da Informação;
- 7.3.56** Apoiar o CONTRATANTE na revisão e atualização da política de backup;
- 7.3.57** Executar periodicamente testes de alta disponibilidade na infraestrutura do CONTRATANTE com o objetivo de validar o seu funcionamento;
- 7.3.58** 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;
- 7.3.59** Executar a atualização de versão de todos os softwares e hardwares do parque tecnológico que sustenta a segurança da informação.
- 7.3.60** Execução de mudanças de configuração nos ativos sob sua administração;
- 7.3.61** Execução das atividades relativas aos normativos e governança do CONTRATANTE naquilo que for relativo à sua área de atuação.
- 7.4** Os produtos listados abaixo devem ser criados e atualizados em conformidade com os padrões e necessidade do CJF e homologados formalmente junto à STI:
 - 7.4.1** Documento contendo a volumetria média de acessos, listando os limites a partir do qual serão considerados um incidente de segurança;
 - 7.4.2** Guia de procedimentos de sustentação do serviço de proteção de e-mail;
 - 7.4.3** Guia de procedimentos de sustentação do serviço de antivírus;
 - 7.4.4** Guia de procedimentos de sustentação do serviço de proteção unificada;
 - 7.4.5** Guia de procedimentos de sustentação do serviço de gestão unificado de ameaças;
 - 7.4.6** Guia de procedimentos de sustentação do serviço de firewall de aplicação;
 - 7.4.7** Guia de procedimentos de sustentação do serviço de gerenciamento de vulnerabilidades;
 - 7.4.8** Relatórios de Continuidade de Negócios contendo indicadores de capacidade e disponibilidade dos ativos, além de projeções de elevação do uso dos recursos computacionais;



PODER JUDICIÁRIO
CONSELHO DA JUSTIÇA FEDERAL

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

7.4.10 Catálogo de Serviços e Base de Itens de Configuração;

7.4.11 Base de Conhecimento.

- 7.5** 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;
- 7.6** A CONTRATADA deverá apoiar o CONTRATANTE em caso de mudanças requeridas por conta de atualizações ou remanejamentos de infraestrutura;
- 7.7** A CONTRATADA deverá realizar a configuração das ferramentas que compõem as soluções, a fim de garantir o uso eficiente delas;
- 7.8** Sempre que houver atendimento, a CONTRATADA deverá enviar relatório de atividades por e-mail para o CONTRATANTE;
- 7.9** A CONTRATADA deverá acionar o fabricante das ferramentas sempre que necessário, sem nenhum custo adicional para o CONTRATANTE.

8. SERVIÇO DE GESTÃO DE INCIDENTES DE SEGURANÇA (CSIRT – BLUE TEAM)

- 8.1** Tem por objetivo 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* NIST e SANS de resposta a incidente de segurança da informação e boas práticas de mercado.
- 8.2** As equipes de ataque (RED TEAM) e defesa (BLUE TEAM) devem interagir e funcionar de maneira integrada. A equipe de ataque deve compartilhar seu conhecimento no sentido de indicar soluções para vulnerabilidades encontradas e a equipe de defesa deve possuir conhecimento das táticas e técnicas de ataque para que, por meio da atuação conjunta (PURPLE TEAM), aumente-se a efetividade da proteção do ambiente.
- 8.3** Um incidente de segurança é definido como qualquer evento adverso, confirmado ou sob suspeita, relacionado à segurança de sistemas de informação do CONTRATANTE, levando a perda de um ou mais princípios básicos de Segurança da Informação: Confidencialidade, Integridade e Disponibilidade.



PODER JUDICIÁRIO
CONSELHO DA JUSTIÇA FEDERAL

- 8.4** O início do processo de resposta a incidente de segurança se dará, sempre que um evento adverso for submetido pelo SERVIÇO DE MONITORAMENTO DE ATAQUES CIBERNÉTICOS descrito no presente termo de referência, porém não se limitando a este. Poderá o corpo técnico de segurança do CONTRATANTE a qualquer tempo, abrir um incidente de segurança.
- 8.5** Após o incidente de segurança aberto, será de responsabilidade do grupo de resposta a incidente de segurança (CSIRT – Blue Team) da CONTRATADA, analisar os logs e artefatos enviados, a fim de no primeiro instante identificar as fontes geradoras de tais logs.
- 8.6** 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.
- 8.7** Como próximo passo o grupo de resposta a incidente de segurança (CSIRT – Blue Team) da CONTRATADA, deverá comunicar ao time de segurança da informação do CONTRATANTE as informações iniciais sobre o incidente de segurança gerado, e quais serão as linhas de atuação para solução do incidente.
- 8.8** Juntamente com o CONTRATANTE o grupo de resposta a incidente de segurança (CSIRT – Blue Team) da CONTRATADA, deverá definir a severidade do incidente de segurança. A severidade 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. Mais detalhes sobre definição da severidade se encontram no tópico NÍVEIS MÍNIMOS DE SERVIÇO.
- 8.9** Após análises iniciais do incidente, caberá ao o 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).
- 8.10** Todo o processo de análise e resultados obtidos, devem ser documentados a todo tempo na ferramenta de gestão de incidente da segurança da informação, para que o CONTRATANTE acompanhe todos os passos para a solução do incidente.
- 8.11** Uma vez identificado comportamento e os principais vetores de ataque, o grupo de resposta a incidente de segurança (CSIRT – Blue Team) da CONTRATADA, deverá definir e executar uma estratégia para a mitigação e contenção do ataque em questão. Caso seja necessário qualquer tipo de alteração no parque computacional do CONTRATANTE, para contenção e mitigação do incidente,



PODER JUDICIÁRIO
CONSELHO DA JUSTIÇA FEDERAL

deverá antes ser autorizado tal alteração pelo corpo técnico de segurança do CONTRATANTE.

- 8.12** 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.
- 8.13** Inicia-se então o processo de restauração dos serviços e soluções afetadas. Todo este processo é de responsabilidade da CONTRATADA, sendo realizado pelo grupo de resposta a incidente de segurança (CSIRT – Blue Team) da CONTRATADA.
- 8.14** 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 de segurança em questão.
- 8.15** 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.
- 8.16** O grupo de resposta a incidente de segurança (CSIRT – Blue Team) da CONTRATADA, deve documentar na ferramenta de incidente de segurança, 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.
- 8.17** O serviço de resposta a incidentes serão responsáveis por monitorar equipamentos e softwares componentes da soluções de segurança do CONTRATANTE, envolvendo identificação, classificação e análise de eventos que possam comprometer a disponibilidade, integridade e confidencialidade dos serviços;
- 8.18** O regime de execução deste serviço deverá ser 24x7x365 (vinte e quatro horas por dia, sete dias por semana, trezentos e sessenta e cinco dias por ano);
- 8.19** A contratada deverá prover serviços de resposta aos incidentes de segurança da informação diante os eventos registrados no monitoramento;



PODER JUDICIÁRIO
CONSELHO DA JUSTIÇA FEDERAL

- 8.20** Os serviços de monitoramento e resposta a incidentes de segurança poderão ser prestados por meio de Centro de Operações de Segurança da Informação.
- 8.21** A solução deve ter sua base de inteligência diariamente atualizada através de alimentadores (feeds) de informação, provenientes da base de conhecimento em ameaças da própria empresa e de terceiros;
- 8.22** A CONTRATADA deverá prover inteligência de proteção contra ataques cibernéticos e serviços de pesquisa e desenvolvimento de inteligência de proteção contra ataques cibernéticos, sendo responsável por:
- 8.22.1** Pesquisar novos tipos de ataques, vírus, malwares, botnets, vulnerabilidades e afins com intuito de melhoria contínua de detecção e mitigação destes males dentro dos serviços e ativos de segurança fornecidos pela CONTRATADA;
 - 8.22.2** Criar, em colaboração com a CONTRATANTE, casos de uso (regras) que devem ser implementados no SIEM fornecido no serviço de Monitoramento e Visibilidade de Ataques;
 - 8.22.3** Revisar periodicamente as regras do SIEM, realizando as adaptações e evoluções necessárias;
 - 8.22.4** Produzir e entregar informação de inteligência acionável, na forma de procedimentos para triagem de alertas e procedimentos para resposta a incidentes, correspondentes às regras do SIEM;
- 8.23** Fornecer serviços de integração de informações de inteligência sobre ameaças (threat intelligence):
- 8.23.1** Coletar diariamente informações de pelo menos 20 fontes relevantes de inteligência sobre ameaças (cyber threat intelligence feeds) disponíveis pelo mundo, de categorias como phishing, códigos maliciosos, botnets, internet profunda (deep web), spam, ataques APT (advanced persistent threats), ransomware etc.;
 - 8.23.2** Correlacionar as informações coletadas, utilizando plataforma de big data para processamento visando normalizar e deduplicar informações, gerando listas acionáveis de inteligência contra ameaças;
 - 8.23.3** Integrar as listas no serviço de Monitoramento e Resposta a Incidentes, no intuito de aprimorar a capacidade da detecção de incidentes e diminuir falso-positivos;
 - 8.23.4** Monitorar ameaças emergentes e avaliar a aplicabilidade especificamente no ambiente do CONTRATANTE, propondo proativamente a realização de contramedidas com o objetivo de prevenir a exploração de alguma brecha de segurança;



PODER JUDICIÁRIO
CONSELHO DA JUSTIÇA FEDERAL

8.23.5 A solução deve ser capaz de detectar em tempo real, ameaças alimentadas pelas seguintes bases de inteligência:

- a) relatórios de ameaças e segurança;
- b) relatórios de botnets e centros de Comando e Controle;
- c) identificação de exploit kits;
- d) indicadores de ataques “zeroday”;
- e) indicadores de comprometimento, suspeitas e avisos Informativos;
- f) inteligência de tendências;
- g) proxies anônimos;
- h) classificação de sites;
- i) endereços de rede TOR.

9. SERVIÇO DE GESTÃO DE VULNERABILIDADES

- 9.1** Tem por objetivo, de forma proativa e recorrente (uma vez por mês), identificar possíveis vulnerabilidades de segurança da informação no ambiente a fim de evitar que ataques cibernéticos obtenham sucesso explorando vulnerabilidades conhecidas;
- 9.2** O serviço também contempla as correções de vulnerabilidade, quando estas são identificadas nos equipamentos e soluções de segurança;
- 9.3** Para a prestação deste serviço deverão ser utilizadas ferramentas para descoberta de novas vulnerabilidades de aplicações e infraestrutura bem como a gestão de todo ciclo de vida das vulnerabilidades encontradas, desde a descoberta até a correta mitigação;
- 9.4** O CONTRATANTE possui licenças da solução para gestão de vulnerabilidades *Nexpose* da fabricante *Rapid7* que atualmente não estão cobertas por suporte. Apesar desta solução ser de propriedade do CONTRATANTE, será de responsabilidade da CONTRATADA a renovação ou substituição da solução, bem como operar, sustentar, suportar e apresentar a melhoria contínua da ferramenta ofertada durante todo o período de vigência do contrato;
- 9.5** A ferramenta de gestão de vulnerabilidades deverá ser capaz de escanear e gerenciar no mínimo 1.500 (hum mil e quinhentos) ativos, podendo ser estações de trabalho, notebooks, switches, roteadores, *access points*, servidores de rede, servidores de aplicações, servidores de banco de dados, aplicações web etc;



PODER JUDICIÁRIO
CONSELHO DA JUSTIÇA FEDERAL

- 9.6** Efetuar descoberta dos ativos que possuam endereço IP, sejam servidores de rede, máquinas virtuais, estações de trabalho, serviços de infraestrutura, aplicações, switches etc;
- 9.7** Suportar múltiplos scanners, gerenciando e compartilhando recursos de verificação de uma console centralizada;
- 9.8** Permitir correlacionar eventos baseados no sistema operacional, porta/protocolo, banners e vulnerabilidades.
- 9.9** Permitir detectar vulnerabilidades em aplicações Web, bases de dados, aplicações comerciais, sistemas operacionais e dispositivos de rede;
- 9.10** Permitir verificar vulnerabilidades em ambiente Windows para, no mínimo: detecção de *hot fixes*, *service packs*, registros, *backdoors*, trojans, *malwares*, *peer to peer*, portas de serviço habilitadas e antivírus.
- 9.11** Suportar efetuar varredura à procura de vulnerabilidades e *exploits*.
- 9.12** Permitir detectar vulnerabilidades em dispositivos de redes sem fio, aplicações baseadas em WEB, bases de dados, aplicações comerciais, sistemas operacionais e dispositivos de rede.
- 9.13** Permitir a descoberta das vulnerabilidades para os equipamentos, produtos, peças ou softwares alocados para atender aos requisitos de todos os itens de serviço e para todo o ambiente computacional do CJF.
- 9.14** CONTRATADA deverá compor ao ambiente de segurança da informação atualmente implementadas no CONTRATANTE, soluções de gestão de vulnerabilidades capazes de identificar vulnerabilidades de infraestrutura e aplicações, que possam comprometer a disponibilidade, integridades e confiabilidade dos dados e serviços do CONTRATANTE.
- 9.15** As soluções de prestação dos Serviços de Gestão de Vulnerabilidades deverão serem instaladas no CONTRATANTE, de modo a prover varredura, identificação e gestão de vulnerabilidades do parque computacional do CONTRATANTE.
- 9.16** Deverá ser utilizada, pelo menos, 01 (uma) ferramenta de análise de vulnerabilidade com foco em infraestrutura, e 01 (uma) ferramenta de análise de vulnerabilidade com foco em aplicações web.
- 9.17** Apesar de ser necessário e permitida a utilização de ferramentas para descoberta de vulnerabilidades no ambiente do CONTRATANTE, se espera que a CONTRATADA se utilize também de métodos e técnicas assistidas, para identificar possíveis vulnerabilidades no ambiente do CONTRATANTE.
- 9.18** A fim de mitigar e prever possíveis impactos durante as rotinas de validação de vulnerabilidade, antes do início da execução do serviço, as ferramentas



PODER JUDICIÁRIO
CONSELHO DA JUSTIÇA FEDERAL

adotadas para execução deverão ser apresentadas ao time de segurança da informação do CONTRATANTE, que poderá ou NÃO aprovar a utilização delas.

9.19 Todas as ferramentas e soluções hardware e/ou software, deverão possuir os seguintes requisitos nativos, a saber:

- 9.19.1** Varredura e descoberta de vulnerabilidades para todos os equipamentos e softwares que compõem a solução de Serviços Gerenciados de Segurança, bem como para todo o ambiente computacional do CONTRATANTE, ou seja, estações de trabalho, impressoras, dispositivos móveis, *access points*, entre outros;
- 9.19.2** Agrupamento de eventos baseada em sistemas operacionais, endereços IP, nome DNS, nome NetBIOS, porta de serviços e vulnerabilidades;
- 9.19.3** Detecção de vulnerabilidades em sistemas operacionais, protocolos de rede, aplicações WEB, banco de dados, aplicativos para escritório, processadores de texto, planilha de cálculo, apresentação gráfica, gerenciador de tarefas e de e-mails;
- 9.19.4** Detecção de vulnerabilidades em ambiente Microsoft Windows, incluindo Hot Fixes, Service Packs e registros de sistema operacional;
- 9.19.5** Detecção de vulnerabilidades em ambientes Oracle, SQL Server e Microsoft Exchange;
- 9.19.6** Varredura de ativos de modo intrusivo e não intrusivo;
- 9.19.7** Capacidade de selecionar e agrupar ativos encontrados, com possibilidade de incluir faixa de exclusão de endereços IP para varredura;
- 9.19.8** Capacidade de definir *templates* de configuração de *scans* e de agendamento de *scans*;
- 9.19.9** Capacidade de configuração de usuário e senha para realização de varredura autenticada de sistemas operacionais e aplicações;
- 9.19.10** Capacidade de identificação de links em aplicações WEB e de navegação pelos links identificados;
- 9.19.11** Geração de tickets para vulnerabilidades encontradas, permitindo marcar uma vulnerabilidade em determinado ativo como corrigida ou ignorada;
- 9.19.12** Integração com a base de dados de vulnerabilidades CVE (Common Vulnerabilities and Exposures);
- 9.19.13** Definição de, no mínimo, 3 (três) níveis de criticidade de vulnerabilidades;



PODER JUDICIÁRIO
CONSELHO DA JUSTIÇA FEDERAL

- 9.19.14** Recurso de base de conhecimento com, no mínimo, 40.000 (quarenta mil) assinaturas de vulnerabilidades, com atualização automática a partir do site do fabricante;
- 9.19.15** Recurso para acompanhamento da evolução das remediações de vulnerabilidades encontradas;
- 9.19.16** Apresentação de graduação de riscos, baseada em pontuação, que permite medir o nível de riscos dos recursos e sistemas encontrados;
- 9.19.17** Apresentação de procedimentos necessários para eliminar, remediar ou mitigar vulnerabilidades encontradas, tais como indicação de atualizações de software;
- 9.19.18** Levantamento e classificação de criticidade de ativos, baseada na importância do ativo e nas vulnerabilidades encontradas; Configuração de frequência e periodicidade de varreduras na rede;
- 9.19.19** Apresentação de relatórios analíticos contendo dados, informações, indicadores e métricas que permitam avaliar a exposição do parque computacional do CONTRATANTE em relação aos riscos de segurança em TI, contendo: hosts encontrados, topologia de rede, serviços, vulnerabilidades descobertas, nível de risco por plataforma e por vulnerabilidade;
- 9.19.20** Atualização automática de tabela de ativos monitorados, com suporte à ferramenta de gestão de incidentes detectados (baseline), contendo informações sobre serviços e vulnerabilidades encontradas por ativo;
- 9.19.21** Recurso de alertas por e-mail de vulnerabilidades encontradas;
- 9.19.22** Capacidade de exportação de relatório de vulnerabilidades em formato PDF e CSV;
- 9.19.23** Gerenciamento por WebUI (WEB User Interface) via HTTPS (Secure Hypertext Transfer Protocol) e console gráfica centralizada;
- 9.19.24** Gerenciamento único, centralizado, responsável pela aplicação das políticas de segurança, administração e controle das funcionalidades dos serviços;
- 9.19.25** Gerenciamento com perfis de acessos distintos para administração de funcionalidades, acesso a logs e emissão de relatórios;
- 9.19.26** Gerenciamento com visualização de status dos serviços;
- 9.19.27** Gerenciamento com recurso de informações estatísticas de fluxo de tráfego, incluindo quantidade de conexões, throughput e desempenho dos serviços;



PODER JUDICIÁRIO
CONSELHO DA JUSTIÇA FEDERAL

- 9.19.28** Gerenciamento com recurso de auditoria de alteração de configurações e acesso à ferramenta de administração, incluindo usuário, data e horário de acesso e ações realizadas;
- 9.19.29** Gerenciamento com recurso de validação de políticas de segurança antes da aplicação, responsável pela identificação de erros e inconsistências;
- 9.19.30** Gerenciamento com recurso de replicação de configurações e atualização de software;
- 9.19.31** Gerenciamento com recurso de monitoramento de logs, debugging e captura de pacotes;
- 9.19.32** Gerenciamento com recurso de backup e importação automáticos de arquivos de configuração;
- 9.19.33** Deve possuir integração com VMware vCenter para automaticamente popular bases de ativos do ambiente virtual;
- 9.20** Analisar diariamente até 25 (vinte e cinco) sites contra pichação (defacement) e ataques, tais como cross-site scripting, SQL injection e DoS.
- 9.21** A ferramenta deverá ser instalada no ambiente do CONTRATANTE ou, mediante solicitação justificada da CONTRATADA, o CONTRATANTE poderá permitir a instalação em ambiente da CONTRATADA.
- 9.22** Realizar e apresentar relatório de testes de vulnerabilidades de todo o ambiente tecnológico, conforme as práticas de Segurança da Informação;
- 9.23** A solução deve utilizar sistema de pontuação e priorização das vulnerabilidades, utilizando no mínimo os seguintes critérios:
 - 9.23.1** CVSS Impact Score;
 - 9.23.2** Existência de códigos de exploração da vulnerabilidade encontrada (exploit);
 - 9.23.3** Existência de módulos de exploração da vulnerabilidade em frameworks automatizados, tais como: Metasploit, Core Impact, CANVAS.
- 9.24** A CONTRATADA deve apresentar relatório das principais remediações para o tratamento das vulnerabilidades mais comuns, das vulnerabilidades mais críticas e dos exploits conhecidos;
- 9.25** A solução deve ter uma API para automação de processos e integração com produtos de terceiros.



PODER JUDICIÁRIO
CONSELHO DA JUSTIÇA FEDERAL

- 9.26** A solução deve possuir capacidade de realizar o escaneamento de vulnerabilidades em imagens e contêiners e de se integrar com fluxo de integração contínua.

10. SERVIÇO DE MONITORAMENTO E VISIBILIDADE DE ATAQUES CIBERNÉTICOS

- 10.1** Visa o monitoramento contínuo e ininterrupto de ataques cibernéticos direcionados ao CJF, através de correlacionamento de logs, pacotes de redes, 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 de segurança da informação, conforme definido em processo de gestão de incidentes.

- 10.2** A CONTRATADA deverá prover ao ambiente de soluções de segurança da informação permitam a visibilidade de logs, rede e informações, capaz de identificar eventos maliciosos, através de correlacionamento de eventos e tráfego de rede, que possam comprometer os serviços tecnológicos do CONTRATANTE;

10.3 Serviço de Visibilidade de Logs, Fluxos e Informações:

- 10.3.1** Todos os módulos que compõe a solução deverão se integrar visando constituir um ambiente homogêneo de análise, investigação, inteligência, defesa cibernética e resposta a incidentes nos processos, incluindo má utilização dos sistemas e tentativas sequenciais de utilização suspeitas inclusive entre sistemas e plataformas diferentes;
- 10.3.2** Deve possuir no mínimo as seguintes funcionalidades: coleta de pacotes, coleta de logs, geração de metadados, indexação, agregação e enriquecimento dos metadados dos coletores, correlacionamento avançado de alertas e tratamento de incidentes;
- 10.3.3** Permitir a correlação de eventos provenientes de logs e pacotes, devidamente estruturados em metadados;
- 10.3.4** A solução deverá ter capacidade e ser licenciada para processar, no mínimo, todos os eventos gerados pelos ativos de segurança do ambiente tecnológico;
- 10.3.5** Deverá possuir retenção mínima de 1 (um) ano dos registros de eventos, sendo que no período mínimo de 6 (seis) meses os dados devem estar prontamente acessíveis ("quentes");



PODER JUDICIÁRIO
CONSELHO DA JUSTIÇA FEDERAL

- 10.3.6** A solução ofertada deverá possuir armazenamento próprio independente, sem onerar o sistema de armazenamento de dados do CONTRATANTE;
- 10.3.7** A solução deve ser capaz de integrar em uma única console de visualização, dados e metadados de logs e fluxos de rede;
- 10.3.8** A solução deve permitir buscas utilizando expressões regulares e palavras-chave em todo o conteúdo dos dados e metadados capturados;
- 10.3.9** A solução deve possuir compatibilidade e integração com solução de detecção, análise e forense comportamental de malware do tipo “Oday” em *endpoints* (EDR) do CONTRATANTE, com intuito de complementar a visibilidade entregue e capacidade de análise de atividade maliciosa;
- 10.3.10** A solução deve possuir a capacidade de navegação contínua sobre os dados em formato “*drill down*”, podendo realizar pesquisas avançadas para melhor correlação de eventos;
- 10.3.11** A solução deve prover uma interface intuitiva, permitindo que em até 5 (cinco) cliques seja possível chegar a uma ação suspeita ou ataque, sem prévio conhecimento dela;
- 10.3.12** A solução deve permitir a criação e customização de regras, alertas, gráficos e relatórios na própria interface;
- 10.3.13** A solução deve possuir pelo menos 150 (cento e cinquenta) regras pré-definidas;
- 10.3.14** A solução deve permitir o agendamento automático e manual de relatórios, com a possibilidade de envio por e-mail;
- 10.3.15** O fabricante da solução deve possuir ampla capacidade de análise de malwares e acessar centro de pesquisa e desenvolvimento e inteligência às novas ameaças;
- 10.3.16** A solução deve permitir o desenvolvimento e customização de interpretadores (*parsers*) utilizando linguagens XML, LUA ou REGEX através de ferramenta gráfica do mesmo fabricante;
- 10.3.17** A solução deve possuir integração com ferramenta de emulação e identificação malwares (sandbox) do CONTRATANTE;
- 10.3.18** O módulo de análise de malware deve permitir o uso de regras YARA;
- 10.3.19** A solução deve possuir integração com soluções de gestão de centro de operações de segurança (Security Operations Center SOC);
- 10.3.20** A solução deve permitir a criação de perfis de visualização do metadados derivados dos dados capturados;



PODER JUDICIÁRIO
CONSELHO DA JUSTIÇA FEDERAL

- 10.3.21** A solução deve possuir mecanismo de auditoria através da geração de logs das atividades realizadas no console de gerência e investigação;
- 10.3.22** A solução deve permitir a visualização e análise dos dados capturados em formato gráfico de linha do tempo, construindo os gráficos com base no número de sessões, bytes ou pacotes;
- 10.3.23** A solução deve possuir controle de acesso baseado em papéis e perfis de usuários;
- 10.3.24** A solução deve permitir gerar relatórios em formatos HTML, PDF e CSV;
- 10.3.25** A solução deve possuir um módulo para construção de relatórios customizados pelo usuário, com funcionalidade do tipo “selecionar” ou “arrastar e soltar” para definição dos campos e elementos;
- 10.3.26** A solução deve possuir a capacidade de integração com outras soluções de segurança, por meio de envio de logs/eventos via protocolos SYSLOG e SNMP;
- 10.3.27** A solução deve possuir integração com serviço de diretório (Active Directory) e possuir capacidade de obter logs de autenticações em servidores Linux;
- 10.3.28** A solução deve suportar a comunicação criptografada entre os componentes envolvidos;
- 10.3.29** A solução deve suportar o gerenciamento dos componentes através de uma interface de gerência central;
- 10.3.30** A solução deve possuir a criação de relatórios utilizando qualquer informação armazenada no sistema;
- 10.3.31** A solução deve suportar a integração com sistemas de GRC (Governance, Risk e Compliance), provendo contexto de governança a um incidente gerado pela solução proposta;
- 10.3.32** A solução deve possuir a funcionalidade para resolução de endereços IP, como localização da cidade, país e organização das conexões;
- 10.3.33** A solução deve suportar a análise de dados na camada de aplicação (modelo OSI) a partir de entidades como usuários, email, endereço, arquivos e ações;
- 10.3.34** A solução deve possuir um módulo de análise avançada de eventos, podendo comparar metadados e correlacionar eventos em uma base histórica;



PODER JUDICIÁRIO
CONSELHO DA JUSTIÇA FEDERAL

- 10.3.35** A solução deve suportar a criação de interpretadores (parsers) customizados para, no mínimo, 20 (vinte) sistemas proprietários do CONTRATANTE;
- 10.3.36** A solução deve suportar de forma nativa os logs de todos os produtos de segurança utilizados pelo CONTRATANTE;
- 10.3.37** A solução deve ser capaz de coletar logs e eventos de quaisquer dispositivos e aplicações IP que suportem nativamente os protocolos: SYSLOG, SYSLOGNG, SNMP, Microsoft Windows Event Logging API, Microsoft Windows Remote Management, arquivos de logs recebido via FTP, arquivos de logs formatados por delimitadores, ODBC e CISCO Security Device Event Exchange (SDEE);
- 10.3.38** A solução deve utilizar formatos de logs/eventos através de formatos nativos de cada fabricante do dispositivo, sem utilizar um tipo de formato comum definido pelo proponente da solução;
- 10.3.39** A solução não deve exigir a adição de agentes ou software nos dispositivos monitorados, exceto caso o dispositivo a ser monitorado não disponibilize nenhum meio nativo de envio de logs citado no item anterior;
- 10.3.40** A solução deve coletar e armazenar logs/eventos dos dispositivos sem realizar normalização no momento da coleta;
- 10.3.41** A solução não deve fazer uso de sistema de bancos de dados relacional por questão de desempenho, normalização e DBAs requeridos por esses sistemas;
- 10.3.42** A solução deve permitir que os logs/eventos dos dispositivos da CONTRATANTE sejam enriquecidos com informações de classificação de risco;
- 10.3.43** A solução deve permitir o correlacionamento de logs/eventos próximo ao tempo real;
- 10.3.44** A solução deve notificar através de alertas, comportamentos anômalos baseados em múltiplos eventos que ocorrerem em um determinado período;
- 10.3.45** A solução deve ser capaz de notificar o administrador caso algum dispositivo monitorado pare de enviar eventos;
- 10.3.46** A solução deve permitir que o administrador possa filtrar logs/eventos ao gerar relatórios;



PODER JUDICIÁRIO
CONSELHO DA JUSTIÇA FEDERAL

- 10.3.47** A solução deve permitir que os relatórios sejam executados em periodicidade diária, semanal, mensal ou em ocasiões específicas de forma automática;
- 10.3.48** A solução deve possuir a capacidade de análise avançada de eventos em tempo real através de regras de correlacionamento e eventos complexos em dados correlacionados através da linguagem EPL (Event Processing Language) ou inteligência artificial;
- 10.3.49** A solução deve suportar nativamente a coleta de NetFlow e IPFIX, sendo capaz de detectar ataques do tipo NetFlow Synflood na coleta dos fluxos de rede;
- 10.3.50** A solução deve ter a habilidade de receber logs/eventos oriundos de um relay de syslogs;
- 10.3.51** A solução deve suportar o recebimento de eventos no formato Common Event Format (CEF);
- 10.3.52** A solução deve possuir procedimento de Backup & Restore para um sistema de armazenamento de longo prazo, implementando o conceito de arquivador.
- 10.3.53** A solução deve suportar o armazenamento em camadas, com as seguintes funcionalidades: HOT (dados presentes em sistemas como DACs e SANs), WARM (dados presentes em sistemas como NAS para pesquisa, execução de relatórios, exportação de dados) e COLD (dados presentes em sistemas de armazenamento offline para possível restauração em WARM);
- 10.3.54** A solução deve suportar nos sistemas de armazenamento de longo prazo, pelo menos um dos três algoritmos de compressão: gzip, bzip2 ou lzma;
- 10.3.55** A solução deve permitir a agregação em grupos de instâncias dos vários sistemas de armazenamento de longo prazo;
- 10.3.56** A solução deve permitir a exportação de logs/eventos armazenados nos formatos texto, XML, JSON, CSV;
- 10.3.57** A solução deve permitir a criação e acompanhamento de Incidentes de Segurança, de forma manual ou automática, com no mínimo as seguintes características:
- a) Sumário do incidente, incluindo título, sumário e detalhes. Também deverá incluir o status do incidente, incluindo data de criação, de modificação, de fechamento, tempo em que o chamado está aberto, número de alertas agregados, prioridade e analistas envolvidos;



PODER JUDICIÁRIO
CONSELHO DA JUSTIÇA FEDERAL

- b) Classificação inicial da ameaça, incluindo categoria, origem (interna/externa), possibilidade de modificação manual da prioridade e justificativa, além de informações específicas para subsidiar o relatório de incidentes e possibilidade de inclusão de documentação adicional através da anexação de arquivos;
- c) Possibilidade de manter o histórico de atividades realizadas pelos analistas, tais como criação de registros, atualização de campos etc.;
- d) Permitir agregar vários alertas em um único incidente. Esta agregação de alertas deverá permitir a visualização rápida de, no mínimo, os seguintes campos: horário do alerta, nome, prioridade e aspectos comportamentais;
- e) Definição das tarefas a serem executadas. A plataforma deverá conter uma biblioteca de procedimentos de resposta já existente;
- f) Permitir inserir comentários dos analistas no incidente, de tal forma a possibilitar o registro de todas as atividades de análise;
- g) Permitir inserir análise forense como um complemento da análise do incidente;
- h) Permitir registrar os resultados de um Incidente incluindo sua confirmação, categoria de ataque, identificação de técnicas utilizadas, detalhes sobre o alvo dos ataques e eficácia dos controles de detecção, prevenção e investigação;
- i) Permitir análise comportamental para detecção automática de incidentes relacionados às atividades de Comando e Controle (C2) ;
- j) Permitir detecção de Movimentos Laterais para identificação de atividades de login suspeitas em ambientes Windows e Linux.

10.3.58 A solução deve possuir tecnologia de análise comportamental (UBA), baseado em técnicas de "machine learning" e análises estatísticas para a monitoração de segurança, gerando índices de riscos para eventos e entidades mapeadas;

10.3.59 A solução deve exibir na tela inicial a data e hora do último login de forma garantir que a credencial não esteja sendo compartilhada ou utilizada indevidamente;

10.3.60 A solução deve permitir o processamento de informações estruturadas de ameaças STIX™ ("Structured Threat Information eXpression") ;



PODER JUDICIÁRIO
CONSELHO DA JUSTIÇA FEDERAL

- 10.3.61** A solução deve possuir um ambiente de construção de regras que ofereça um mecanismo de testes (debug), visando à redução de erros de lógica e sintaxe;
- 10.3.62** A solução deve permitir o ajuste de sessões concorrentes na interface de gerência;
- 10.3.63** A solução deve possuir um menu de contexto na interface de investigações, de forma visualizar instantaneamente se endereços foram encontrados em Alertas, Incidentes ou Listas.
- 10.3.64** Permitir o controle de acesso dos usuários à solução por meio de autenticação em serviço de diretório como Microsoft Active Directory e LDAP;
- 10.3.65** A distribuição dos módulos, conectores ou agentes - o que for aplicável ao correto funcionamento da solução - no ambiente tecnológico deve ser livre, no sentido de permitir a conexão com os ativos do CONTRATANTE sem a necessidade de licenças adicionais, dentro do limite de processamento e indexação licenciados;
- 10.3.66** A modalidade de licenciamento deverá permitir a distribuição livre de elementos de coleta, filtragem e agregação, gerados com o uso de SDK ou API (Application Programming Interface), independentemente do número e arquitetura;
- 10.3.67** Deve-se considerar os eventos com tamanho médio de 400 (quatrocentos) bytes;
- 10.3.68** Deve ter capacidade de coletar, processar e correlacionar flows de rede NetFlow v9;
- 10.3.69** Cada sessão deve ser considerada como composta por 2 flows entrante (inbound) e saínte (outbound) do tráfego monitorado de protocolos IP, TCP, UDP, ICMP, dentre outros protocolos IP;
- 10.3.70** A solução deve garantir o processamento do fluxo de eventos gerados pelos dispositivos, sem limitação por dispositivo em qualquer momento (pico, vale ou operação normal) ;
- 10.3.71** Permitir a instalação de todos os seus componentes em ambiente virtual ou servidores físicos;
- 10.3.72** Ser virtualmente ilimitada (conforme políticas internas de retenção) no volume de dados coletados, processados e armazenados, sendo limitada apenas ao volume de dados licenciados neste certame;



PODER JUDICIÁRIO
CONSELHO DA JUSTIÇA FEDERAL

- 10.3.73** Todas as funções abaixo deverão ser executadas pela mesma solução tecnológica. Caso sejam necessários componentes externos, eles devem fazer parte da solução proposta;
- 10.3.74** Suportar a coleta de dados de no mínimo 1000 (hum mil) ativos;
- 10.3.75** Caso a solução trabalhe sem agentes (agentless), deverá prover funcionalidades análogas, sem perda de caracterização da solução;
- 10.3.76** Ter seu coletor de dados com funcionalidades de coletar, aplicar parsing, normalizar, classificar, agregar informações, sumarizar, processar regras, compactar e armazenar os dados recebidos dos elementos geradores de eventos presentes no ambiente tecnológico;
- 10.3.77** Ter seu correlacionador a capacidade de processar regras tanto em tempo de coleta como em tempo de análise, analisar e correlacionar eventos globais advindos dos dispositivos do ambiente tecnológico e aplicar regras de correlacionamento e análise conforme regras configuráveis antes, durante e após o processamento. Essas regras serão definidas e customizadas na fase de instalação e configuração da solução;
- 10.3.78** Ter um sistema de armazenamento de eventos capaz de receber informações e dados enviados pelos ambientes tecnológicos, ou de diferentes fontes, compactar, organizar e armazenar e gerenciar todo o ciclo de armazenamento da solução, garantida a integridade do dado no formato raw;
- 10.3.79** Ter um console de monitoramento e operação para visualizar os dados dos dispositivos do ambiente tecnológico exibindo resultados que proporcionem o controle sobre o ambiente corporativo no ponto de vista de:
- a) Análise de incidentes;
 - b) Segurança da informação na perspectiva de SIEM (alertas) e forense (correlação, pesquisas ad hoc e relatórios) ;
 - c) Análise de segurança da informação garantindo a integridade dos eventos e evidências.
- 10.3.80** Permitir investigação de ataques, anomalias, alvos de ataque, atacantes da rede e correlacionar eventos e atividades de rede, bem como identificar os alvos;
- 10.3.81** Emitir relatórios executivos, operacionais e de conformidade a normas de mercado e flexibilidade na criação de novos relatórios pelos próprios usuários, sem interferência de componentes externos ou a necessidade



PODER JUDICIÁRIO
CONSELHO DA JUSTIÇA FEDERAL

de customização em código complexa que exija serviços profissionais terceiros;

- 10.3.82** Visualizar os dados dos dispositivos do ambiente tecnológico de forma centralizada, fornecendo um conjunto de funções e indicadores gerenciais específicos, contemplando o panorama de monitoramento e segurança no ambiente da instituição e flexibilidade na criação de novos relatórios pelos próprios usuários, sem interferências de componentes externos ou a necessidade de customização em código complexa que exija serviços profissionais terceiros;
- 10.3.83** Desenvolvimento de regras para o correlacionamento para possibilitar a criação de regras de correlacionamento, através de ferramenta gráfica ou linha de comando. A solução deverá prover módulo de construção e testes de regras. Toda a construção das regras deverá ser feita em ambiente gráfico e as regras deverão possibilitar ações, como por exemplo, enviar e-mails e traps SNMP;
- 10.3.84** Ser capaz de agregar informações sobre a localização geográfica dos endereços IP envolvidos no evento;
- 10.3.85** A comunicação entre os componentes da solução deve ser feita através de criptografia, com uso de algoritmos RSA 2048, AES (128 bits ou mais) e/ou 3DES (192 bits ou mais), garantindo a autenticidade, confidencialidade e integridade dos dados, utilizando o protocolo TCP/IP;
- 10.3.86** Prover juntamente com a subscrição de atualização dos componentes da solução pelo período do contrato de suporte, o acesso à biblioteca de casos de uso do fabricante, que contenha pacotes especializados de regras, dashboards e coletores desenvolvidos pelo fabricante que permitam a implementação de correlação e monitoração avançada, sem necessidade de redesenvolvimento;
- 10.3.87** Ser capaz de realizar consulta por eventos em tabelas de bancos de dados Oracle, MySQL e Microsoft SQL Server;
- 10.3.88** A comunicação entre os dispositivos do ambiente tecnológico geradores os dados e a solução devem ser feita no mínimo por meio dos protocolos a seguir: SYSLOG, SDEE, SNMPv2 e SNMPv3, além da capacidade de mapeamento de pastas de redes ou serviços nativos de coleta de dados;
- 10.3.89** A coleta de eventos de dispositivos não suportados nativamente pode ser feita através de conectores customizados. Estes conectores customizados devem utilizar padrões de mercado como CSV, arquivo



PODER JUDICIÁRIO
CONSELHO DA JUSTIÇA FEDERAL

texto, XML, ODBC, JDBC, JSON, ou pela criação de campos realizado dentro da própria solução;

10.3.90 Possuir a funcionalidade de ler e normalizar eventos de log armazenados em formato texto (w3c), SQL database, compactados ou não;

10.3.91 Ofuscar os campos sensíveis dos eventos (senhas, identidade funcional, números de cartões de crédito e outros similares);

10.3.92 Marcar (através de tag, label ou similar) os eventos com base em unidade organizacional: departamento, setor, divisão corporativa ou similar;

10.3.93 Filtrar e selecionar os eventos que serão inseridos na solução e permitir a criação e alteração de filtros;

10.3.94 Os conectores, ou solução similar, deverão coletar as plataformas: Windows, Linux (RHEL, Debian), AIX, HP-UX, sempre na última versão;

10.3.95 Os conectores, ou solução similar, deverão coletar logs das seguintes soluções:

a) Anti-malware: Trend Micro, Symantec, McAfee, Kaspersky;

b) Antispam: Trend Micro, Proofpoint, Symantec;

c) UTM: Fortinet, Checkpoint e Palo Alto;

d) Firewall de Aplicação: Fortinet, F5 e Imperva;

e) Switches: Cisco e HP;

10.3.96 Coletar e aplicar parsing (segmento do dado) nos eventos do dispositivo monitorado em tempo próximo ao real;

10.3.97 A solução deve ser composta de agentes que têm como função básica fazer a interface com o dispositivo monitorado, recebendo ou buscando eventos relevantes que serão inseridos na solução;

10.3.98 Suporte ao padrão de criptografia FIPS, em todos os conectores;

10.3.99 Controlar a utilização da banda utilizada diretamente do conector sem a necessidade de usar recursos do sistema operacional;

10.3.100 Separar eventos por meio de anotações em campos, originados por quaisquer campos disponíveis e normalizados (ex: Cliente 1 - VLAN ID 10, Cliente 2 - VLAN ID 20) mesmo que o evento seja de um mesmo firewall;

10.3.101 Verificar conformidade com as políticas, controles e normas internas e externas;



PODER JUDICIÁRIO
CONSELHO DA JUSTIÇA FEDERAL

- 10.3.102** A solução deve ser capaz de normalizar e categorizar os eventos em um padrão único;
- 10.3.103** O coletor da solução deverá ser capaz de armazenar os dados localmente (cache) em caso de indisponibilidade do componente correlacionador;
- 10.3.104** Deve permitir a configuração do tamanho do cache;
- 10.3.105** O envio dos dados em cache deve ocorrer imediatamente a disponibilização do correlacionador;
- 10.3.106** Informar os eventos que compõem um alerta e/ou incidente de segurança, identificado pelas regras de correlação da solução, referenciando estes eventos raw a partir do evento de alerta/incidente;
- 10.3.107** Deve permitir acrescentar o horário (timestamp) correto da recepção do evento/log na solução, preservando o horário original do evento. Esse horário deve ser obtido pelo sistema através de sincronização com servidores NTP previamente definidos, e sincronizado entre todos os componentes da solução;
- 10.3.108** A solução deve ser capaz de marcar (através de tag, label ou similar) os eventos com base em unidade organizacional: departamento, setor, secretaria ou similar. Essa marcação pode ser feita por atributos da própria mensagem, da origem do log, ou do endereço de origem do evento;
- 10.3.109** A solução deve ser capaz de inserir nos eventos normalizados metadados sobre georreferência dos mesmos, ainda que sejam endereços privados;
- 10.3.110** Tanto os eventos de segurança quanto os de conformidade devem ser normalizados para um único padrão de eventos utilizado pela solução;
- 10.3.111** Todo serviço técnico para coleta dos dados dos dispositivos do ambiente tecnológico deve estar incluído na proposta técnica;
- 10.3.112** A solução deve ser capaz de coletar dados dos mais diversos dispositivos do ambiente tecnológico, garantindo que quaisquer alterações do atual ambiente tecnológico sejam suportadas;
- 10.3.113** Identificar rapidamente a causa raiz dos incidentes detectados no ambiente em console única;



PODER JUDICIÁRIO
CONSELHO DA JUSTIÇA FEDERAL

- 10.3.114** Capacidade de monitoramento de ambientes virtualizados em todas as suas camadas (virtualização, aplicação, sistemas operacionais, rede, servidores físicos e storages);
- 10.3.115** Implementar relatórios do grau de conformidade com normas reguladores de mercado, para no mínimo as seguintes normas: COBIT, ISO/IEC família 27000;
- 10.3.116** Emissão de relatórios de conformidade do ambiente monitorado em relação à norma ISO/IEC 27001 e ISO/IEC 27002, com base nos eventos recebidos;
- 10.3.117** Permitir testar as regras com eventos reais capturados anteriormente e mantidos na base de dados da solução, sem afetar a execução das regras em produção;
- 10.3.118** Executar regras de correlação pré-programadas. Deve permitir a criação de novas regras e a edição das existentes;
- 10.3.119** Permitir o correlacionamento de eventos e alerta com dados existentes em listas (watchlist), criação de novas listas e edição das existentes, tanto de forma automatizada quanto manual;
- 10.3.120** Deve ter capacidade de sumarizar múltiplos alertas idênticos automaticamente;
- 10.3.121** Permitir execução de regras agendadas, que rodam em frequência e horário específico, sem ficarem ativas em tempo real;
- 10.3.122** Reinserir no próprio fluxo de correlacionamento os alertas gerados a partir de regras de correlação, visando correlacionar este alerta como novos eventos e/ou outros alertas no intuito de detectar padrões mais complexos de ameaças ou violações de conformidade;
- 10.3.123** Priorizar os eventos e alertas com base pelo menos nos critérios de severidade do evento e criticidade do ativo;
- 10.3.124** Armazenar os eventos, alertas e incidentes na base de dados da solução de forma indexada;
- 10.3.125** Deve implementar funcionalidade de agendar relatórios de segurança em múltiplos perfis. Os relatórios deverão ser gerados automaticamente (agendados) com frequência e intervalo de tempo a serem definidos pela instituição, conforme perfis dos elementos gerenciados;
- 10.3.126** O sistema deverá detectar o uso indevido da rede, como tentativa de acessar arquivos que o usuário não tenha permissão;



PODER JUDICIÁRIO
CONSELHO DA JUSTIÇA FEDERAL

- 10.3.127** O sistema deverá detectar ataques como de força bruta ou exploração de alguma vulnerabilidade;
- 10.3.128** Os dados dos dispositivos do ambiente tecnológico devem ser armazenados em base de dados única (parte integrante da solução);
- 10.3.129** Deve ser capaz de realizar a classificação de alertas em níveis de criticidade;
- 10.3.130** Deve possuir mecanismos que proporcionem a exibição da informação de forma amigável e compreensível após coleta e normalização dos eventos;
- 10.3.131** Deve classificar eventos de acordo com os grupos de ativos afetados e sua criticidade para o negócio da empresa, por meio de parâmetros pré-definidos;
- 10.3.132** Permitir a categorização manual de eventos (já normalizados) inéditos não categorizados por padrão. Esta categorização deverá ser aplicada nos eventos futuros de mesma característica;
- 10.3.133** Deve permitir a identificação de anomalias a partir de eventos inéditos e através de análise histórica do comportamento de rede (flows);
- 10.3.134** Possuir arquitetura tolerante a falhas
- 10.3.135** A solução deve possuir sistema de auditoria de uso. Cada evento de auditoria deve possuir, no mínimo, os seguintes campos:
- a) Data e horário da ação executada pelo usuário;
 - b) Identificação do usuário que executou a ação;
 - c) Informação sobre a ação executada.
- 10.3.136** Deverá apresentar painéis gráficos (dashboards) com indicativos de situações diversas, facilmente configuráveis e com ferramentas que facilitem a criação pelos usuários;
- 10.3.137** Deverá permitir a fácil criação de uma vasta gama de efeitos visuais (não se limitando a relatórios pré-definidos e fixos):
- a) Tabelas;
 - b) Gráfico com agrupamento em período;
 - c) Gráficos de linhas;
 - d) Gráficos de barras;
 - e) Gráficos de área;
 - f) Gráficos de pizza;



PODER JUDICIÁRIO
CONSELHO DA JUSTIÇA FEDERAL

g) Mapas Geo – IP.

- 10.3.138** Deverá permitir para todos os gráficos, capacidade fácil mudar títulos, legendas e rótulos do eixo e as configurações;
- 10.3.139** Deverá ter capacidade de integração com as estruturas externas de visualização e opções (Qlikview, Tableau etc.) para visualizações adicionais por meio de conectores ODBC ou similares;
- 10.3.140** Capacidade de geração de relatórios Ad Hoc e compartilhamento do resultado com outros usuários;
- 10.3.141** Gerar relatórios ocultando campos sensíveis dos eventos (senhas, números de cartões de crédito, importâncias monetárias e outros similares);
- 10.3.142** Deve possuir integração com soluções de gestão de patches como, no mínimo, o Microsoft System Center Configuration Manager (SCCM);
- 10.3.143** A solução deve poder coletar dados de feeds externos;
- 10.3.144** Para a coleta de dados e feeds externos deve suportar, no mínimo, os seguintes formatos/protocolos/fontes:
- a) STIX/TAXII;
 - b) Bases de reputação de endereço IP e URL's;
 - c) Bases de índice de comprometimento (IOC) próprios do fabricante;
- 10.3.145** Para coletar de logs deve suportar, no mínimo, os seguintes métodos:
- a) Syslog (UDP, TCP e TLS);
 - b) CIFS;
 - c) FTP;
 - d) SCP;
 - e) MySQL;
 - f) MS SQL;
 - g) Postgres;
 - h) API.
- 10.3.146** Deverá permitir a procura por texto, campos pré-definidos, palavras chaves, operações booleanas e expressões regulares;



PODER JUDICIÁRIO
CONSELHO DA JUSTIÇA FEDERAL

- 10.3.147** Deverá permitir a utilização de procuras complexas através do encadeamento de comandos de consulta (pipeline format ou similar a SQL);
- 10.3.148** Deve utilizar algoritmos para verificação de integridade e autenticidade dos eventos armazenados para fins de auditoria (Ex: HMAC com SHA-2) devidamente reconhecidos como seguros
- 10.3.149** Deverá implementar dashboards com visualização de EPS de entrada, EPS de saída e utilização de CPU;
 - a) Caso a ferramenta utilize outra métrica, como GB/dia, a visualização acima deverá ser do licenciamento padrão da solução.

10.4 Serviço de Análise de Tráfego de Rede:

- 10.4.1** A solução deve possuir interface de rede dedicada para a gerência da solução em 1Gbps Ethernet (fibra ou cobre);
- 10.4.2** A solução deve possuir interface de rede dedicada para a aquisição (captura) de dados;
- 10.4.3** A solução deve permitir o uso das seguintes interfaces de rede: 1 Gbps (cobre), 1 Gbps (fibra SFP LR/ SR) e 10 Gbps (fiber SPF+LR / SR);
- 10.4.4** Deve se integrar com a ferramenta ofertada no serviço de visibilidade de logs, fluxos e informações para prover a análise e payload de pacotes trafegados na rede com o objetivo de reconstruir o tráfego e identificar ataques e possibilitar o bloqueio automatizado de ataques;
- 10.4.5** Deve possuir no mínimo as seguintes funcionalidades: coleta de pacotes, coleta de logs, geração de metadados, indexação, agregação e enriquecimento dos metadados dos coletores, correlacionamento avançado de alertas e tratamento de incidentes;
- 10.4.6** Deverá possuir retenção mínima de 6 (seis) meses, sendo que no período mínimo de 3 (três) meses os dados devem estar prontamente acessíveis ("quentes");
- 10.4.7** Permitir a correlação de eventos provenientes de logs e pacotes, devidamente estruturados em metadados;
- 10.4.8** A solução deve ser capaz de integrar a visualização de dados, metadados de logs e pacotes do tráfego de rede;
- 10.4.9** A solução deve permitir a visualização e análise dos dados capturados em formato gráfico de linha do tempo, construindo os gráficos com base no número de sessões, bytes ou pacotes;



PODER JUDICIÁRIO
CONSELHO DA JUSTIÇA FEDERAL

- 10.4.10** A solução deve permitir a visualização das sessões nos seguintes formatos: metadado, texto, hexadecimal, pacotes, reconstrução Web (HTTP), reconstrução de e-mail (SMTP) e arquivos (binários);
- 10.4.11** A solução deve armazenar todos os pacotes de forma segura;
- 10.4.12** Prover juntamente com a subscrição de atualização dos componentes da solução pelo período do contrato de suporte, o acesso à biblioteca de casos de uso do fabricante, que contenha pacotes especializados de regras, dashboards e coletores desenvolvidos pelo fabricante que permitam a implementação de correlação e monitoração avançada, sem necessidade de redesarvolvimento;
- 10.4.13** A CONTRATADA será responsável pelos serviços de implantação das novas versões e releases dos produtos por ela fornecidos como partes do objeto, bem como pela aplicação dos patches de correção e pacotes de serviço (service packs) relativos a esses produtos. Para a implantação das novas versões/releases, bem como para a aplicação dos patches, deverá ser aberto chamado de suporte técnico com nível de severidade adequado e a prestação dos serviços deve ser agendada com os responsáveis pela solução na contratante;
- 10.4.14** A solução deve possuir a capacidade de exportar e importar arquivos no formato packet capture (pcap);
- 10.4.15** Deve integrar com a solução de SIEM e ser capaz de extrair os dados de usuário e ações executadas dos eventos coletados para geração de score de risco;
- 10.4.16** A solução deverá ser capaz de processar, no mínimo, 1 Gbps (um gigabit por segundo) de volume de tráfego de rede;
- 10.4.17** A solução deve suportar a aplicação de filtros na camada de rede e de aplicação, no mínimo MAC, IP, usuário e palavras-chave;
- 10.4.18** A solução deve suportar a deciptação de tráfego SSL, por meio do uso de appliances físicos dedicados a este propósito;
- 10.4.19** A solução deve suportar a geração de hash (SHA1) para verificação de integridade dos arquivos extraídos a partir do tráfego de rede capturado;
- 10.4.20** A solução deve possuir a capacidade de extração de metadados do tráfego de dados capturado, com reconhecimento nativo de no mínimo os seguintes protocolos e aplicações: FTP, SFTP, SCP, Gtalk, H323, HTTP, HTTPS, IMAP, IRC, MAIL (RFC822), MSN, Net2Phone, NETBIOS, POP3, RDP, RTP, SIP, SMB, SMIME, SMTP, SNMP, SSH, TELNET, TNS, DNS, TORRENT, P2P, SKYPE, ARP;



PODER JUDICIÁRIO
CONSELHO DA JUSTIÇA FEDERAL

- 10.4.21** A solução deve possuir a capacidade de criação de interpretadores (parsers) para protocolos e aplicações proprietárias e/ou não conhecidas;
- 10.4.22** A solução deve possuir a capacidade de identificação de protocolo pelo conteúdo das sessões, independente da porta utilizada de comunicação;
- 10.4.23** A solução deve permitir isolar sessões de tráfegos, com identificação de conteúdo (payload) de origem e destino, para os protocolos ICMP, TCP e UDP;
- 10.4.24** A solução deve permitir a extração dos arquivos presentes no tráfego de rede capturado no formato compactado .zip e .rar;
- 10.4.25** A solução deve alertar em tempo real sobre tráfego coincidente com assinaturas pré-definidas e permitir a visualização da sessão em que a assinatura ocorreu, assim como a exportação da sessão para o formato .pcap;
- 10.4.26** A solução deve permitir a criação customizada de interpretadores (parsers) através de linguagem XML para identificação de protocolos de rede específicos;
- 10.4.27** A solução deve ser capaz de analisar tráfego IPv4 e IPv6;
- 10.4.28** A solução deve permitir a customização de um interpretador de busca, cuja função é analisar todas as sessões de rede em busca de palavras chaves ou sentenças;
- 10.4.29** A solução deve funcionar somente em modo passivo sem adicionar latência à rede durante a monitoração passiva;
- 10.4.30** A solução deve possuir discos de alto desempenho como SolidState Drives (SSDs) nos servidores físicos que realizam a indexação de metadados;
- 10.4.31** A solução deve armazenar todos os pacotes de forma segura;
- 10.4.32** A solução deve permitir a análise automatizada e ampla de malwares e suas atividades de rede;
- 10.4.33** A solução deve permitir a captura e análise de características suspeitas em arquivos de conteúdo executável na rede em tempo real;
- 10.4.34** A solução deve possuir um mecanismo de pontuação de risco no momento da análise de malwares;
- 10.4.35** A solução deve permitir a integração com Sandbox do CONTRATANTE;



PODER JUDICIÁRIO
CONSELHO DA JUSTIÇA FEDERAL

- 10.4.36** A solução deve possuir painel (dashboard) configurável que permita a rápida visualização do status da segurança e acesso granular a sessão reconstruída equivalente ao tráfego que gerou o alerta;
- 10.4.37** A solução deve possuir a capacidade de exibir visualmente os objetos trafegados pela rede sem a necessidade de manipular os dados diretamente na console ou banco de dados;
- 10.4.38** A solução deve permitir que a partir de uma informação existente em um relatório, se verifique o tráfego de rede que a gerou através de recurso de “drilldown” ;
- 10.4.39** A solução deve ser capaz de identificar a troca de extensão de arquivos (arquivo .exe enviado como .jpg) ;

11. SERVIÇO DE ORQUESTRAÇÃO, AUTOMAÇÃO E RESPOSTA (SOAR)

- 11.1** Este serviço tem o objetivo de automatizar os processos e fluxos de trabalho, a aplicação de atividades rotineiras ou de difícil execução e a **orquestração das diversas ferramentas de segurança**, sem necessidade de atuação humana.
- 11.2** A CONTRATADA deverá ser disponibilizar software para o gestão da operação de segurança (SecOps) por meio do gerenciamento do processo de identificação e avaliação de ameaças, bem como a análise e classificação de incidentes de segurança da informação.
- 11.3** A ferramenta deverá ser capaz de gerenciar eficazmente incidentes de segurança e privacidade da informação. O software de gerenciamento de incidentes de segurança deve permitir a definição de um processo abrangente desde o registro e triagem inicial de um incidente até sua resolução e prevenção.
- 11.4** A ferramenta deverá possuir interface web para a administração de catálogo de serviços, níveis de serviço e painéis de visualização de atividades (dashboards).
- 11.5** A CONTRATADA deverá promover a automação de processos e fluxos de trabalho em solução deve interativa, prática e de fácil implementação. Neste sentido, a solução deve:
 - 11.5.1** Possuir recursos gráficos de workflow interativos para criação de processos e rotinas operacionais, que permita operações como arrastar-e-soltar para o desenho dos fluxos de trabalho.
 - 11.5.2** Apresentar componente próprio para a modelagem gráfica e a automação de processos e fluxos de trabalho da solução.



PODER JUDICIÁRIO
CONSELHO DA JUSTIÇA FEDERAL

- 11.5.3** Permitir a automação de fluxos de automação de forma gráfica, incluindo estágios, tarefas paralelas ou sequenciais, regras de decisão e aprovação, sem a necessidade de programação ou alteração de código-fonte.
- 11.5.4** Possuir ferramenta de criação de formulários com campos específicos de cada processo e fluxo de trabalho, a fim de personalizar a inserção de informações e controles de acordo com a necessidade, sem a necessidade de programação ou alteração do código-fonte.
- 11.5.5** Dispensar a necessidade da criação de tabelas, colunas e campos de banco de dados na solução, ou a necessidade de programação ou alteração do código-fonte, tornando estas alterações, quando necessárias, transparentes aos operadores e administradores que implementam os fluxos de trabalho.
- 11.5.6** Permitir a criação de campos compartilhados que possam ser utilizados em quaisquer outras entidades da solução, sem a necessidade de programação ou alteração do código-fonte.
- 11.5.7** Disponibilizar recursos tecnológicos de catálogo de serviços que possibilitem a automação de processos de gestão de TI.
- 11.5.8** Permitir a customização de menus, formulários, labels, automatizações de fluxos de trabalho e processos de TI, desenvolvidos na solução, permitindo a adequação às necessidades de uso de cada usuário, sem a necessidade de programação ou alteração do código-fonte.
- 11.5.9** Permitir a criação e automação de processos e fluxos de trabalho de forma segregada e independente a fim de permitir a personalização para cada departamento.
- 11.5.10** Permitir a automação de processos e fluxos de trabalho.
- 11.5.11** Permitir a criação de painéis e dashboards com gráficos de gestão, de forma ágil e intuitiva, sem a necessidade de programação e alteração do código-fonte.
- 11.5.12** Permitir a criação de painéis e dashboards com gráficos do tipo pizza, linha, colunas, barras e tabelas dinâmicas, sem a necessidade de programação e alteração do código-fonte. E que contemple as diversas necessidades de visão gerencial com agilidade e flexibilidade de ajustes necessários.
- 11.5.13** Permitir alterações de atributos de forma dinâmica em gráficos de gestão, contidos em painéis e dashboards da solução, possibilitando a alteração de eixos, título do gráfico, legenda, escala, rótulos de dados,



PODER JUDICIÁRIO
CONSELHO DA JUSTIÇA FEDERAL

tamanho do gráfico, de forma gráfica na solução e sem a necessidade de alterações do código-fonte.

- 11.5.14** Permitir aos atendentes e solucionadores de chamados criarem seus próprios painéis e gráficos dentro da solução e compartilharem com grupos ou usuários específicos da solução, permitindo gerenciar as permissões de compartilhamento de acordo com os perfis de usuários da solução.
- 11.5.15** Permitir a criação de gráficos com informações de diferentes entidades da solução, permitindo a sobreposição e cruzamento de informações e delimitação de linhas de tendência.
- 11.5.16** Permitir que a partir de qualquer gráfico de gestão, contido em painéis e dashboards da solução, o usuário possa clicar e listar os registros relacionados com os dados contidos no gráfico (funcionalidade drill down).
- 11.5.17** Permitir ao usuário organizar os gráficos e informações, em seus painéis e dashboards de gestão, ajustando o layout e conteúdo do painel de acordo com suas necessidades.
- 11.5.18** Permitir aos usuários a configuração de painéis e dashboards agrupados por assunto e independentes entre si.
- 11.5.19** Permitir o gerenciamento de permissões por usuários e grupos para acesso aos painéis e dashboards da solução.
- 11.5.20** Permitir ao usuário organizar seus painéis e dashboards com listas de registros de seu interesse, possibilitando a escolha de colunas, realização de filtros e ordenação da lista.
- 11.5.21** Permitir a criação de painéis e dashboards com gráficos de gestão a partir de qualquer coluna do banco de dados da solução, sem a necessidade de programação e alteração do código-fonte.
- 11.5.22** Permitir a geração de relatórios, impressão e exportação para arquivos no mínimo do tipo .csv, .html, .pdf e .xml.
- 11.5.23** Prover informação em “real-time” de maneira gráfica por meio de dashboards.
- 11.5.24** Permitir configurar o envio automático e agendado de relatórios e gráficos gerenciais para grupos de usuários ou usuários específicos.



PODER JUDICIÁRIO
CONSELHO DA JUSTIÇA FEDERAL

12. SERVIÇO DE TESTES DE INVASÃO (RED TEAM)

- 12.1** 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
- 12.2** As equipes de ataque (RED TEAM) e defesa (BLUE TEAM) devem interagir e funcionar de maneira integrada. A equipe de ataque deve compartilhar seu conhecimento no sentido de indicar soluções para vulnerabilidades encontradas e a equipe de defesa deve possuir conhecimento das táticas e técnicas de ataque para que, por meio da atuação conjunta (PURPLE TEAM), aumente-se a efetividade da proteção do ambiente.
- 12.3** 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. Esses testes envolvem, necessariamente, o uso de técnicas e ferramentas específicas para tentar obter acesso não autorizado e privilegiado aos ativos e informações. 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:
- 12.3.1** OSSTMM 3 (The Open Source Security Testing Methodology Manual) ;
 - 12.3.2** ISSAF/PTF (Information Systems Security Assessment Framework);
 - 12.3.3** NIST Special Publication 800115 (Technical Guide to Information Security Testing and Assessment);
 - 12.3.4** NIST Special Publication 80042;
 - 12.3.5** (Guideline on Network Security Testing);
 - 12.3.6** OWASP TESTING GUIDE 3.0 The Open Web Application Security Project.
- 12.4** Neste documento os termos “pentest”, teste de penetração, teste de intrusão e testes de invasão, são considerados sinônimos;
- 12.5** Os alvos dos “Testes de Invasão” bem como as premissas e condições para realização dos mesmos serão, necessariamente, definidos e aprovados através de Ordem de Serviço (OS);



PODER JUDICIÁRIO
CONSELHO DA JUSTIÇA FEDERAL

- 12.6** A Contratada deverá observar que os testes de invasão serão executados internamente (qualquer ponto da rede corporativa do CONTRATANTE) E externamente (através da Internet);
- 12.7** Todas as fases dos “Testes de Invasão” serão acompanhadas e supervisionadas a critério do CONTRATANTE;
- 12.8** 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;
- 12.9** O teste de invasão deverá obedecer às seguintes fases:
- 12.9.1** Planejamento;
 - 12.9.2** Descoberta;
 - 12.9.3** Ataque;
 - 12.9.4** Relatório Teste de Invasão;
 - 12.9.5** Reunião para apresentação do relatório de recomendações e descrição das atividades executada durante o teste;
 - 12.9.6** Reavaliação, novo teste pós remediação;
 - 12.9.7** Relatório Final do Teste de Invasão.
- 12.10** **Planejamento:**
- 12.10.1** Todas as premissas, processos, atividades descritas e aprovadas na OS, inclusive os cronogramas serão detalhados e apresentados na fase de planejamento;
 - 12.10.2** Informações sobre o ambiente corporativo, utilizando-se das seguintes técnicas (podendo ser utilizadas ambas, conforme definição do escopo):
 - a) Técnica da caixa-preta (pouco ou nenhum conhecimento sobre o ambiente a ser avaliado. O ambiente deverá ser descoberto pelo especialista) ;
 - b) Técnica da caixa branca (o avaliador tem acesso irrestrito a qualquer informação que possa ser relevante ao teste) ;
 - c) Técnica da caixa cinza ou híbrida (conhecimento limitado sobre o alvo).
- 12.11** **Descoberta:**
- 12.11.1** Deverá ser utilizada, pelo menos, ferramentas de Análise de Vulnerabilidades, descritas no objeto, gestão de vulnerabilidades, além de técnicas manuais de análise de vulnerabilidade. As ferramentas



PODER JUDICIÁRIO
CONSELHO DA JUSTIÇA FEDERAL

deverão ser apresentadas para ciência e aprovação antes de sua efetiva utilização, assim como a metodologia para análise manual de vulnerabilidades;

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

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

- a) Whois e nslookup (consultas DNS) ;
- b) Sites de busca;
- c) Listas de discussão;
- d) Blogs de colaboradores;
- e) Dumpster diving ou trashing;
- f) Informações livres;
- g) Packet sniffing “passive eavesdropping”;
- h) Captura de banner.

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

- a) Port scanning (Mapeamento de rede) ;
- b) Varredura de vulnerabilidade.

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

- a) Hosts ativos na rede;
- b) Portas e serviços em execução;
- c) Serviços ativos e vulneráveis nos hosts;
- d) Sistemas operacionais;
- e) Vulnerabilidades associadas com sistemas operacionais e aplicações descobertas;
- f) Configurações feitas nos hosts sem observância de boas práticas em segurança computacional;
- g) Identificação de rotas e estimativa de impacto, caso estas sejam modificadas/desconfiguradas;
- h) Identificação de vetores de ataque e cenários para exploração;



PODER JUDICIÁRIO
CONSELHO DA JUSTIÇA FEDERAL

- i) Vulnerabilidades Detectadas (CVE);
- j) Vulnerabilidades de Alto Risco;
- k) Vulnerabilidades de Médio Risco;
- l) Vulnerabilidades de Baixo Risco;
- m) Informações a serem aplicadas na fase de ataques;

12.11.6 Dos serviços e aplicações web:

- a) Uso indevido de sistema de arquivos e arquivos temporários;
- b) Evasão de informação por configurações default de tratamento de erros;
- c) Tratamento indevido de entrada;
- d) Problemas relacionados à má configuração dos serviços;
- e) Gerenciamento inseguro de sessões web.

12.12 Ataque (exploração):

12.12.1 Quaisquer atividades com 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;

12.12.2 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;

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

- a) Violações do protocolo HTTP;
- b) SQL Injection;
- c) LDAP Injection;
- d) Cookie Tampering;
- e) CrossSite
- f) Scripting (XSS);
- g) Directory Transversal;
- h) Buffer Overflow;
- i) OS Command Execution;
- j) Command Injection;



PODER JUDICIÁRIO
CONSELHO DA JUSTIÇA FEDERAL

- k) Remote Code Inclusion;
- l) Server Side Includes (SSI) Injection;
- m) File disclosure;
- n) Information Leak;
- o) Zero day attacks;
- p) DDos (Distributed Denial of Service) ;
- q) Dos (Denial of Service) ;
- r) Contra protocolo TCP;
- s) Ataques contra a aplicação.

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

- a) Bugs em serviços, aplicativos e sistemas operacionais;
- b) SYN flooding;
- c) Fragmentação de pacotes de IP;
- d) Smurf e fraggle;
- e) Teardrop, nuke e land.
- f) Para ataques contra o protocolo TCP.

12.12.5 Sequestro de conexões;

12.12.6 Prognóstico de número de sequência do protocolo TCP.

- a) Ataque de Mitnick;
- b) Source routing.

12.12.7 Para ataques em nível da aplicação:

- a) Buffer Overflow;
- b) Problemas com o SNMP;
- c) Vírus, worms e cavalos de Tróia.

12.12.8 Injeção de Código:

- a) Ataques XSS (Crosssite Script) ;
- b) Comprometimento do acesso remoto;
- c) Manutenção de acesso;



PODER JUDICIÁRIO
CONSELHO DA JUSTIÇA FEDERAL

d) Encobrimento de rastros da invasão.

12.12.9 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 3.0 (The Open Web Application Security Project):

12.12.10 Para testes de coleta de informações, aplicar padrão: OWASPIG001, OWASPIG002, OWASPIG003, OWASPIG004, OWASPIG005 e OWASPIG006;

12.12.11 Para testes de gerenciamento de configuração, aplicar padrão: OWASPCM001, OWASPCM002, OWASPCM003, OWASPCM004, OWASPCM005, OWASPCM006, OWASPCM007, OWASPCM008;

12.12.12 Para testes de autenticação, aplicar padrão: OWASPAT001, OWASPAT002, OWASPAT003, OWASPAT004, OWASPAT005, OWASPAT006, OWASPAT007, OWASPAT008, OWASPAT009 e OWASPAT010;

12.12.13 Para testes de gerenciamento de sessão, aplicar padrão: OWASPSM001, OWASPSM001, OWASPSM002, OWASPSM003, OWASPSM004, OWASPSM005;

12.12.14 Para testes de autorização, aplicar padrão: OWASPAZ001, OWASPAZ002 e OWASPAZ003;

12.12.15 Para testes de negócio lógico, aplicar padrão: OWASPBL001;

12.12.16 Para testes de validação de dados, aplicar padrão: OWASPDV001; OWASPDV002, OWASPDV003, OWASPDV004, OWASPDV005, OWASPDV006, OWASPDV007, OWASPDV008, OWASPDV009, OWASPDV010, OWASPDV011, OWASPDV012, OWASPDV013, OWASPDV014, OWASPDV015 e OWASPDV016;

12.12.17 Para testes de negação de serviços, aplicar padrão: OWASPDS001, OWASPDS002, OWASPDS003, OWASPDS004, OWASPDS005, OWASPDS006, OWASPDS007 e OWASPDS008;

12.12.18 Para testes de serviços web, aplicar padrão: OWASPWS001, OWASPWS002, OWASPWS003, OWASPWS004, OWASPWS005, OWASPWS006 e OWASPWS007.

12.12.19 Observa-se que o resultado de cada teste deverá vir acompanhado de relatórios contendo:

a) Referência-base (Whitepaper);



PODER JUDICIÁRIO
CONSELHO DA JUSTIÇA FEDERAL

- b) Ameaças encontradas;
- c) Riscos levantados ao ambiente computacional;
- d) Contramedidas para mitigar as ameaças encontradas.

12.13 Relatório de Teste de Invasão:

12.13.1 Deverá ser elaborado 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:

12.13.2 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.

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

- a) Detalhes da infraestrutura descoberta, alvo dos testes de invasão;
- b) Equipamentos e recursos demandados para este teste;
- c) Tipos de ataque;
- d) Prazos (janelas de tempo para execução dos testes) ;
- e) Pontos de contato da contratada (responsáveis para tratamento de questões abordadas nos testes) ;
- f) Tipos de testes realizados pelos especialistas em segurança da informação;
- g) Confirmação ou refutação de a existência de vulnerabilidades;
- h) Documentação sobre o caminho utilizado para exploração, avaliação do impacto e prova da existência da
- i) vulnerabilidade;
- j) Obtenção de acesso e possível escalada de privilégios;
- k) Detalhamento da metodologia do ataque;
- l) Recomendações para sanar riscos e vulnerabilidades.

12.13.4 Reunião para apresentação do relatório de recomendações e descrição das atividades executada durante o teste;



PODER JUDICIÁRIO
CONSELHO DA JUSTIÇA FEDERAL

12.13.5 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.

12.14 Relatório Final do Teste de Invasão:

12.14.1 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.

12.14.2 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.

12.15 Atividades de Apoio:

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

- a) PLANO DE TRABALHO com o detalhamento do escopo dos testes e cronograma de execução;
- b) APRESENTAÇÃO INICIAL das ações a serem aplicadas pela Contratada;
- c) RELATÓRIOS DE ACOMPANHAMENTO SEMANAIS do plano de trabalho.

12.16 Periodicidade de execução:

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

12.16.2 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:

- a) Atividades do Pentest;
- b) Entrega do relatório “Teste de Invasão”;
- c) Ações corretivas das vulnerabilidades apontadas pela Contratada e aplicadas pelo CONTRATANTE;
- d) Reavaliação Pentest, caso necessário;
- e) Entrega do relatório “Relatório Final do Teste de Invasão”.



PODER JUDICIÁRIO
CONSELHO DA JUSTIÇA FEDERAL

- 12.16.3** O CONTRATANTE deverá aplicar, no que couber, 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”.

13. DOS PERFIS PROFISSIONAIS

- 13.1** A CONTRATADA deverá dimensionar adequadamente a sua equipe de profissionais de forma a atingir os níveis de serviço estabelecidos no contrato;
- 13.2** Todos os profissionais deverão possuir qualificação plena e conhecimento técnico compatível com o complexidade das demandas a serem atendidas;
- 13.3** A formação da equipe de profissionais é de exclusiva responsabilidade da CONTRATADA e serão gerenciados exclusivamente pelo PREPOSTO da empresa;
- 13.4** Os profissionais deverão conhecer o funcionamento dos negócios internos da STI, e respectivas áreas do CJF, bem como executar os procedimentos de acordo com as regras de segurança da informação;
- 13.5** Os profissionais deverão utilizar vestimenta compatível com a utilizada pelos servidores do CJF e portar crachá de identificação durante toda a prestação de serviço;
- 13.6** Durante a execução dos serviços, a CONTRATADA se obriga, durante a execução do Contrato, a manter todos os profissionais com as qualificações abaixo especificadas:

13.6.1 Formação:

- a) 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.

13.6.2 Certificações:

- a) Serviço de Operação e Atendimento a Requisições:
- CompTIA Security+;
 - Fortinet Network Security Expert 4 – NSE4;



PODER JUDICIÁRIO
CONSELHO DA JUSTIÇA FEDERAL

- FortiWeb Specialist Exam;
- Certificação ITILv3 Foundation.
- b) Serviço de Gestão de Incidentes de Segurança:
 - CompTIA Cybersecurity Analyst (CySA+);
 - Certified Ethical Hacker – CEH;
 - Fortinet Network Security Expert 4 – NSE4;
 - FortiWeb Specialist Exam;
 - Certificação ITILv3 Foundation.
- c) Serviço de Gestão de Vulnerabilidades:
 - Certificação dos produtos ofertados;
 - Certificação ITILv3 Foundation.
- d) Serviço de Monitoramento e Visibilidade de Ataques Cibernéticos:
 - Certificação dos produtos ofertados;
 - Certificação ITILv3 Foundation.
- e) Serviço de Automação de Processos e Fluxos de Trabalho:
 - Certificação dos produtos ofertados;
 - Certificação ITILv3 Foundation.
- f) Serviço de Testes de Invasão:
 - EC-Concil Licensed Penetration Tester – LPT ou IACRB Certified Expert Penetration Tester – CEPT ou GIAC Exploit Researcher and Advanced Penetration Tester – GXPN ou Offensive Security Certified Professional – OSCP;
 - Certificação ITILv3 Foundation.

13.6.3 Capacitação:

- a) Serviço de Operação e Atendimento a Requisições e Serviço de Gestão de Incidentes de Segurança:
 - Trend Micro Deep Security, com certificado de participação em curso oficial do fabricante de no mínimo 16 (dezesesseis) horas;
 - Trend Micro OfficeScan ou Apex One, com certificado de participação em curso oficial do fabricante de no mínimo 16 (dezesesseis) horas;



PODER JUDICIÁRIO
CONSELHO DA JUSTIÇA FEDERAL

13.7 A comprovação dos requisitos deverá ser composta de:

13.7.1 Documento digitalizado com apresentação documento original, cópia autenticada ou documento digital em que seja possível comprovar a autenticidade em site do emissor.

13.7.2 Todos os documentos apresentados estarão sujeitos à diligência do CONTRATANTE para fins de confirmação das informações prestadas;

13.8 A CONTRATADA deverá promover, no prazo máximo de 3 (três) meses, a atualização das certificações de seus profissionais caso haja 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.

13.9 Caso uma certificação não seja mais válida, será aceita a nova certificação que substituiu a anterior.

14. DO FATURAMENTO E DO PAGAMENTO

14.1 Os pagamentos 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;

14.2 A nota fiscal deverá apresentada até o quinto dia útil do mês subsequente à prestação do serviço;

14.3 A fim de que o CONTRATANTE possa efetuar o pagamento, a CONTRATADA deverá apresentar nota fiscal constando a indicação do banco, da agência e do número da conta-corrente onde deverá ser efetuado o crédito;

14.4 O CONTRATANTE, deverá efetuar a análise dos relatórios gerenciais de serviços em até cinco dias úteis do recebimento destes. Após manifestação formal do Contratante, a CONTRATADA deverá emitir as notas fiscais de cobrança em até 10 (dez) dias úteis da manifestação;

14.5 Obedecendo a pontuação atribuída no Anexo I para cada inadimplemento, o CONTRATANTE **aplicará glosa de 1% (um por cento) sobre o valor da nota fiscal a cada 15 pontos**, limitada a glosa total ao percentual máximo de 30% (trinta por cento) do valor mensal previsto em contrato, devendo o CONTRATANTE cientificar à CONTRATADA sobre as razões que ensejaram o desconto;



PODER JUDICIÁRIO
CONSELHO DA JUSTIÇA FEDERAL

- 14.6** A nota de cobrança emitida pela CONTRATADA deverá ser atestada em até 7 (sete) dias úteis pelo Gestor do contrato e encaminhada para a área financeira efetuar o pagamento, acompanhada dos relatórios gerenciais de serviços e documentação comprobatória do não atendimento dos resultados ou níveis de serviço exigidos;
- 14.7** No caso de discordância das glosas aplicadas, a CONTRATADA deverá apresentar o recurso que será analisado pela área administrativa. Se a decisão da Administração for favorável ao recurso da CONTRATADA, esta emitirá a nota de cobrança adicional para que seja efetuado o pagamento referente ao valor glosado;
- 14.8** Apresentada a nota fiscal de cobrança na forma aqui estabelecida, terá o CONTRATANTE o prazo máximo de 10 (dez) dias úteis para efetuar o pagamento, contados a partir do atesto;
- 14.9** Para os inadimplimentos que não estão previstos no Anexo I, o CONTRATANTE abrirá processo administrativo e seguirá o rito definido nas SANÇÕES ADMINISTRATIVAS;
- 14.10** Deverá ser encaminhado mensalmente, em conjunto com a fatura, a seguinte documentação que será analisada e aprovada pelo representante da área administrativa (Fiscal Administrativo do Contrato). Os documentos comprobatórios listados nos itens abaixo são necessários apenas para os colaboradores que prestaram serviço nas dependências do CJF por mais de 15 (quinze) dias no mês em questão:
- 14.10.1** Comprovação de pagamento de salários do mês da prestação dos serviços objeto de faturamento, mediante apresentação de folha de pagamento específica, em que conste como tomador o Conselho da Justiça Federal, acompanhada de cópias dos recibos de depósitos bancários ou contracheques assinados pelos profissionais;
- 14.10.2** Planilha de composição de custo, com a discriminação dos custos de mão-de-obra;
- 14.10.3** Planilha formadora de custos de mão-de-obra, nos termos da IN n.05/2017 e IN n.07/2018 do Ministério do Planejamento, Desenvolvimento e Gestão;
- 14.10.4** Guia de Recolhimento do Fundo de Garantia do Tempo de Serviço e Informações à Previdência Social – GFIP específica, em que conste como tomador o CJF, relativa ao mês da prestação de serviço;
- 14.10.5** Comprovante de entrega de benefícios suplementares (vale transporte, vale-alimentação etc.), a que estiver obrigada, por força de lei ou de convenção ou acordo coletivo de trabalho;



PODER JUDICIÁRIO
CONSELHO DA JUSTIÇA FEDERAL

- 14.10.6** Comprovação do pagamento do 13º salário;
- 14.10.7** Relação mensal de prestadores referente ao mês da prestação dos serviços, na qual constem todos os empregados que atuaram no Conselho, mesmo que transitoriamente em substituição à mão de obra faltante, com discriminação do período de atuação;
- 14.10.8** Folha de pagamento do mês de referência constando todos os funcionários que prestaram serviço no Conselho, ou contracheque individual de cada funcionário, e comprovante de depósito nominal.
- 14.10.9** Guia de Recolhimento do FGTS e Informações à Previdência Social (GFIP), referente ao mês da prestação dos serviços, individualizada por tomador (CJF);
- 14.10.10** Quando ocorrer demissão de pessoal, será necessário o encaminhamento dos Termos de Rescisão de Contrato de Trabalho, integrando-se à documentação exigida para pagamento da nota fiscal.
- 14.10.11** Quando exigível, os Termos de Rescisão deverão estar homologados pelo sindicato que assiste a categoria profissional do trabalhador.
- 14.11** Em conformidade com a Instrução Normativa CJF-INN-2016/00001 e as Resoluções nº 169/2013 e nº 183/2013, do Conselho Nacional de Justiça (CNJ), na ocasião do pagamento mensal, serão retidos da CONTRATADA, e transferidos para conta-depósito bloqueada para movimentação os custos relativos às provisões de férias e adicional de férias; ao 13º salário; à multa do FGTS por dispensa sem justa causa; à incidência dos encargos previdenciários e FGTS sobre férias, 1/3 constitucional e 13º salário; e ao valor das despesas com a cobrança de abertura e de manutenção da referida conta vinculada, caso necessário.
- 14.11.1** Os valores depositados na conta-depósito, bloqueada para movimentação, deixarão de compor o valor mensal devido à empresa.
- 14.11.2** Os valores retidos da CONTRATADA, referentes às provisões com férias e abono de férias, 13º salário, multa do FGTS, e incidência dos encargos previdenciários e FGTS sobre férias, 1/3 constitucional e 13º salário, serão liberados somente quando da ocorrência e do pagamento das verbas trabalhistas, com prévia autorização do CONTRATANTE, na forma prevista na Instrução Normativa CJF-INN-2016/00001 e nas Resoluções CNJ nº 169/2013, 183/2013 e 248/2018.
- 14.12** Para fins de conformidade com a Instrução Normativa CJF-INN-2016/00001 e as Resoluções CNJ nº 169/2013 e nº 183/2013, entende-se como mão de obra



PODER JUDICIÁRIO
CONSELHO DA JUSTIÇA FEDERAL

residente (e, portanto, suscetível à retenção tratada no item anterior), todos os funcionários da CONTRATADA que prestem serviço nas dependências do CJF;

- 14.13** Os valores retidos na conta-depósito bloqueada para movimentação serão liberados na forma prevista na Instrução Normativa CJF-INN-2016/00001 e nas Resoluções CNJ nº 169/2013, 183/2013 e 248/2018.

15. DA EXECUÇÃO DO CONTRATO

PRAZO E EXECUÇÃO DOS SERVIÇOS

- 15.1** A CONTRATADA deverá iniciar a prestação dos serviços objeto deste termo, de acordo com os cronogramas apresentados no Anexo V;
- 15.2** Para execução dos serviços, será implementado método de trabalho baseado no conceito de delegação de responsabilidade. Esse conceito define o CONTRATANTE como responsável pela gestão do contrato e pela atestação da aderência aos padrões de qualidade exigidos dos serviços entregues e a CONTRATADA como responsável pela execução dos serviços e gestão dos profissionais a seu cargo;
- 15.3** A CONTRATADA será responsável pela execução dos serviços e seu acompanhamento diário da qualidade e dos níveis de serviço alcançados com vistas a efetuar eventuais ajustes e correções. Quaisquer problemas que venham a comprometer o bom andamento dos serviços ou o alcance dos níveis de serviço estabelecidos devem ser imediatamente comunicados por escrito ao CONTRATANTE;
- 15.4** Após a assinatura do contrato, será emitida Ordem de Serviço de Transição – OST com o objetivo de viabilizar a transferência de conhecimentos e o repasse dos serviços à nova CONTRATADA;
- 15.5** A CONTRATADA deverá apresentar no prazo máximo de 10 (dez) dias corridos a partir da emissão da Ordem de Serviço de Transição - OST, carta de apresentação juntamente com os documentos comprobatórios (certificados oficiais) contendo os respectivos dados pessoais e informações quanto à habilitação e qualificação profissional de todos os seus profissionais que serão alocados na execução de serviços no CONTRATANTE;
- 15.6** Quando da apresentação dos documentos comprobatórios de qualificação, a CONTRATADA deverá observar atenciosamente à qualificação exigida, conforme descrito no Item 13 - Dos perfis profissionais. Caso a documentação não atenda às exigências deste item, a CONTRATADA deverá apresentar



PODER JUDICIÁRIO
CONSELHO DA JUSTIÇA FEDERAL

documentação de um novo profissional que atenda as exigências, dentro do prazo estabelecido, antes do início das atividades;

15.7 Para fins de comprovação de atendimento aos requisitos de qualificação profissional serão aceitos:

15.7.1 Cópia autenticada de certificados ou diplomas que comprovem a conclusão dos cursos exigidos. No caso dos cursos de nível médio e/ou superior deverão ser apresentados os diplomas;

15.7.2 Todos os documentos apresentados estarão sujeitos à diligência do CONTRATANTE para fins de confirmação das informações prestadas;

15.7.3 Caso uma certificação não seja mais válida, será aceita a nova certificação que substituiu a anterior;

15.7.4 As certificações técnicas exigidas devem estar válidas;

15.8 O CJF poderá a qualquer momento recusar o atendimento dos serviços por profissionais que não atendam aos requisitos de qualificação especificados. A CONTRATADA terá o prazo de 2 (dois) dias úteis a contar da data de recusa para apresentar a documentação do novo profissional;

15.9 Será considerado como período de transição, os 10 (dez) dias corridos contados a partir da entrega da documentação completa da equipe de profissionais na forma dos subitens anteriores. Neste período a CONTRATADA antecessora atuará conjuntamente com a recém-CONTRATADA, priorizando a documentação e retenção de conhecimento para a continuidade dos serviços de TI e a mitigação de impacto nas atividades dos usuários de tais serviços;

15.10 A CONTRATADA deverá iniciar a prestação dos serviços em; no máximo; 20 (vinte) dias corridos após a emissão da Ordem de Serviço – OS.

15.11 Não ocorrerá período de transição caso não ocorra a substituição da empresa prestadora de serviços. A prestação dos serviços deverá seguir o Cronograma de Atividades, conforme Anexo V;

15.12 O edital de contratação dos serviços deverá estabelecer que o contrato será considerado rescindido, bem como serão aplicadas as sanções contratuais, caso a empresa vencedora deixe de apresentar:

15.12.1 Plano de Operacionalização dos Serviços, no prazo de 5 (cinco) dias corridos após a emissão da Ordem de Serviço de Transição - OST, contendo o detalhamento das ações necessárias para a absorção dos conhecimentos, e repasse dos serviços; ou,

15.12.2 Documentação com a relação completa dos profissionais que prestarão serviço, no prazo máximo de 10 (dez) dias corridos após



PODER JUDICIÁRIO
CONSELHO DA JUSTIÇA FEDERAL

a emissão da Ordem de Serviço de Transição - OST, acompanhada das devidas comprovações de qualificação e experiência exigidas para cada perfil estabelecido no Termo de Referência.

- 15.13** O período inicial de 90 (noventa) dias após a emissão da Ordem de Serviço Rotineira - OSR, será considerado como **período de estabilização** da operação dos serviços, durante o qual os indicadores de serviço não atingidos terão aplicadas as glosas da tabela do Anexo I conforme os seguintes critérios:
- 15.13.1** Nos primeiros 30 (trinta) dias: aplicar-se-á efetivamente 25% (vinte e cinco por cento) dos pontos previstos na tabela do Anexo I para cada ocorrência de indicador de serviço não atingido;
 - 15.13.2** Do 31º ao 60º dia: aplicar-se-á efetivamente 50% (cinquenta por cento) dos pontos previstos na tabela do Anexo I para cada ocorrência de indicador de serviço não atingido;
 - 15.13.3** Do 61º ao 90º dia: aplicar-se-á efetivamente 75% (setenta e cinco por cento) dos pontos previstos na tabela do Anexo I para cada ocorrência de indicador de serviço não atingido;
 - 15.13.4** Após 90 (noventa): aplicar-se-ão integralmente os pontos previstos na tabela do Anexo I para cada ocorrência de indicador de serviço não atingido.
- 15.14** Caso haja prorrogação da vigência contratual, não haverá novo período de estabilização;
- 15.15** Ao final do contrato de prestação dos serviços, a empresas CONTRATADA deverão fornecer, pelo período 90 (noventa) dias corridos, todas as informações necessárias à transição para a nova CONTRATADA, além de elaborar e atualizar toda a documentação que por ventura não tenha sido devidamente gerada ou atualizada durante o período de vigência do contrato;
- 15.16** A CONTRATADA deverá responsabilizar-se pela transição inicial e final dos serviços, absorvendo as atividades de forma a documentá-las minuciosamente para que os repasses de informações, conhecimentos e procedimentos, no final dos contratos, aconteçam de forma precisa e responsável;
- 15.17** Quando houver necessidade de qualquer alteração na equipe de profissionais que prestam o serviço no CONTRATANTE, a CONTRATADA deverá apresentar os documentos comprobatórios de qualificação deste(s) profissional(ais) antes do início de suas atividades no CONTRATANTE.



PODER JUDICIÁRIO
CONSELHO DA JUSTIÇA FEDERAL

- 15.18** Em conformidade com a pela Instrução Normativa CJF-INN-2016/00001 e as Resoluções CNJ nº 169/2013 e nº 183/2013, o gestor do contrato irá acompanhar a presença dos funcionários da CONTRATADA alocados para prestar serviço nas dependências do CJF. Para tal, será utilizado um sistema de ponto eletrônico da CONTRATADA. O registro do ponto neste sistema será obrigatório para todos os funcionários da CONTRATADA que prestarem serviço nas dependências do Conselho;
- 15.19** Para a realização da monitoração proativa do ambiente tecnológico, a CONTRATADA deverá oferecer serviço SMS (Short Message Service) ou mensageria instantânea (WHATSAPP), para que sejam enviadas mensagens aos prestadores de serviço e aos gestores de TI conforme a geração de alertas dos softwares de monitoração. É de responsabilidade da CONTRATADA o custo da contratação deste serviço;
- 15.20** Todos os profissionais da CONTRATADA alocados para a prestação dos serviços objeto deste Termo de Referência deverão ter vínculo com a CONTRATADA, baseado na CLT.

ENCAMINHAMENTO DE DEMANDAS

- 15.21** Os serviços deverão ser executados somente após a emissão de Ordens de Serviços, com a obrigatória autorização pelo CONTRATANTE;
- 15.22** As Ordens de Serviços deverão ser classificadas pelo CONTRATANTE, conforme nível e continuidade de execução:
- 15.22.1** Transição: entendida como o processo de transferência dos conhecimentos e competências necessárias para prover a continuidade dos serviços contratados ou executados;
 - 15.22.2** Rotineira: atividades contínuas, realizáveis periodicamente, emitidas para execução durante a vigência do contrato. Podendo, mediante realinhamento, ter novas atividades inseridas ou excluídas no decorrer da vigência contratual, quando passará a vigorar nova versão de OSR;
 - 15.22.3** Exclusiva: atividades de natureza não contínua, emitidas a partir da demanda do CONTRATANTE.
- 15.23** Nas Ordens de Serviços deverão constar:
- 15.23.1** Número de controle: identificação em ordem sequencial;
 - 15.23.2** Área demandante: que deverá assinar a solicitação e o aceite e contabilização periódica das atividades, para efeito dos pagamentos;



PODER JUDICIÁRIO
CONSELHO DA JUSTIÇA FEDERAL

- 15.23.3** Objetivo da tarefa: definição das expectativas e justificativas para realização das atividades;
 - 15.23.4** Data de início e conclusão das atividades (exceto rotineira): definição do período de realização, inclusive dos períodos e horários realizáveis para serviços que impactem com os trabalhos de usuários;
 - 15.23.5** Listagem das atividades a serem realizadas, especificadas, quantificadas e classificadas conforme complexidade;
 - 15.23.6** Resultado e Nível de Qualidade definido para a tarefa;
 - 15.23.7** Glosa e Penalidades, em caso de descumprimento, e de acordo com a previsão contratual;
 - 15.23.8** Responsáveis pela fiscalização e autorização no CONTRATANTE;
 - 15.23.9** Responsável pelo aceite na CONTRATADA.
- 15.24** Atestação técnica:
- 15.24.1** A Ordem de Serviço somente poderá ser encerrada quanto todos os objetivos propostos forem plenamente atingidos, e todos os produtos e serviços realizados e entregues com a qualidade demandada e devidamente atestada pelo demandante e pelo gestor do CONTRATANTE;
 - 15.24.2** Antes do fechamento de cada OS a CONTRATADA consultará o representante indicado pelo CONTRATANTE, que avaliará e atestará o serviço realizado;
 - 15.24.3** Uma requisição de serviço ou incidente encerrado sem anuência do CONTRATANTE ou sem que tenha sido de fato resolvido será reaberto e os prazos serão contados a partir da abertura original da requisição de serviço ou incidente, inclusive para efeito de aplicação das sanções previstas.

NÍVEIS MÍNIMOS DE SERVIÇOS EXIGIDOS

- 15.25** Os níveis mínimos de serviços são critérios objetivos e mensuráveis que visam aferir e avaliar diversos fatores relacionados com os serviços contratados, quais sejam: qualidade, desempenho, disponibilidade, abrangência/cobertura e segurança;
- 15.26** Os níveis mínimos de serviços estão detalhados no Anexo I – Níveis Mínimos de Serviço;



PODER JUDICIÁRIO
CONSELHO DA JUSTIÇA FEDERAL

- 15.27** O não atingimento de um mesmo nível de serviços durante 3 (três) meses consecutivos ou 5 (cinco) meses intervalados, em um período de 12 (doze) meses, ensejará a execução das Sanções Administrativas previstas no contrato;
- 15.28** A CONTRATADA sofrerá glosa de 1% (um por cento), sobre o valor da fatura, a cada 15 pontos ou percentual proporcional ao número de pontos, levando em consideração a relação: glosa de 1% a cada 15 pontos;
- 15.29** As metas devem ser medidas do primeiro ao último dia de cada mês;
- 15.30** A meta exigida representa o parâmetro de valor exato (=), limite máximo (<=) ou limite mínimo (>=) que deve ser alcançado pela CONTRATADA para cada um dos indicadores;
- 15.31** Os tempos serão contados a partir do recebimento da solicitação do cliente. No caso da contagem em dias, a contagem é efetuada dia a dia, incluindo o primeiro e o último dia;
- 15.32** No caso da resolução de incidentes, se o mesmo não tiver a sua causa raiz conhecida, ou seja, existe um problema a ser resolvido, a CONTRATADA é obrigada a aplicar uma solução de contorno na resolução do incidente para que o serviço volte à sua operação padrão;
- 15.33** Os níveis de serviço serão mensurados de forma automatizada e não poderão ser manipulados pela CONTRATADA;
- 15.34** A CONTRATADA se responsabilizará somente pelos índices que reflitam as requisições de serviços e incidentes designados a ela, não poderá ser responsabilizada por chamados pendentes de fornecedores/prestadores de serviços externos ou encaminhados a outros níveis, ou situações que dependam de terceiros, que, desta forma, não poderão ser computados;
- 15.35** O termo “Hora do restabelecimento” refere-se a hora em que o incidente de indisponibilidade foi efetivamente resolvido;
- 15.36** Por requisições de serviço e incidentes reabertos entende-se que são requisições de serviço ou incidentes que foram dados como resolvidos, porém os mesmos ainda permanecem pendentes de resolução;
- 15.37** Por horário normal de produção entende-se sendo o período entre 09:00 e 20:00, de segunda à sexta-feira, excetuando-se os feriados;
- 15.38** Sobre o índice de supervisão e intervenção proativa:
- 15.38.1** A manutenção proativa visa detectar com antecedência os possíveis problemas que possam vir a ocorrer devido à necessidade de suporte, como aplicação de *patches*, correções de *firmware*, ou



PODER JUDICIÁRIO
CONSELHO DA JUSTIÇA FEDERAL

algum outro dispositivo que possa impactar no desempenho ou disponibilidade dos Sistemas Monitorados pela CONTRATADA, podendo ser visualizados mediante acompanhamento e análise diária de desempenho e produção dos recursos e também através de testes rotineiros de *stress* e carga;

- 15.38.2** Deverão ser analisados em tempo real os desempenhos dos serviços críticos inserindo as manutenções e os suportes necessários de maneira a proporcionar a continuidade e disponibilidade dos serviços. Diariamente deverão ser analisados os registros internos dos *hardwares* e *softwares* para avaliação e detecção de intervenções necessárias, submetendo-os à CONTRATANTE para programação das intervenções que permitirem agendamento;
- 15.38.3** É obrigação da CONTRATADA efetuar as intervenções necessárias em tempo de produção para sanar os erros apresentados nesta fase e que sejam de sua competência. Se as intervenções propostas forem para melhoria de desempenho ou compatibilização de ambiente e permitirem agendamento deverão ser submetidas para aprovação da CONTRATANTE antes de execução.

SANÇÕES ADMINISTRATIVAS

15.39 O CONTRATANTE poderá aplicar as seguintes sanções: advertência, multa, impedimento de licitar e contratar com CJF, e será descredenciada do SICAF, pelo prazo de até cinco anos, de acordo com a Lei 10.520/2002, Decreto 10.024/2019 e Lei 8.666/1993, assegurados o contraditório e a ampla defesa:

- 15.39.1** Advertência;
- 15.39.2** MULTA MORATÓRIA de 0,5% (zero vírgula cinco por cento) sobre o valor mensal do contrato, por dia de atraso **na apresentação da nota fiscal de faturamento**, de acordo com os níveis de serviços e eventuais glosas apuradas pelo CONTRATANTE;
- 15.39.3** MULTA MORATÓRIA de 0,5% (zero vírgula cinco por cento) sobre o valor mensal do contrato, por dia de atraso **na apresentação da relação de profissionais** que prestarão os serviços alocados no CONTRATANTE;
- 15.39.4** MULTA MORATÓRIA de 0,5% (zero vírgula cinco por cento) do valor mensal do contrato por dia de atraso decorrido em **caso de descumprimento do prazo** estabelecido na cláusula DO



PODER JUDICIÁRIO
CONSELHO DA JUSTIÇA FEDERAL

CONTINGENCIAMENTO DOS ENCARGOS TRABALHISTAS referente a abertura da conta-depósito vinculada;

- 15.39.5** MULTA MORATÓRIA de 0,5% (zero vírgula cinco por cento) sobre o valor mensal do contrato por ocorrência em que o **profissional descumprir as exigências de vestimenta**, conforme determinado na PORTARIA CJF-POR-2018/00129 ou norma que vier a sucedê-la;
- 15.39.6** MULTA MORATÓRIA de 0,5% (zero vírgula cinco por cento) sobre o valor mensal do contrato por ocorrência em que o **profissional descumprir a norma sobre o controle de acesso**, a circulação e a permanência de pessoas no Conselho da Justiça Federal, conforme determinado na Portaria Ministro Presidente nº 34 de 02/02/2017 ou norma que vier a sucedê-la;
- 15.39.7** MULTA MORATÓRIA – de 1% (um por cento) sobre o valor mensal do contrato, a cada ocorrência em que a CONTRATADA:
- a) Substituir profissional sem formalizar à CONTRATANTE;
 - b) Deixar de afastar profissional que se conduza de modo inconveniente ou que não respeite as normas do CJF ou que não atenda às necessidades, num período de 24 (vinte e quatro) horas corridas a contar da notificação do CONTRATANTE;
 - c) Deixar de alocar um novo profissional em caso de substituição, num período de 5 (cinco) dias úteis a contar da notificação do CONTRATANTE quando da substituição;
- 15.39.8** MULTA MORATÓRIA – de 1,5% (um vírgula cinco por cento) sobre o valor mensal do contrato, a cada ocorrência em que a CONTRATADA:
- a) Por motivo de negligência, imprudência ou imperícia na execução das atividades contratuais, causar qualquer dano físico ou lógico aos equipamentos da CONTRATANTE;
 - b) Descumprir Política, Norma ou Procedimento de Segurança da Informação do CONTRATANTE
 - c) Deixar de comunicar formalmente à CONTRATANTE sobre o desligamento de prestador de serviço (profissional que prestava serviço nas dependências do CJF e/ ou remotamente).
- 15.39.9** MULTA MORATÓRIA de 10% (dez por cento) do valor mensal do contrato pelo não atingimento de um mesmo nível de serviço previsto



PODER JUDICIÁRIO
CONSELHO DA JUSTIÇA FEDERAL

no ANEXO I durante 3 (três) meses consecutivos ou 5 (cinco) meses alternados, apurados em um período de 12 (doze meses);

15.39.10 MULTA MORATÓRIA de 20% (vinte por cento) do valor mensal do contrato pelo não atingimento de um mesmo nível de serviço previsto no ANEXO I, durante 6 (seis) meses consecutivos ou 10 (cinco) meses não consecutivos, apurados em um período de 12 (doze meses);

15.39.11 MULTA COMPENSATÓRIA de 10% (dez por cento) do valor total do contrato, em caso de INEXECUÇÃO PARCIAL das obrigações contratuais;

15.39.12 MULTA COMPENSATÓRIA de 20% (vinte por cento) do valor total do contrato, em caso de inexecução total das obrigações contratuais;

15.39.13 Os indicadores fora das metas exigidas no ANEXO I – Níveis Mínimos de Serviço serão considerados como INEXECUÇÃO DOS SERVIÇOS MENSAIS do contrato conforme a tabela abaixo, sem prejuízo da aplicação da glosa referente ao indicador não atingido:

PORCENTAGEM ALCANÇADA DO NÍVEL DE SERVIÇO EM RELAÇÃO A META EXIGIDA NO ANEXO I do Termo de Referência	TIPO DE INEXECUÇÃO DOS SERVIÇOS MENSAIS
50% A 69,9%	PARCIAL
0% A 49,9%	TOTAL

Será aplicada:

- MULTA MORATÓRIA de 10% (dez por cento) do valor mensal do contrato, em caso de INEXECUÇÃO PARCIAL DOS SERVIÇOS MENSAIS do contrato; ou
- MULTA MORATÓRIA de 20% (vinte por cento) do valor mensal do contrato, em caso de INEXECUÇÃO TOTAL DOS SERVIÇOS MENSAIS do contrato;

15.39.14 Suspensão temporária do direito de participar em licitação e impedimento de contratar com a Administração pelo prazo no contrato;

15.39.15 Declaração de inidoneidade para licitar ou contratar com a União, Estados, Distrito Federal ou Municípios, quando a CONTRATADA deixar de cumprir as obrigações assumidas, praticando falta grave, dolosa ou revestida de má-fé;



PODER JUDICIÁRIO
CONSELHO DA JUSTIÇA FEDERAL

- 15.40** As sanções de multa podem ser aplicadas à CONTRATADA juntamente com a de advertência, suspensão temporária do direito de participar de licitação e impedimento de contratar com o Conselho da Justiça Federal e declaração de inidoneidade para licitar ou contratar com a Administração Pública, descontando-a do pagamento a ser efetuado.

16. VIGÊNCIA

- 16.1** O Contrato terá vigência de 24 (vinte e quatro) meses a contar da data do início da prestação dos serviços, podendo ser prorrogado até o limite de 60 (sessenta) meses, nos termos da Lei.
- 16.2** Caso ocorra a prorrogação da vigência do Contrato, observadas as disposições constantes no art. 57, da Lei n.º 8.666/1993, a CONTRATADA deverá providenciar a devida renovação da garantia prestada, com validade de 3 (três) meses após o término da vigência contratual, tomando-se por base o valor atualizado do Contrato.

17. REPACTUAÇÃO E REAJUSTE

- 17.1** Do reajuste dos serviços e dos insumos:

- 17.1.1** Em caso de prorrogação do contrato será adotada, para fins de reajuste para os serviços em que não houver a alocação continuada de profissionais, bem como os preços de eventuais equipamentos, softwares e demais insumos utilizados para a prestação dos serviços previstos no contrato e que tenham sido declarados nas planilhas de custos e formação de preços, poderão ser reajustados mediante negociação entre as partes, tendo como limite máximo a variação do IPCA – IBGE, conforme a seguir:
- a) Na primeira prorrogação de vigência, as partes observarão para que o percentual a ser aplicado não seja superior à variação acumulada, no período compreendido entre a data da apresentação da proposta e aquela em que se verificar o aniversário da celebração do contrato, conforme estabelece a Lei n. 8.666/1993, art. 40, inciso XI.
 - b) Nas prorrogações seguintes, o reajuste será calculado considerando-se a variação acumulada dos 12 (doze) últimos meses, contados do aniversário do contrato.



PODER JUDICIÁRIO
CONSELHO DA JUSTIÇA FEDERAL

- c) Caso o índice estabelecido para delimitar o reajustamento dos preços seja extinto ou, de qualquer forma, não possa mais ser utilizado para esse fim, as partes desde já concordam que em substituição seja adotado o que vier a ser determinado pela legislação então em vigor.
- d) Na ausência de previsão legal quanto ao índice substituto, as partes elegerão novo índice para delimitar o reajustamento dos preços.

17.2 Da Repactuação DOS SERVIÇOS:

17.2.1 Os valores referentes aos serviços gerenciados de segurança, quando houver à alocação continuada de profissionais da CONTRATADA nas dependências do CONTRATANTE, previstos no contrato poderão ser repactuados, mediante negociação entre as partes, observado o interregno mínimo de um ano, a contar da data do orçamento a que a proposta se referir, cabendo à CONTRATADA apresentar, junto à solicitação, a devida justificativa e demonstração analítica da variação dos componentes de custo do Contrato, de acordo com planilha de custos e formação de preços, acordo, convenção ou dissídio coletivo de trabalho ou equivalente, registrado no Sistema de Negociações Coletivas de Trabalho - Mediador, entre outros, visando à análise e aprovação pelo CONTRATANTE.

17.3 A repactuação para fazer face à elevação dos custos da contratação, respeitada a anualidade disposta no item anterior e que vier a ocorrer durante a vigência do Contrato, é direito da CONTRATADA, e não poderá alterar o equilíbrio econômico e financeiro do Contrato, conforme estabelece o art. 37, inciso XXI da Constituição da República Federativa do Brasil, sendo assegurado à CONTRATADA receber pagamento mantidas as condições efetivas da proposta;

17.4 A repactuação poderá ser dividida em tantas parcelas quanto forem necessárias em respeito ao princípio da anualidade do reajuste dos preços da contratação, podendo ser realizada em momentos distintos para discutir a variação de custos que tenham sua anualidade resultante em datas diferenciadas, tais como os custos decorrentes da mão de obra e os custos decorrentes dos insumos necessários à execução do serviço;

17.5 A repactuação, em razão de novo acordo, dissídio ou convenção coletiva deve repassar integralmente o aumento de custos da mão de obra decorrente desses instrumentos;

17.6 O interregno mínimo de 1 (um) ano para a primeira repactuação será contado a partir da data do acordo, convenção ou dissídio coletivo de trabalho ou equivalente, vigente à época da apresentação da proposta, quando a variação



PODER JUDICIÁRIO
CONSELHO DA JUSTIÇA FEDERAL

dos custos for decorrente da mão de obra e estiver vinculada às datas-bases destes instrumentos;

- 17.7** Nas repactuações subsequentes à primeira, a anualidade será contada a partir da data do fato gerador que deu ensejo à última repactuação;
- 17.8** As repactuações serão precedidas de solicitação da CONTRATADA, acompanhada de demonstração analítica da alteração dos custos, por meio de apresentação da planilha de custos e formação de preços ou do novo acordo convenção ou dissídio coletivo que fundamenta a repactuação, conforme for a variação de custos objeto da repactuação;
- 17.9** A proposta de repactuação dependerá de iniciativa da CONTRATADA, devendo ser apresentada ao CONTRATANTE em até 30 (trinta) dias da ocorrência do fato ensejador da variação dos componentes de custos do Contrato, ou até a prorrogação contratual ou o encerramento do contrato, se esses eventos ocorrerem antes daquele prazo;
- 17.10** A CONTRATADA apresentará justificativa expressa, nos mesmos prazos indicados no item anterior, caso não seja possível a apresentação da proposta de repactuação;
- 17.11** Caso o CONTRATANTE concorde com a justificativa, a CONTRATADA, para fazer jus à repactuação retroativa, deverá solicitá-la até a prorrogação contratual ou o encerramento do contrato, pois serão objeto de preclusão com a assinatura da prorrogação contratual ou com o fim de vigência do ajuste;
- 17.12** É vedada a inclusão, por ocasião da repactuação, de benefícios não previstos na proposta inicial, exceto quando se tornarem obrigatórios por força de instrumento legal, sentença normativa, acordo coletivo ou convenção coletiva;
- 17.13** A decisão sobre o pedido de repactuação deve ser feita no prazo máximo de sessenta dias, contados a partir da solicitação e da entrega dos comprovantes de variação dos custos;
- 17.14** Na hipótese de iminente prorrogação do contrato, não havendo concessão do pedido até a assinatura do termo aditivo respectivo, a CONTRATADA deverá deixar consignado o seu direito expressamente nesse instrumento;
- 17.15** O prazo referido subitem anterior ficará suspenso enquanto a CONTRATADA não cumprir os atos ou apresentar a documentação solicitada pelo CONTRATANTE para a comprovação da variação dos custos;
- 17.16** O CONTRATANTE poderá realizar diligências para conferir a variação de custos alegada pela CONTRATADA;
- 17.17** Os novos valores contratuais decorrentes das repactuações terão suas vigências iniciadas observando-se o seguinte:



PODER JUDICIÁRIO
CONSELHO DA JUSTIÇA FEDERAL

- 17.17.1** A partir da ocorrência do fato gerador que deu causa à repactuação;
- 17.17.2** Em data futura, desde que acordada entre as partes, sem prejuízo da contagem de periodicidade para concessão das próximas repactuações futuras; ou
- 17.17.3** Em data anterior à ocorrência do fato gerador, exclusivamente quando a repactuação envolver revisão do custo de mão de obra em que o próprio fato gerador, na forma de acordo, convenção ou sentença normativa, contemplar data de vigência retroativa, podendo esta ser considerada para efeito de compensação do pagamento devido, assim como para a contagem da anualidade em repactuações futuras.
- 17.18** Os efeitos financeiros da repactuação deverão ocorrer exclusivamente para os itens que a motivaram, e apenas em relação à diferença porventura existente;
- 17.19** As repactuações não interferem no direito das partes de solicitar, a qualquer momento, a manutenção do equilíbrio econômico dos contratos com base no disposto no art. 65 da Lei n. 8.666. de 1993;
- 17.20** A CONTRATADA para a execução de remanescente de serviço tem direito à repactuação nas mesmas condições e prazos a que fazia jus a empresa anteriormente contratada, devendo os seus preços serem corrigidos antes do início da contratação, conforme determina o art. 24, inciso XI da Lei n. 8.666, de 1993;
- 17.21** As repactuações poderão ser formalizadas por meio de apostilamento, e não poderão alterar o equilíbrio econômico e financeiro do Contrato, exceto quando coincidirem com a prorrogação contratual, em que deverão ser formalizadas por aditamento;
- 17.22** Em decorrência da variação anual do Fator Acidentário de Prevenção - FAP (cf. Decreto n. 6.957/2009), a CONTRATADA deverá apresentar, com o pedido de repactuação a documentação comprobatória acerca da alteração/manutenção da alíquota do FAP.

18. DO CONTINGENCIAMENTO DOS ENCARGOS TRABALHISTAS

- 18.1** Os encargos sociais trabalhistas serão contingenciados pelos percentuais abaixo, incidentes sobre a remuneração mensal dos profissionais alocados no CONTRATANTE para execução do contrato.



PODER JUDICIÁRIO
CONSELHO DA JUSTIÇA FEDERAL

Percentuais para contingenciamento de encargos trabalhistas a serem aplicados sobre a NF

Título	VARIAÇÃO RAT AJUSTADO 0,50% A 6,00%			
	EMPRESAS		SIMPLES	
Grupo A SUBMÓDULO 4.1 - DA IN 1/2016 – CJF: RAT:	Mínimo 34,30% 0,50%	Máximo 39,80% 6,00%	Mínimo 28,50% 0,50%	Máximo 34,00% 6,00%
13º salário	9,09	9,09	9,09	9,09
Férias	9,09	9,09	9,09	9,09
1/3 Constitucional	3,03	3,03	3,03	3,03
Subtotal	21,21	21,21	21,21	21,21
Incidência do Grupo A (*)	7,28	8,44	6,04	7,21
Multa do FGTS	4,36	4,36	4,36	4,36
Encargos a contingenciar	32,85	34,01	31,61	32,78
Taxa da conta corrente vinculada (inciso III, artigo 2º IN) (**)				
Total a contingenciar				

(*) A incidência recai sobre as verbas de 13º salário, férias e 1/3 constitucional, variando de acordo com o RAT Ajustado da contratada.

(**) Caso o contrato firmado entre a empresa e o banco oficial tenha previsão de desconto da taxa de abertura e manutenção diretamente na conta vinculada, esse valor deverá ser retido da fatura e devolvido à conta vinculada, nos termos do inciso VIII do artigo 17 da Resolução CNJ n. 169/2013.

- 18.2** O contingenciamento será feito mensalmente, mediante depósito em conta-depósito vinculada – bloqueada para movimentação -, cujo saldo será remunerado pelo índice da poupança ou outro definido com a instituição financeira, recaiando a opção sempre pelo de maior rentabilidade, na forma estabelecida pela Instrução Normativa CJF nº 01/2016;
- 18.3** A CONTRATADA deverá providenciar a assinatura dos documentos relativos à abertura e movimentação da conta-depósito vinculada (bloqueada para movimentação), em até 20 (vinte) dias a contar da notificação do CONTRATANTE;
- 18.4** Eventuais despesas com abertura e manutenção da conta-depósito vinculada deverão ser suportadas pela CONTRATADA e integrarão os custos com taxa de administração, constante da proposta comercial da empresa;
- 18.5** Caso o banco promova desconto(s) diretamente na conta-depósito vinculada – bloqueada para movimentação –, das despesas com abertura e manutenção da referida conta, o valor correspondente será retido do pagamento mensal devido à CONTRATADA e depositado na conta-depósito vinculada;



PODER JUDICIÁRIO
CONSELHO DA JUSTIÇA FEDERAL

- 18.6** Sempre que necessário, o gestor do contrato poderá requerer à CONTRATADA a apresentação dos documentos comprobatórios da remuneração dos profissionais alocados na execução deste contrato, bem como daqueles necessários à apuração do RAT ajustado;
- 18.7** As parcelas correspondentes a Férias e 13º salário serão liberadas ao longo da execução do contrato na medida em que os eventos ocorrerem.

19. UNIDADE GESTORA/ FISCALIZADORA DO CONTRATO

- 19.1** A Subsecretaria de Segurança da Tecnologia da Informação - SUSTI acompanhará a execução do contrato (Gestor do Contrato), devendo proceder à orientação, fiscalização e interdição da execução do contrato, se necessário, a fim de garantir o exato cumprimento das condições estabelecidas em contrato;
- 19.2** A Seção de Segurança de Rede – SESERE atuará na fiscalização (Fiscal Técnico) e acompanhamento da execução técnica do contrato a fim de garantir o exato cumprimento das condições estabelecidas em contrato;
- 19.3** O representante da Área Administrativa (Fiscal Administrativo do Contrato), indicado pela autoridade competente dessa área, fiscalizará o contrato quanto aos aspectos administrativos, tais como a verificação de regularidades fiscais, trabalhistas e previdenciárias para fins de pagamento.
- 19.4** Também cabe ao representante da Área Administrativa, conforme definido na Instrução Normativa CJF-INN-2016/00001, a verificação dos percentuais das rubricas, o acompanhamento, o controle, a conferência dos cálculos efetuados, a confirmação dos valores e da documentação apresentada e demais verificações pertinentes, bem como a autorização para movimentar a conta-depósito vinculada – bloqueada para movimentação.

20. SELEÇÃO DO FORNECEDOR

- 20.1** Objetivando atender ao princípio da segregação de funções previsto na Norma NBR ISO/IEC 27002:2005 e manutenção da qualidade dos serviços de SI, conforme exposto na justificativa deste Termo, a licitante não poderá ser declarada vencedora caso preste serviços técnicos especializados de sustentação da infraestrutura de TI ou serviços técnicos especializados de desenvolvimento e sustentação de software, em regime de fábrica de software para o CJF;



PODER JUDICIÁRIO
CONSELHO DA JUSTIÇA FEDERAL

- 20.2** A proposta de preços deverá ser redigida em língua portuguesa, sem alternativas, opções, emendas, ressalvas, borrões, rasuras ou entrelinhas, e dela deverá constar declaração da licitante de ciência de que o CJF realizará o contingenciamento das obrigações trabalhistas, conforme previsto Instrução Normativa CJF-INN-2016/00001, nos termos estabelecidos na cláusula da minuta do contrato;
- 20.3** A licitante classificada provisoriamente em primeiro lugar deverá encaminhar a proposta de preço adequada ao último lance devidamente preenchida na forma do Anexo II – Planilha de preços, em arquivo único;
- 20.4** A proposta de preço deverá conter, ainda, memória de cálculo detalhada que contenha a metodologia e fórmulas adotadas pela licitante para obtenção dos valores propostos para os encargos e demais componentes da planilha de composição de custos e formação de preços dos serviços que envolvam a alocação de profissionais no CONTRATANTE;
- 20.5** Os documentos remetidos poderão ser solicitados em original ou por cópia autenticada a qualquer momento, em prazo a ser estabelecido pelo Pregoeiro;
- 20.6** A licitante que abandonar o certame, deixando de enviar a documentação indicada nesta seção, será desclassificada e sujeitar-se-á às sanções previstas;
- 20.7** Não se admitirá proposta que apresente valores simbólicos, irrisórios ou de valor zero, incompatíveis com os preços de mercado, exceto quando se referirem a materiais e instalações de propriedade da licitante, para os quais ela renuncie à parcela ou à totalidade de remuneração;
- 20.8** É obrigatório às licitantes, em sua proposta, apresentar atestado(s) ou certidão(ões) de capacidade técnico-operacional comprobatórios de que a empresa proponente tenha executado ou esteja executando, serviços de características técnicas ou complexidade semelhantes às do objeto do presente Termo de Referência, ou seja:
- 20.8.1** Os Atestado(s) de Capacidade Técnica-Operacional deverá(ão) ser emitido(s) por entidade da Administração Federal, Estadual ou Municipal, direta ou indireta e/ou empresa privada que comprove ter a empresa licitante executado serviços de características técnicas semelhantes ao objeto desta contratação nos termos da Lei, comprovando:
- a) Experiência na prestação de serviços de administração de solução de Gerenciamento Unificado de Ameaças - UTM;
 - b) Experiência na prestação de serviços de administração de solução de anti-malware para estações de trabalho em ambiente computacional com, no mínimo, 250 (duzentos e cinquenta) estações de trabalho;



PODER JUDICIÁRIO
CONSELHO DA JUSTIÇA FEDERAL

- c) Experiência na prestação de serviços de administração de solução de anti-malware para ambiente de datacenter utilizando plataforma de virtualização de rede VMware NSX com, no mínimo, 200 (duzentos) servidores de rede;
 - d) Experiência na prestação de serviços de administração de solução de segurança para proteção de gateway de e-mail, contemplando proteção *anti-malware* e *anti-spam* em ambiente computacional com, no mínimo, 250 (duzentos e cinquenta) caixas postais;
 - e) Experiência na prestação de serviços de monitoramento proativo e resposta a incidentes de segurança da informação em ambientes com, no mínimo, 400 (quatrocentos) ativos;
 - f) Experiência na prestação de serviços de gestão de vulnerabilidades, incluindo o monitoramento e o tratamento das vulnerabilidades encontradas em ambientes com, no mínimo, 400 (quatrocentos) ativos;
 - g) Experiência na prestação de serviços de administração de solução de Gerenciamento e Correlação de Eventos de Segurança da Informação - SIEM, em ambientes com, no mínimo, 400 (quatrocentos) ativos;
 - h) Experiência na prestação de serviços de testes de invasão para exploração de vulnerabilidades de segurança da informação, em conformidade com boas práticas internacionais;
- 20.9** Entende-se por similar, soluções ou produtos (equipamentos ou softwares) com funcionalidades equivalentes, escalabilidade compatível e porte corporativo;
- 20.10** Deverão constar do(s) atestado(s) de capacidade técnica em destaque, os seguintes dados: identificação do emitente, especificação completa do fornecimento/serviço executado, prazo de vigência do contrato, local e data de expedição, data de início e término do contrato;
- 20.11** Será permitido o somatório de atestado(s) de capacidade técnica-operacional para efeito de comprovação de experiência na prestação dos serviços de características técnicas semelhantes ao objeto desta contratação;
- 20.12** O CONTRATANTE poderá diligenciar a pessoa jurídica indicada no Atestado de Capacidade Técnica, visando validar ou esclarecer informações sobre o serviço prestado.



PODER JUDICIÁRIO
CONSELHO DA JUSTIÇA FEDERAL

21. VISTORIA

21.1 A LICITANTE, caso julgue conveniente para o correto dimensionamento e cumprimento das obrigações, poderá realizar uma vistoria nas instalações do CONTRATANTE para tomar conhecimento dos serviços a serem realizados. Não serão admitidas, em hipótese alguma, alegações posteriores de desconhecimento da complexidade dos serviços e de dificuldades técnicas não previstas:

21.1.1 A vistoria deverá ocorrer por horário marcado, e será agendada pela Secretaria de Tecnologia da Informação - STI através dos telefones (61) 3022-7400/ 7403;

21.1.2 O agendamento da vistoria poderá ocorrer até 48 (quarenta e oito) horas antes da data e horário de abertura do processo licitatório;

21.1.3 A vistoria deverá ser realizada em até, no máximo, 24 (vinte e quatro) horas da abertura do processo licitatório.

22. GARANTIA

22.1 Para assinatura do Contrato, decorrente do procedimento licitatório, a CONTRATADA prestará garantia no valor correspondente a 3% (três por cento) do valor total do Contrato, nos termos do art. 56 e seus parágrafos, da Lei nº. 8.666/93, quais sejam:

22.1.1 Caução em dinheiro ou títulos da dívida pública; ou

22.1.2 Seguro – garantia; ou

22.1.3 Fiança bancária.

22.2 O valor da garantia permanecerá integral até o término da vigência do Contrato. A reposição de seu valor, quando for o caso, será feita em até 10 (dez) dias, contadas da data de recebimento da notificação do CONTRATANTE.

22.3 O valor da garantia reverterá, integralmente, em favor do CONTRATANTE, ou pelo saldo que apresentar, no caso de rescisão contratual por culpa exclusiva da CONTRATADA, sem prejuízo das perdas e danos porventura verificados.

22.4 O CONTRATANTE poderá utilizar o valor da garantia prestada para descontar, entre outros, os valores referentes a eventuais multas aplicadas à CONTRATADA, bem como nos casos decorrentes de inadimplemento



PODER JUDICIÁRIO
CONSELHO DA JUSTIÇA FEDERAL

contratual, e de indenização por danos causados ao Patrimônio da União ou de terceiros, ocorridos nas suas dependências.

23. DOCUMENTOS ANEXOS

23.1 Seguem anexos a este termo de referência os seguintes documentos:

- Anexo I - Níveis de Qualidade dos Serviços e Tabela de Glosas
- Anexo II – Planilha de Preços
- Anexo III – Plataforma de Segurança
- Anexo IV – Modelo de Declarações
- Anexo V – Cronograma de atividade da prestação dos serviços

ANEXO I do Termo de Referência

NÍVEIS MÍNIMOS DE SERVIÇO E TABELA DE GLOSAS

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 adiante.

A CONTRATADA deverá manter os seguintes níveis de qualidade para a prestação dos Serviços Gerenciados de Segurança:

Item	Indicadores de Níveis de Serviço	Fórmula de Cálculo com base no mês calendário	Meta Exigida	Glosa por inadimplemento
1	Índice de disponibilidade dos serviços de segurança do CJF.	Total de tempo com disponibilidade no mês / total de tempo no mês X 100	>= 99,7 %	30 pontos (+5 pontos a cada 0,1% abaixo da meta)



PODER JUDICIÁRIO
CONSELHO DA JUSTIÇA FEDERAL

Item	Indicadores de Níveis de Serviço	Fórmula de Cálculo com base no mês calendário	Meta Exigida	Glosa por inadimplemento
2	Tempo máximo para correção de incidente nos serviços de segurança do CJF, em caso de indisponibilidade .	Tempo = Hora do restabelecimento – Hora do início da indisponibilidade	<= 60 minutos	30 pontos (+5 pontos a cada 10 minutos excedentes)
3	Tempo máximo para correção de incidente nos serviços de segurança do CJF, em caso de degradação de desempenho .	Tempo = Hora do restabelecimento – Hora do início da degradação de desempenho	<= 90 minutos	15 pontos (+5 pontos a cada 10 minutos excedentes)
4	Tempo máximo para triagem de incidentes de segurança	Tempo = Hora da triagem – Hora de entrada do evento de segurança	<= 15 minutos	3 pontos (+1 ponto a cada 5 minutos excedentes)
5	Tempo máximo para resposta de incidentes de segurança de gravidade alta	Tempo = Hora do início da resposta – hora da triagem	<= 60 minutos	10 pontos (+3 pontos a cada 5 minutos excedentes)
6	Tempo máximo para resposta de incidentes de segurança de gravidade média	Tempo = Hora do início da resposta – hora da triagem	<= 120 minutos	10 pontos (+3 pontos a cada 5 minutos excedentes)
7	Tempo máximo para resposta de incidentes de segurança de gravidade baixa	Tempo = Hora do início da resposta – hora da triagem	<= 180 minutos	10 pontos (+3 pontos a cada 10 minutos excedentes)
8	Tempo máximo para requisição de mudança para aplicação de patches e hotfixes de segurança ou indicação de solução de contorno para tratamento de greve vulnerabilidade ou ameaça emergente	Tempo = Hora de conclusão do planejamento da requisição de mudança – hora de disponibilização dos patches e hotfixes ou divulgação de grave vulnerabilidade ou ameaça emergente	<= 72 horas	5 pontos (+2 pontos a cada hora excedente)



PODER JUDICIÁRIO
CONSELHO DA JUSTIÇA FEDERAL

Item	Indicadores de Níveis de Serviço	Fórmula de Cálculo com base no mês calendário	Meta Exigida	Glosa por inadimplemento
9	Tempo máximo para resolução de requisições de serviços relacionadas aos produtos de UTM, WAF ou NSX.	Tempo = Hora da resolução da solicitação – hora de início da solicitação	<= 90 minutos	10 pontos (+3 pontos a cada 10 minutos excedentes)
10	Tempo máximo para resolução das demais requisições de serviços .	Tempo = Hora da resolução da solicitação – hora da solicitação	<= 24 horas	10 pontos (+3 pontos a cada hora excedente)
11	Tempo máximo para comunicação de incidentes ao SAC e aos gestores de TI do CJF.	Tempo = Hora da comunicação – hora da triagem	<= 15 minutos	5 pontos (+2 pontos a cada 5 minutos excedentes)
12	Índice de cumprimento dos prazos acordados para a execução das Ordens de Serviço Exclusivas .	Prazo Real – (Prazo Acordado + 25%)	<= 0	15 pontos
13	Tempo máximo para abertura de chamados de suporte com terceiros	Tempo = Hora de abertura do chamado – hora da triagem	<= 15 minutos	5 pontos (+2 pontos a cada 5 minutos excedente)

Serão aplicadas as referidas pontuações para efeito de glosa, no caso de a CONTRATADA:

Item	Descrição	Referência	Glosa por inadimplemento
14	Finalizar a requisição de serviço ou incidente sem a devida resolução ou sem realizar os testes necessários para aferir a efetiva resolução.	Por ocorrência	10 pontos
15	Finalizar uma requisição de serviço sem documentar os procedimentos executados para atendimento da solicitação.	Por ocorrência	5 pontos



PODER JUDICIÁRIO
CONSELHO DA JUSTIÇA FEDERAL

16	Finalizar um incidente sem documentar a causa, a solução de contorno (se houver) ou os procedimentos adotados para solução.	Por ocorrência	5 pontos
17	Finalizar um problema sem documentar a investigação realizada, a causa-raiz ou a solução aplicada.	Por ocorrência	5 pontos
18	Fraudar, manipular ou descaracterizar indicadores/metadados de níveis de serviço por quaisquer subterfúgios, por indicador/meta de nível de serviço manipulado.	Por ocorrência	30 pontos
19	Manter profissionais sem formalização ou sem a qualificação exigida para executar os serviços contratados, ainda que em casos de substituição temporária.	Por profissional e por dia	30 pontos
20	Causar qualquer indisponibilidade dos serviços da contratante por motivo de imperícia ou imprudência na execução das atividades contratuais.	Por ocorrência	30 pontos
21	Utilizar indevidamente os recursos de TI (acessos indevidos, utilização para fins particulares) ou utilizar equipamento particular;	Por ocorrência	30 pontos
22	Realizar mudanças de configuração nas soluções de segurança sem autorização da unidade responsável.	Por regra incluída, alterada ou excluída.	15 pontos

Serão aplicadas as referidas pontuações para efeito de glosa, no caso de a CONTRATADA **DEIXAR DE:**

Item	Descrição	Referência	Glosa por inadimplemento
23	Cumprir ou implementar as rotinas em conformidade com a Política de Segurança ou determinações da equipe de fiscalização do contrato.	Por ocorrência	10 pontos
24	Cumprir ou implementar as rotinas em conformidade com os Planos de Gerenciamento de Incidentes, de Disponibilidade, de Continuidade e de Recuperação de Desastres das soluções de segurança.	Por ocorrência	10 pontos



PODER JUDICIÁRIO
CONSELHO DA JUSTIÇA FEDERAL

25	Executar testes de continuidade de cada solução de segurança da informação em alta disponibilidade a, no mínimo, cada 6 (seis) meses.	Por ocorrência	10 pontos
26	Atuar proativamente em caso de identificação de situação de desconformidade com boas práticas de segurança.	Por ocorrência	10 pontos
27	Apresentar mensalmente plano de tratamento de vulnerabilidades, indicando as ações mais efetivas para redução dos riscos.	Por ocorrência	10 pontos
28	Apresentar os relatórios consolidados conforme exigências do Termo de Referência até o dia 5º dia útil do mês subsequente.	Por dia de atraso	05 pontos
29	Apresentar relatórios, levantamentos ou inventários conforme demanda em até 3 dias úteis;	Por ocorrência	05 pontos
30	Manter o Configuration Management Database (CMDB) atualizado.	Por ocorrência	10 pontos
31	Manter a documentação e os desenhos das topologias atualizados e completos.	Por ocorrência	05 pontos
32	Notificar sobre ocorrências recorrentes.	Por ocorrência	05 pontos
33	Cumprir ou implementar as rotinas em conformidade com os processos de trabalho da Secretaria de Tecnologia da Informação.	Por ocorrência	10 pontos
34	Elaborar auditorias de dados, consultas às bases de logs de transações ou relatórios diversos.	Por ocorrência	15 pontos
35	Analisar a viabilidade e o impacto da instalação de novas soluções ou correções.	Por ocorrência	05 pontos
36	Apresentar mensalmente proposta de melhorias no ambiente.	Por ocorrência	05 pontos
37	Cumprir quaisquer obrigações estabelecidas no contrato e anexos, não previstas nesta tabela, após reincidência formalmente notificada pelo CJF.	Por ocorrência	15 pontos



PODER JUDICIÁRIO
CONSELHO DA JUSTIÇA FEDERAL

ANEXO II do Termo de Referência

PLANILHA DE PREÇOS

Item	Descrição		Quantidade	Descrever os nomes dos produtos ofertados (se aplicável)	Preço unitário Médio Estimado (R\$)	Preço unitário (R\$)	Preço Total (R\$)
1	Serviço de Operação e Atendimento à Requisições		24 meses		67.125,89		
2	Serviço de Gestão de Incidentes de Segurança (CSIRT - Blue Team)		24 meses		26.200,41		
3	Serviço de Gestão de Vulnerabilidades		24 meses		19.994,09		
4	Serviço de Monitoramento e Visibilidade de Ataques Cibernéticos	4.1 Serviço de Visibilidade de Logs, Fluxos e Informações	24 meses (15 GB/dia ou 440 EPS)		21.764,05		
		4.2 Serviço de Análise de Comportamento de Usuário (UBA)	24 meses		10.624,93		
		4.3 Serviço de Análise de Tráfego de Rede (NTA)	24 meses		13.395,71		
5	Serviço de Orquestração, Automação e Resposta de Segurança (SOAR)		24 meses		24.921,42		
6	Serviço de Testes de Invasão (Red Team)		15 sistemas		14.703,67		
VALOR TOTAL DOS SERVIÇOS GERENCIADOS DE SEGURANÇA							

Observação: Os serviços serão solicitados **SOB DEMANDA**, mediante emissão de Ordem de Serviço (OS), em períodos múltiplos



PODER JUDICIÁRIO
CONSELHO DA JUSTIÇA FEDERAL

de 12 (doze) meses, **SEM GARANTIA DE CONSUMO MÍNIMO DE MESES.**



PODER JUDICIÁRIO
CONSELHO DA JUSTIÇA FEDERAL

Modelo de planilha para apresentação dos custos quando houver alocação de profissionais no CONTRATANTE:

Dados para composição dos custos referentes a mão de obra			
1	Tipo de Serviço (mesmo serviço com características distintas)		
2	Classificação Brasileira de Ocupações (CBO)		
3	Salário da Categoria Profissional	R\$	-
4	Sindicato da Categoria Profissional (vinculada à execução contratual)		
5	Data-Base da Categoria (dia/mês/ano)		
6	Nº da Convenção Coletiva de trabalho (CCT)		
Módulo 1 - Composição da Remuneração			
1	Composição da Remuneração		Valor (R\$)
A	Salário-Base		-
B	Adicional de Periculosidade		R\$ -
C	Adicional de Insalubridade		R\$ -
D	Adicional Noturno		R\$ -
E	Adicional de Hora Noturna Reduzida		R\$ -
F	Outros (especificar)		R\$ -
Total			-
Nota 1: O Módulo 1 refere-se ao valor mensal devido ao empregado pela prestação do serviço no período de 12 meses.			
Módulo 2 - Encargos e Benefícios Anuais, Mensais e Diários			
Submódulo 2.1 - 13º (décimo terceiro) Salário, Férias e Adicional de Férias			
2.1	13º (décimo terceiro) Salário, Férias e Adicional de Férias	Percentual (%)	Valor (R\$)
A	13º (décimo terceiro) Salário	9,09%	-
B	Férias e Adicional de Férias	12,12%	-
Total		21,21%	-
Nota 1: Como a planilha de formação de preços e custos é calculada mensalmente, provisiona-se proporcionalmente 1/11 (um onze avos) dos valores referentes a gratificação natalina, férias e adicional de férias. (Redação dada pela Instrução Normativa CJF nº 1, de 2016)			
Nota 2: O adicional de férias contido no Submódulo 2.1 corresponde a 1/3 (um terço) da remuneração que por sua vez é dividido por 11 (onze) conforme Nota 1 acima.			



PODER JUDICIÁRIO
CONSELHO DA JUSTIÇA FEDERAL

Nota 3: Levando em consideração a vigência contratual prevista no art. 57 da Lei nº 8.666, de 23 de junho de 1993, a rubrica férias tem como objetivo principal suprir a necessidade do pagamento das férias remuneradas ao final do contrato de 12 meses.

Submódulo 2.2 - Encargos Previdenciários (GPS), Fundo de Garantia por Tempo de Serviço (FGTS) e outras contribuições.

2.2	GPS, FGTS e outras contribuições	Percentual (%)	Valor (R\$)
A	INSS	20,00%	-
B	Salário Educação	2,50%	-
C	RATajustado (RAT x FAP)	1,00%	-
D	SESC ou Sesi	1,50%	-
E	SENAI - SENAC	1,00%	-
F	SEBRAE	0,60%	-
G	INCRA	0,20%	-
H	FGTS	8,00%	-
Total		34,80%	-

Nota 1: O percentual do INSS poderá sofrer alteração de acordo com a "Desoneração da Folha de Pagamento" (Lei 12.546/2011).

Nota 2: Os percentuais dos encargos previdenciários, do FGTS e demais contribuições são aqueles estabelecidos pela legislação vigente.

Nota 3: O RAT a depender do grau de risco do serviço irá variar entre 1%, para risco leve, de 2%, para risco médio, e de 3% de risco grave. Deverá ser ajustado ao fator acidentário previdenciário (FAP).

Nota 4: Esses percentuais incidem sobre o Módulo 1, o Submódulo 2.1.

Nota 5: Os percentuais do Submódulo 2.2 já incidem sobre remuneração, 13º salário, férias e adicional de férias.

Submódulo 2.3 - Benefícios Mensais e Diários.

2.3	Benefícios Mensais e Diários	Dias úteis	Valor (R\$)
A	Transporte		-
B	Auxílio-Refeição/Alimentação		-
C	Assistência Médica e Familiar		-
D	Assistência Odontológica		-
Total			-

Nota 1: O valor informado deverá ser o custo real do benefício (descontado o valor eventualmente pago pelo empregado).

Nota 2: Observar a previsão dos benefícios contidos em Acordos, Convenções e Dissídios Coletivos de Trabalho..



PODER JUDICIÁRIO
CONSELHO DA JUSTIÇA FEDERAL

Quadro-Resumo do Módulo 2 - Encargos e Benefícios anuais, mensais e diários			
2	Encargos e Benefícios Anuais, Mensais e Diários		Valor (R\$)
2.1	13º (décimo terceiro) Salário, Férias e Adicional de Férias		-
2.2	GPS, FGTS e outras contribuições		-
2.3	Benefícios Mensais e Diários		-
Total			-
Módulo 3 - Provisão para Rescisão			
3	Provisão para Rescisão	Percentual (%)	Valor (R\$)
A	Aviso Prévio Indenizado	0,00%	-
B	Incidência do FGTS sobre o Aviso Prévio Indenizado	0,00%	-
C	Multa do FGTS e contribuição social sobre o Aviso Prévio Indenizado	0,00%	-
D	Aviso Prévio Trabalhado	0,00%	-
E	Incidência de GPS, FGTS e outras contribuições sobre o Aviso Prévio Trabalhado	0,00%	-
F	Multa do FGTS e contribuição social sobre o Aviso Prévio Trabalhado	0,00%	-
G	Multa do FGTS	0,00%	-
Total		0,00%	-
Nota 1: O percentual de 1,94% indicado no Aviso Prévio Trabalhado torna-se custo não renovável decorridos 12 meses.			
Nota 2: Os percentuais do Módulo 3 já incidem sobre remuneração, 13º salário, férias e adicional de férias.			
Módulo 4 - Custo de Reposição do Profissional Ausente			
Nota 1: Os itens que contemplam o módulo 4 se referem ao custo dos dias trabalhados pelo repositor/substituto, quando o empregado alocado na prestação de serviço estiver ausente, conforme as previsões estabelecidas na legislação.			
Submódulo 4.1 - Substituto nas Ausências Legais			
4.1	Substituto nas Ausências Legais	Percentual (%)	Valor (R\$)
A	Substituto na cobertura de Férias	0,69%	-
B	Substituto na cobertura de Ausências Legais	0,00%	-



PODER JUDICIÁRIO
CONSELHO DA JUSTIÇA FEDERAL

C	Substituto na cobertura de Licença-Paternidade	0,00%	-
D	Substituto na cobertura de Ausência por acidente de trabalho	0,00%	-
E	Substituto na cobertura de Afastamento Maternidade	0,00%	-
F	Substituto na cobertura de outras ausências (especificar)	0,00%	-
Total		0,69%	-
Nota 1: Os percentuais do Submódulo 4.1 já incidem sobre remuneração, 13º salário, férias e adicional de férias.			
Quadro-Resumo do Módulo 4 - Custo de Reposição do Profissional Ausente			
4	Custo de Reposição do Profissional Ausente	Valor (R\$)	
4.1	Substituto nas Ausências Legais	-	
Total		-	
Módulo 5 - Insumos Diversos			
5	Insumos Diversos	Valor (R\$)	
A	Uniformes	-	
B	Materiais	-	
C	Equipamentos	-	
D	Outros (especificar)	-	
Total		-	
Nota: Valores mensais por empregado.			
Módulo 6 - Custos Indiretos, Tributos e Lucro			
Regime de tributação:		Lucro presumido	
6	Custos Indiretos, Tributos e Lucro	Percentual (%)	Valor (R\$)
A	Custos Indiretos	0,00%	-
B	Lucro	0,00%	-
C	Tributos (C.1 + C.2 + C.3)	8,65%	-
C.1.	Tributos Federais (PIS)	0,65%	-
C.2.	Tributos Federais (COFINS)	3,00%	-
C.3.	Tributos Estaduais/Municipais (ISS)	5,00%	-
D	Contribuição Previdenciária sobre a Receita Bruta - CPRB	0,00%	-



PODER JUDICIÁRIO
CONSELHO DA JUSTIÇA FEDERAL

Total	8,65%	-
Nota 1: Custos Indiretos, Tributos e Lucro por empregado.		
Nota 2: A empresa que indicar "desoneração" do Submódulo 2.2 deverá incluir uma rubrica para tributação da Contribuição Previdenciária sobre a Receita Bruta - CPRB.		
QUADRO-RESUMO DO CUSTO POR EMPREGADO		
Mão de obra vinculada à execução contratual (valor por empregado)		Valor(R\$)
A	Módulo 1 - Composição da Remuneração	-
B	Módulo 2 - Encargos e Benefícios Anuais, Mensais e Diários	-
C	Módulo 3 - Provisão para Rescisão	-
D	Módulo 4 - Custo de Reposição do Profissional Ausente	-
E	Módulo 5 - Insumos Diversos	-
Subtotal (A + B +C+ D+E)		-
F	Módulo 6 - Custos Indiretos, Tributos e Lucro	-
Valor Total por Empregado		-



PODER JUDICIÁRIO
CONSELHO DA JUSTIÇA FEDERAL

ANEXO III do Termo de Referência
PLATAFORMA DE SEGURANÇA

Tipo do Proteção	Marca / Modelo do Ativo	Descrição	Quantidade
Borda	Fortinet FortiGate 1500D	Firewall UTM com 4 portas 10 Gbps e 8 portas 1 Gbps	2
	Fortinet FortiWeb 3000D	Firewall de aplicação Web - WAF	2
	Fortinet FortiSandbox 2000E	Sandbox para emulação e análise de malwares	1
E-mail	Trend Micro InterScan Messaging Security Virtual Appliance	Ferramenta de segurança de borda (MTA) para proteção anti-malware de e-mail	2
	Trend Micro ScanMail for Microsoft Exchange	Ferramenta de segurança para proteção anti-malware para Microsoft Exchange	2
	Fortinet FortiMail VM	Ferramenta de segurança de borda (MTA) para proteção anti-malware de e-mail	1
Datacenter	Trend Micro Deep Security	Anti-malware para servidores de rede	400
	VMware NSX	Virtualização de rede e microssegmentação de segurança	
Endpoint	Trend Micro OfficeScan	Anti-malware para estações de trabalho	500



PODER JUDICIÁRIO
CONSELHO DA JUSTIÇA FEDERAL

Tipo do Proteção	Marca / Modelo do Ativo	Descrição	Quantidade
	Trend Micro Vulnerability Protection	Bloqueio contra exploração de vulnerabilidades conhecidas (virtual patch)	500
	Trend Micro Endpoint Application Control	Controle de aplicações instaladas nas estações de trabalho	500
	Trend Micro Apex One	Anti-malware para estações de trabalho, Bloqueio contra exploração de vulnerabilidades conhecidas (virtual patch), Bloqueio contra exploração de vulnerabilidades conhecidas (virtual patch) e EDR.	500
Nuvem	Trend Micro Cloud App Security	Proteção para Office 365	1
Mobile	Trend Micro Mobile Security for Enterprise	Proteção para smartphones	10
Ferramentas de Gerência	Trend Micro Control Manager	Gerenciador dos produtos Trend Micro	1
	Trend Micro Smart Protection Server	Servidor de atualização e de verificação de reputação de arquivos que se comunica com a nuvem da Trend Micro	1
	Rapid 7 Nexpose Security Console	Solução para gestão de vulnerabilidades de segurança dos ativos de TI	1



PODER JUDICIÁRIO
CONSELHO DA JUSTIÇA FEDERAL

Tipo do Proteção	Marca / Modelo do Ativo	Descrição	Quantidade
	Fortinet FortiManager VM	Gerenciamento centralizado de segurança	1
	Fortinet FortiAnalyzer VM	Centralizador de logs dos produtos Fortinet	1
	ServiceNow ITSM	Gerenciamento de serviços de TI	1
	ELK stack	Análise de dados	1

MINUTA



PODER JUDICIÁRIO
CONSELHO DA JUSTIÇA FEDERAL

ANEXO IV do Termo de Referência
MODELOS DE DECLARAÇÕES

1 - TERMO DE VISTORIA

Declaro, para fins de participação na licitação em epígrafe, que vistoriei minuciosamente o ambiente tecnológico do CONTRATANTE em que será prestado o serviço e que tomei conhecimento de todas as informações necessárias à execução do contrato e proclamo estar ciente da complexidade dos serviços, bem como dos termos e condições descritos no respectivo edital e seus módulos.

Declaro que todas as dúvidas que porventura foram por mim questionadas, foram respondidas pela equipe técnica do CJF e que marquei de próprio punho os itens abaixo.

☐	Visitei os locais de realização dos serviços, como Datacenter, ativos de redes, dutos de cabeamento, periféricos de apoio e setores de demanda de Ordem de Serviço.
☐	Vistoriei o ambiente de trabalho destinado para execução dos serviços, e os recursos materiais disponibilizados para a equipe contratada.
☐	Conheci os modelos e quantidades de equipamentos <i>hardwares</i> e periféricos objeto dos serviços.
☐	Tomei conhecimento dos principais <i>softwares</i> , aplicativos e ferramentas auxiliares em utilização nos computadores servidores e estações de trabalho.
☐	Tomei conhecimento dos procedimentos adotados, documentação existente, modelos de acompanhamento, recomendações e normatizações da Organização.
☐	Vistoriei o ambiente de monitoramento e ferramentas de <i>software</i> para acompanhamento de disponibilidade e desempenho dos recursos de infraestrutura.
☐	Estou ciente do grau de dificuldade e a devida especialização necessária para a execução dos serviços a serem contratados.

Brasília, / /20__.

ASSINATURA DO REPRESENTANTE TÉCNICO DA EMPRESA



PODER JUDICIÁRIO
CONSELHO DA JUSTIÇA FEDERAL

ASSINATURA DO REPRESENTANTE TÉCNICO DO CJF

2 – DECLARAÇÃO DE NÃO-NEPOTISMO

2.1. O modelo a seguir corresponde à declaração a ser assinada por cada profissional alocado em qualquer serviço objeto deste edital.

DECLARAÇÃO DE RELAÇÃO FAMILIAR OU DE PARENTESCO

(Resolução 7/2005 – CNJ, alterada pela Resolução 9/2005 – CNJ)

• IDENTIFICAÇÃO DA EMPRESA CONTRATADA

XXXXXXXXXXXXXXXXXXXXXXXXXXXX

CNPJ/MF: xxxxxxxxx

Endereço: XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX

Telefone/fax (NN) NNNNNN

CONTRATO DA EMPRESA EMPREGADORA COM O XXXXXXXXXXXXXXX

Contrato n. NNNNNN

• IDENTIFICAÇÃO DO(A) EMPREGADO(A)

NOME:.....

RG:..... ÓRGÃO EMISSOR:..... CPF:

DATA DE INGRESSO NO TRIBUNAL:

ÁREA DE LOTAÇÃO ATUAL:

DECLARAÇÃO DE PARENTESCO

O(A) empregado(a) acima qualificado(a) se declara cônjuge, companheiro(a) e/ou parente de ocupante(s) de cargo(s) de direção e/ou de assessoramento de membro(s) e/ou de juiz(es) vinculado(s) ao CJF ?

NÃO ()

SIM () ☐ pormenorizar em folha anexa.

DECLARO, sob as penas da Lei, que as informações prestadas são verdadeiras.

Local

Data/...../.....



PODER JUDICIÁRIO
CONSELHO DA JUSTIÇA FEDERAL

Assinatura _____ do _____ (a) _____ empregado
(a):

EMPRESA: XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX

CNPJ/MF: NNNNNNNNN

NOME

DO(A)

EMPREGADO(A):

RG:

ÓRGÃO

EMISSION:

CPF:

RELAÇÃO DE CÔNJUGE, COMPANHEIRO(A) E/OU PARENTE(S) QUE O(A) EMPREGADO(A) ABAIXO POSSUI NO ÂMBITO DO XXXXXXXXXXXX, CONFORME RESOLUÇÃO 7/2005 – CNJ, ALTERADA PELA RESOLUÇÃO 9/2005 – CNJ:

Nome do parente:

Grau de parentesco:

Órgão e cargo do parente:

DECLARO, sob as penas da Lei, que as informações prestadas são verdadeiras.

Local Data/...../.....

Assinatura do (a) empregado (a):

2.2. O modelo a seguir corresponde à declaração a ser assinada pelo representante da empresa na assinatura do contrato e em cada renovação.

DECLARAÇÃO DE NÃO OCORRÊNCIA DE NEPOTISMO

Eu, _____, brasileiro, casado, RG n. _____
Órgão Emission:, CPF n. _____, na qualidade de representante legal da empresa _____, inscrita no CNPJ/MF sob n. _____, estabelecida na _____, Cep: _____, telefone/fax () _____, DECLARO, para os fins da Resolução 7/2005 - CNJ, alterada pela Resolução 9/2005 - CNJ, que os prestadores de serviço locados no Contrato n. _____, firmado entre a _____ e o _____, não se enquadram nas hipóteses de parentesco previstas no artigo 3º da citada Resolução, não configurando ocorrência de nepotismo.



PODER JUDICIÁRIO
CONSELHO DA JUSTIÇA FEDERAL

Local e data

Assinatura

(representante legal da empresa)

MINUTA



PODER JUDICIÁRIO
CONSELHO DA JUSTIÇA FEDERAL

– DECLARAÇÃO DE SIGILO

2.3. O modelo a seguir corresponde à declaração a ser assinada pelo representante e por cada profissional alocado em qualquer serviço objeto deste edital.

Eu, _____, portador (a) da Carteira de Identidade n. _____, expedida pela _____ e do Cadastro de Pessoa Física, CPF/MF sob o n. _____, declaro que todos os dados e informações recebidos do Conselho de Justiça Federal, em relação ao Contrato n. _____, firmado entre a _____ e o _____, deverão ser mantidos em sigilo e serão utilizados exclusivamente para a execução do mesmo.

Local e data

Assinatura

3 – DECLARAÇÃO DE BOM USO DOS RECURSOS DE TI

3.1. O modelo a seguir corresponde à declaração a ser assinada pelo representante e por cada profissional alocado em qualquer serviço objeto deste edital.

Eu, _____, portador (a) da Carteira de Identidade n. _____, expedida pela _____ e do Cadastro de Pessoa Física, CPF/MF sob o n. _____, declaro estar ciente de que a estrutura computacional e telefônica disponibilizada pelo Conselho de Justiça Federal - CJF, referente ao Contrato n. _____, firmado entre a _____ e o _____, não poderá ser utilizada para fins particulares, que não devo fazer uso de equipamentos particulares no ambiente do CJF e que a navegação em sítios da Internet e as correspondências em meio eletrônico utilizando o endereço do CJF ou acessado a partir dos seus equipamentos deverão ser utilizados somente para fins de trabalho e poderão ser auditadas.

Local e data

Assinatura



PODER JUDICIÁRIO
CONSELHO DA JUSTIÇA FEDERAL

ANEXO V do Termo de Referência

CRONOGRAMA DE ATIVIDADES DA PRESTAÇÃO DOS SERVIÇOS

ANEXO V do - Prazo Máximo (em dias Corridos)	Cronograma de Atividade da Prestação dos Serviços Gerenciados de Segurança	Responsável
D	Emissão da Ordem de Serviço de Transição – OST (em até 20 dias após a assinatura do contrato entre as partes)	CJF
D + 5	Apresentação de Plano de Operacionalização dos Serviços contendo o detalhamento das ações necessárias para a absorção dos conhecimentos e repasse dos serviços.	CONTRATADA
D + 10	Carta de apresentação acompanhada da relação de prestadores da CONTRATADA que irão prestar os serviços, juntamente com os documentos comprobatórios de vínculo empregatício, experiência, qualificações e certificações exigidas para o perfil profissional.	CONTRATADA
D + 10	Início de período de transição.	CJF e CONTRATADA
D + 20	Início da prestação dos serviços.	CJF e CONTRATADA



PODER JUDICIÁRIO
CONSELHO DA JUSTIÇA FEDERAL

MÓDULO II DO EDITAL 1/2020
MINUTA da Ata De Registro De Preços – CJF

ATA DE REGISTROS DE PREÇOS CJF 000/2020

PROCESSO SEI N. 0001989-89.2019.4.90.8000
(SIGA-DOC N. CJF-ADM-2015/00202)

PREGÃO ELETRÔNICO N. 000/20000

O **CONSELHO DA JUSTIÇA FEDERAL**, (doravante denominado **ÓRGÃO GERENCIADOR**) órgão integrante do Poder Judiciário, inscrito no CNPJ/MF n. 00.508.903/0001-88, com sede no Setor de Clubes Esportivos Sul, Trecho III, Polo 8, Lote 9, Brasília-DF, neste ato representado por sua Secretária-Geral, a Exma. Juíza Federal **SIMONE DOS SANTOS LEMOS FERNANDES**, brasileira, CPF/MF n. 418.381.906-78, Carteira de Identidade n. 1075089-SSP/MG, residente em Brasília - DF, considerando o resultado do **Pregão Eletrônico CJF n. 000/2020** e atendendo as condições previstas no edital, sujeitando-se as partes às normas constantes da Lei no 10.520 (de 17 de julho de 2002); Lei Complementar n. 123 (de 14 de dezembro de 2006); dos Decretos n. 10.024 (de 20 de setembro de 2019), n. 7.892 (de 23 de janeiro de 2013), e 8.538 (de 6 de outubro 2015) e alterações posteriores, e, subsidiariamente, da Lei n. 8.666 (de 21 de junho de 1993) e, em conformidade com as informações constantes do Processo SEI n. 0001989-89.2019.4.90.8000, resolve registrar os preços da

(_____)doravante denominada **DETENTORA**, pessoa jurídica de direito privado, inscrita no CNPJ/MF n. 0000, estabelecida na (endereço), CEP: (000), neste ato representada por seu (sua) (cargo/função), o (a) senhor (a) (**nome SIGNATÁRIO**), brasileiro (a), CPF/MF n. 0000 e Carteira de Identidade n. 0000 – SSP/00, residente em (domicílio), mediante as disposições a seguir:

CLÁUSULA PRIMEIRA – DO OBJETO

1.1 Constitui objeto deste contrato a contratação de Serviços Gerenciados de Segurança da Informação para o Conselho de Justiça Federal – CJF de acordo com as especificações técnicas contidas no Termo de Referência e seus anexos, englobando os seguintes serviços:

- a) Serviço de operação e atendimento a requisições.
- b) Serviço de gestão de incidentes de segurança (CSIRT - Blue Team).



PODER JUDICIÁRIO
CONSELHO DA JUSTIÇA FEDERAL

- c) Serviço de gestão de vulnerabilidades.
- d) Serviço de monitoramento e visibilidade de ataques cibernéticos.
- e) Serviço de orquestração, automação e resposta de segurança (SOAR).
- f) Serviço de testes de invasão (Red Team).

1.2 As especificações constantes do edital de licitação (Pregão Eletrônico n. 00/0000), do termo de referência e da proposta comercial da DETENTORA, fazem parte deste instrumento, independentemente de transcrição.

CLÁUSULA SEGUNDA – DOS PREÇOS E DOS QUANTITATIVOS

2.1 Os preços registrados, as especificações do objeto e as quantidades ofertadas na proposta são:

Item	Descrição		Quantidade	Descrever os nomes dos produtos ofertados (se aplicável)	Preço unitário (R\$)	Preço Total (R\$)
1	Serviço de Operação e Atendimento à Requisições		24 meses			
2	Serviço de Gestão de Incidentes de Segurança (CSIRT - Blue Team)		24 meses			
3	Serviço de Gestão de Vulnerabilidades		24 meses			
4	Serviço de Monitoramento e Visibilidade de Ataques Cibernéticos	4.1 Serviço de Visibilidade de Logs, Fluxos e Informações	24 meses (15 GB/dia ou 440 EPS)			
		4.2 Serviço de Análise de Comportamento de Usuário (UBA)	24 meses			
		4.3 Serviço de Análise de Tráfego de Rede (NTA)	24 meses			
5	Serviço de Orquestração, Automação e Resposta de Segurança (SOAR)		24 meses			



PODER JUDICIÁRIO
CONSELHO DA JUSTIÇA FEDERAL

6	Serviço de Testes de Invasão (Red Team)	15 sistemas			
VALOR TOTAL DOS SERVIÇOS GERENCIADOS DE SEGURANÇA					

Observação: Os serviços serão solicitados **SOB DEMANDA**, mediante emissão de Ordem de Serviço (OS), dentro do período de 12 (doze) meses, **SEM GARANTIA DE CONSUMO MÍNIMO DE MESES**.

CLÁUSULA TERCEIRA- DOS PRAZOS E DA EXECUÇÃO DO SERVIÇO

3.1 Dos prazos e da execução dos serviços:

3.1.1 A DETENTORA deverá iniciar a prestação dos serviços objeto deste termo, de acordo com o cronograma apresentado no anexo V do Termo de Referência;

3.1.2 Para execução dos serviços, será implementado método de trabalho baseado no conceito de delegação de responsabilidade. Esse conceito define o ÓRGÃO GERENCIADOR como responsável pela gestão do contrato e pela atestação da aderência aos padrões de qualidade exigidos dos serviços entregues e a DETENTORA como responsável pela execução dos serviços e gestão dos profissionais a seu cargo;

3.1.3 A DETENTORA será responsável pela execução dos serviços e pelo acompanhamento diário da qualidade e dos níveis de serviço alcançados com vistas a efetuar eventuais ajustes e correções. Quaisquer problemas que venham a comprometer o bom andamento dos serviços ou o alcance dos níveis de serviço estabelecidos devem ser imediatamente comunicados por escrito ao ÓRGÃO GERENCIADOR;

3.1.4 Após a assinatura do contrato, será emitida Ordem de Serviço de Transição – OST com o objetivo de viabilizar a transferência de conhecimentos e o repasse dos serviços à nova DETENTORA;

3.1.5 A DETENTORA deverá apresentar, no prazo máximo de 10 (dez) dias corridos a partir da emissão da Ordem de Serviço de Transição - OST, carta de apresentação juntamente com os documentos comprobatórios (certificados oficiais) contendo os respectivos dados pessoais e informações quanto à habilitação e qualificação profissional de todos os profissionais que serão alocados na execução dos serviços no ÓRGÃO GERENCIADOR;

3.1.6 Quando da apresentação dos documentos comprobatórios de qualificação, a DETENTORA deverá observar atenciosamente à qualificação exigida, conforme descrito no Item 13 do Termo de Referência- Dos perfis profissionais. Caso a documentação não atenda às exigências deste item, a DETENTORA deverá apresentar documentação de um novo profissional que atenda as exigências, dentro do prazo estabelecido, antes do início das atividades;

3.1.7 Para fins de comprovação de atendimento aos requisitos de qualificação profissional serão aceitos:

a) Cópia autenticada de certificados ou diplomas que comprovem a conclusão dos cursos exigidos. No caso dos cursos de nível médio e/ou superior deverão ser apresentados os diplomas;

b) Todos os documentos apresentados estarão sujeitos à diligência da DETENTORA para fins de confirmação das informações prestadas;



PODER JUDICIÁRIO
CONSELHO DA JUSTIÇA FEDERAL

c) Caso uma certificação não seja mais válida, será aceita a nova certificação que substituiu à anterior;

d) As certificações técnicas exigidas devem estar válidas;

3.1.8 O CJF poderá a qualquer momento recusar o atendimento dos serviços por profissionais que não atendam aos requisitos de qualificação especificados. A DETENTORA terá o prazo de 2 (dois) dias úteis a contar da data de recusa para apresentar a documentação do novo profissional;

3.1.9 Será considerado como período de transição, os 10 (dez) dias corridos contados a partir da entrega da documentação completa da equipe de profissionais na forma dos subitens anteriores. Neste período a DETENTORA antecessora atuará conjuntamente com a recém- DETENTORA, priorizando a documentação e retenção de conhecimento para a continuidade dos serviços de TI e a mitigação de impacto nas atividades dos usuários de tais serviços;

3.1.10 A DETENTORA deverá iniciar a prestação dos serviços em; no máximo; 20 (vinte) dias corridos após a emissão da Ordem de Serviço – OS.

3.1.11 Não ocorrerá período de transição caso não ocorra a substituição da empresa prestadora de serviços. A prestação dos serviços deverá seguir o Cronograma de Atividades, conforme Anexo V do Termo de Referência.

3.1.12 O período inicial de 90 (noventa) dias após a emissão da Ordem de Serviço Rotineira - OSR, será considerado como período de estabilização da operação dos serviços, durante o qual os indicadores de serviço não atingidos terão aplicadas as glosas da tabela do Anexo I do termo de referência, conforme os seguintes critérios:

a) Nos primeiros 30 (trinta) dias: aplicar-se-á efetivamente 25% (vinte e cinco por cento) dos pontos previstos na tabela do Anexo I do termo de referência, para cada ocorrência de indicador de serviço não atingido;

b) Do 31º ao 60º dia: aplicar-se-á efetivamente 50% (cinquenta por cento) dos pontos previstos na tabela do Anexo I do termo de referência, para cada ocorrência de indicador de serviço não atingido;

c) Do 61º ao 90º dia: aplicar-se-á efetivamente 75% (setenta e cinco por cento) dos pontos previstos na tabela do Anexo I do termo de referência, para cada ocorrência de indicador de serviço não atingido;

d) Após 90 (noventa): aplicar-se-ão integralmente os pontos previstos na tabela do Anexo I do termo de referência, para cada ocorrência de indicador de serviço não atingido.

3.1.13 Caso haja prorrogação da vigência contratual, não haverá novo período de estabilização;

3.1.14 Ao final do contrato de prestação dos serviços, a empresa DETENTORA deverá fornecer, pelo período 90 (noventa) dias corridos, todas as informações necessárias à transição para a nova DETENTORA, além de elaborar e atualizar toda a documentação que por ventura não tenha sido devidamente gerada ou atualizada durante o período de vigência do contrato;

3.1.15 A DETENTORA deverá responsabilizar-se pela transição inicial e final dos serviços, absorvendo as atividades de forma a documentá-las minuciosamente para que os repasses de informações, conhecimentos e procedimentos, no final dos contratos, aconteçam de forma precisa e responsável;

3.1.16 Quando houver necessidade de qualquer alteração na equipe de profissionais que prestam o serviço no ÓRGÃO GERENCIADOR, a



PODER JUDICIÁRIO
CONSELHO DA JUSTIÇA FEDERAL

DETENTORA deverá apresentar os documentos comprobatórios de qualificação deste(s) profissional(ais) antes do início de suas atividades no ÓRGÃO GERENCIADOR.

3.1.17 Em conformidade com a Instrução Normativa CJF-INN-2016/00001 e as Resoluções CNJ nº 169/2013 e nº 183/2013, o gestor do contrato irá acompanhar a presença dos funcionários da DETENTORA alocados para prestar serviço nas dependências do CJF. Para tal, será utilizado um sistema de ponto eletrônico do ÓRGÃO GERENCIADOR. O registro do ponto neste sistema será obrigatório para todos os funcionários da DETENTORA que prestarem serviço nas dependências do Conselho;

3.1.18 Para a realização da monitoração proativa do ambiente tecnológico, a DETENTORA deverá oferecer serviço SMS (Short Message Service) ou mensageria instantânea (WHATSAPP), para que sejam enviadas mensagens aos prestadores de serviço e aos gestores de TI conforme a geração de alertas dos softwares de monitoração. É de responsabilidade da DETENTORA o custo da contratação deste serviço;

3.1.19 Todos os profissionais da DETENTORA alocados para a prestação dos serviços objeto do Termo de Referência deverão ter vínculo com a DETENTORA, baseado na CLT.

3.2 Encaminhamento de Demandas

3.2.1 Os serviços deverão ser executados somente após a emissão de Ordens de Serviços, com a obrigatória autorização pelo ÓRGÃO GERENCIADOR;

3.2.2 As Ordens de Serviços deverão ser classificadas pelo ÓRGÃO GERENCIADOR conforme nível e continuidade de execução:

- a) Transição: entendida como o processo de transferência dos conhecimentos e competências necessárias para prover a continuidade dos serviços contratados ou executados;
- b) Rotineira: atividades contínuas, realizáveis periodicamente, emitidas para execução durante a vigência do contrato. Podendo, mediante realinhamento, ter novas atividades inseridas ou excluídas no decorrer da vigência contratual, quando passará a vigorar nova versão de OSR;
- c) Exclusiva: atividades de natureza não contínua, emitidas a partir da demanda do ÓRGÃO GERENCIADOR.

3.2.3 Nas Ordens de Serviços deverão constar:

- a) Número de controle: identificação em ordem sequencial;
- b) Área demandante: que deverá assinar a solicitação e o aceite e contabilização periódica das atividades, para efeito dos pagamentos;
- c) Objetivo da tarefa: definição das expectativas e justificativas para realização das atividades;
- d) Data de início e conclusão das atividades (exceto rotineira): definição do período de realização, inclusive dos períodos e horários realizáveis para serviços que impactem com os trabalhos de usuários;
- e) Listagem das atividades a serem realizadas, especificadas, quantificadas e classificadas conforme complexidade;



PODER JUDICIÁRIO
CONSELHO DA JUSTIÇA FEDERAL

- f)** Resultado e Nível de Qualidade definido para a tarefa;
- g)** Glosa e Penalidades, em caso de descumprimento, e de acordo com a previsão contratual;
- h)** Responsáveis pela fiscalização e autorização no ÓRGÃO GERENCIADOR;
- i)** Responsável pelo aceite na DETENTORA.

3.2.4 Atestação técnica:

- a)** A Ordem de Serviço somente poderá ser encerrada quando todos os objetivos propostos forem plenamente atingidos, e todos os produtos e serviços realizados e entregues com a qualidade demandada e devidamente atestada pelo demandante e pelo gestor do ÓRGÃO GERENCIADOR;
- b)** Antes do fechamento de cada OS a DETENTORA consultará o representante indicado pela DETENTORA, que avaliará e atestará o serviço realizado;
- c)** Uma requisição de serviço ou incidente encerrado sem anuência do ÓRGÃO GERENCIADOR ou sem que tenha sido de fato resolvido será reaberto e os prazos serão contados a partir da abertura original da requisição de serviço ou incidente, inclusive para efeito de aplicação das sanções previstas.

3.3 Níveis Mínimos de Serviços Exigidos

- 3.3.1** Os níveis mínimos de serviços são critérios objetivos e mensuráveis que visam aferir e avaliar diversos fatores relacionados com os serviços contratados, quais sejam: qualidade, desempenho, disponibilidade, abrangência/cobertura e segurança;
- 3.3.2** Os níveis mínimos de serviços estão detalhados no Anexo I do termo de referência – Níveis Mínimos de Serviço;
- 3.3.3** O não atingimento de um mesmo nível de serviços durante 3 (três) meses consecutivos ou 5 (cinco) meses intervalados, em um período de 12 (doze) meses, ensejará a execução das Sanções Administrativas previstas no contrato;
- 3.3.4** A DETENTORA sofrerá glosa de 1% (um por cento), sobre o valor da fatura, a cada 15 pontos ou percentual proporcional ao número de pontos, levando em consideração a relação: glosa de 1% a cada 15 pontos;
- 3.3.5** As metas devem ser medidas do primeiro ao último dia de cada mês;
- 3.3.6** A meta exigida representa o parâmetro de valor exato (=), limite máximo (<=) ou limite mínimo (>=) que deve ser alcançado pela DETENTORA para cada um dos indicadores;
- 3.3.7** Os tempos serão contados a partir do recebimento da solicitação do cliente. No caso da contagem em dias, a contagem é efetuada dia a dia, incluindo o primeiro e o último dia;
- 3.3.8** No caso da resolução de incidentes, se o mesmo não tiver a sua causa raiz conhecida, ou seja, existe um problema a ser resolvido, a DETENTORA é obrigada a aplicar uma solução de contorno na resolução do incidente para que o serviço volte à sua operação padrão;
- 3.3.9** Os níveis de serviço serão mensurados de forma automatizada e não poderão ser manipulados pela DETENTORA;



PODER JUDICIÁRIO
CONSELHO DA JUSTIÇA FEDERAL

3.3.10 A DETENTORA se responsabilizará somente pelos índices que reflitam as requisições de serviços e incidentes designados a ela, não poderá ser responsabilizada por chamados pendentes de fornecedores/prestadores de serviços externos ou encaminhados a outros níveis, ou situações que dependam de terceiros, que, desta forma, não poderão ser computados;

3.3.11 O termo “Hora do restabelecimento” refere-se a hora em que o incidente de indisponibilidade foi efetivamente resolvido;

3.3.12 Por requisições de serviço e incidentes reabertos entende-se que são requisições de serviço ou incidentes que foram dados como resolvidos, porém os mesmos ainda permanecem pendentes de resolução;

3.3.13 Por horário normal de produção entende-se sendo o período entre 09:00 e 20:00, de segunda à sexta-feira, excetuando-se os feriados;

3.3.14 Sobre o índice de supervisão e intervenção proativa:

a) A manutenção proativa visa detectar com antecedência os possíveis problemas que possam vir a ocorrer devido à necessidade de suporte, como aplicação de patches, correções de firmware, ou algum outro dispositivo que possa impactar no desempenho ou disponibilidade dos Sistemas Monitorados pela DETENTORA, podendo ser visualizados mediante acompanhamento e análise diária de desempenho e produção dos recursos e também através de testes rotineiros de stress e carga;

b) Deverão ser analisados em tempo real os desempenhos dos serviços críticos inserindo as manutenções e os suportes necessários de maneira a proporcionar a continuidade e disponibilidade dos serviços. Diariamente deverão ser analisados os registros internos dos hardwares e softwares para avaliação e detecção de intervenções necessárias, submetendo-os ao DETENTORA para programação das intervenções que permitirem agendamento;

c) É obrigação da DETENTORA efetuar as intervenções necessárias em tempo de produção para sanar os erros apresentados nesta fase e que sejam de sua competência. Se as intervenções propostas forem para melhoria de desempenho ou compatibilização de ambiente e permitirem agendamento deverão ser submetidas para aprovação do DETENTOR antes de execução.

3.4 Os serviços gerenciados de segurança, serão executados conforme os itens 6.1 a 6.26 da cláusula 6 do Termo de Referência.

3.5 Os serviços de operação e atendimento a requisições, serão executados conforme os itens 7.1 a 7.9 da cláusula 7 do Termo de Referência.

3.6 Os serviços de gestão de incidentes de segurança (CSIRT - Blue Team), serão executados conforme os itens 8.1 a 8.23 da cláusula 8 do Termo de Referência.

3.7 Os serviços de gestão de vulnerabilidades, serão executados conforme os itens 9.1 a 9.26 da cláusula 9 do Termo de Referência.

3.8 Os serviços de monitoramento e visibilidade de ataques cibernéticos, serão executados conforme os itens 10.3 e 10.4 da cláusula 10 do Termo de Referência.

3.9 Os serviços de orquestração, automação e resposta de segurança (**SOAR**), serão executados conforme os itens 11.3 a 11.5 da cláusula 11 do Termo de Referência.

3.10 Os serviços de testes de invasão (**RED TEAM**), serão executados conforme os itens 12.2 a 12.16 da cláusula 12 do Termo de Referência.



PODER JUDICIÁRIO
CONSELHO DA JUSTIÇA FEDERAL

CLÁUSULA QUARTA – DO RECEBIMENTO

4.1 O recebimento e a aceitação obedecerão ao disposto nos arts. 73 a 76 da Lei n. 8.666/1993.

4.2 Caso o ÓRGÃO GERENCIADOR constatare que os serviços foram prestados em desacordo com o contrato, com defeito, fora de especificação ou incompletos, a DETENTORA será formalmente notificada, sendo interrompidos os prazos de recebimento, e os pagamentos suspensos, até que a situação seja sanada.

4.3 O recebimento definitivo não exclui a responsabilidade civil da DETENTORA pela solidez e segurança do serviço, nem a ético-profissional pela perfeita execução do contrato, dentro dos limites estabelecidos pela lei ou por este instrumento.

CLÁUSULA QUINTA – DA VALIDADE

5.1 A validade desta ata de registro de preços será de 12 (doze) meses, contados a partir da data de assinatura do CJF.

CLÁUSULA SEXTA – DO VALOR

6.1 O valor mensal estimado do contrato para cobrir as despesas relativas à Ata de Registro de Preços é de **R\$ 0000,00** (por extenso), conforme discriminado na cláusula 2.

CLÁUSULA SÉTIMA – DA DOTAÇÃO ORÇAMENTÁRIA

7.1 As despesas decorrentes desta contratação, no corrente exercício, correrão à conta dos recursos consignados, inclusive os suplementados, ao Conselho da Justiça Federal, no Orçamento Geral da União, no Programa de Trabalho Resumido - PTRES: (_____), Natureza da Despesa - ND: (_____)

7.2 A despesa para o exercício subsequente será alocada à dotação orçamentária prevista para atendimento dessa finalidade, a ser consignada ao ÓRGÃO GERENCIADOR, na respectiva Lei Orçamentária Anual.

CLÁUSULA OITAVA - DA GARANTIA

8.1 A DETENTORA apresentará, nos termos do art. 56 da Lei n. 8.666/1993, em até 20 (vinte) dias úteis, contados da assinatura do instrumento contratual, garantia de execução do contrato no valor de **R\$ 000** _____(extenso), correspondente a 3% (cinco por cento) do valor total estimado da contratação, tendo como beneficiário o ÓRGÃO GERENCIADOR, quais sejam:



PODER JUDICIÁRIO
CONSELHO DA JUSTIÇA FEDERAL

- a) Caução em dinheiro ou títulos da dívida pública; ou
- b) Seguro – garantia; ou
- c) Fiança bancária.

8.1.1 A DETENTORA, caso opte pela modalidade de garantia caução, declara que manterá conta de caução específica para o depósito de valores oferecidos em garantia/caução referentes exclusivamente a contratos firmados com o ÓRGÃO GERENCIADOR.

8.1.2 No caso de a DETENTORA optar pela caução em dinheiro, esta deverá ser feita na Caixa Econômica Federal, conforme Decreto-lei n. 1.737, de 21/12/1979.

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

- a) prejuízos advindos do não cumprimento do objeto do contrato;
- b) prejuízos diretos causados ao ÓRGÃO GERENCIADOR, decorrentes de culpa ou dolo durante a execução do contrato;
- c) multas moratórias e punitivas aplicadas à DETENTORA;
- d) obrigações trabalhistas e previdenciárias de qualquer natureza, não adimplidas pela DETENTORA, quando couber;

8.2.1 Caso o valor da garantia venha a ser utilizado em pagamento de qualquer obrigação atribuída à DETENTORA, está se obriga a efetuar a respectiva reposição no prazo máximo de 10 (dez) dias úteis, a contar da data do recebimento da comunicação pelo ÓRGÃO GERENCIADOR.

8.2.2 Prorrogado o prazo de vigência ou alterado o valor do contrato, fica a DETENTORA obrigada a renovar a garantia, no mesmo percentual e modalidades constantes desta cláusula, em até 20 (vinte) dias úteis, contados da data de assinatura do respectivo instrumento contratual.

8.2.3 A garantia apresentada em desacordo com os requisitos e coberturas previstos neste instrumento será devolvida à DETENTORA, que disporá do prazo improrrogável de 10 (dez) dias úteis para a regularização da pendência.

8.2.4 O ÓRGÃO GERENCIADOR poderá executar a garantia para ressarcimento dos valores que a DETENTORA passe a lhe dever em virtude da ocorrência de qualquer das situações expressamente previstas neste contrato e na legislação pertinente, após a instauração de procedimento administrativo específico.

8.2.5 O valor da garantia reverterá, integralmente, em favor do ÓRGÃO GERENCIADOR, ou pelo saldo que apresentar, no caso de rescisão contratual por culpa exclusiva da DETENTORA, sem prejuízo das perdas e danos porventura verificados.

8.2.6 O ÓRGÃO GERENCIADOR poderá utilizar o valor da garantia prestada para descontar, entre outros, os valores referentes a eventuais multas aplicadas à DETENTORA, bem como nos casos decorrentes de inadimplemento contratual, e de indenização por danos causados ao Patrimônio da União ou de terceiros, ocorridos nas suas dependências.



PODER JUDICIÁRIO
CONSELHO DA JUSTIÇA FEDERAL

8.2.7 A garantia deverá ser prestada com validade de 3 (três) meses após o término da vigência do contrato e será liberada ou restituída ante a comprovação do adimplemento total das obrigações contratuais, desde que não haja pendências.

8.2.8 O termo da garantia será restituído à DETENTORA após o cumprimento integral de todas as obrigações contratuais.

8.2.9 Na ocorrência de qualquer inadimplemento das obrigações contratadas, o ÓRGÃO GERENCIADOR notificará a empresa seguradora da expectativa de sinistro com vistas a resguardar a administração de possíveis prejuízos, mediante provocação da unidade gestora responsável pelo acompanhamento da execução contratual, durante a vigência da apólice.

CLÁUSULA NONA – DAS PENALIDADES

9.1 O atraso injustificado no cumprimento do objeto, sujeitará a DETENTORA a multa, sobre o valor mensal do contrato, a título de mora, quais sejam:

9.1.1 MULTA MORATÓRIA de 0,5% (zero vírgula cinco por cento) sobre o valor mensal do contrato, por dia de atraso **na apresentação da nota fiscal de faturamento**, de acordo com os níveis de serviços e eventuais glosas apuradas pelo ÓRGÃO GERENCIADOR;

9.1.2 MULTA MORATÓRIA de 0,5% (zero vírgula cinco por cento) sobre o valor mensal do contrato, por dia de atraso **na apresentação da relação de profissionais** que prestarão os serviços alocados no ÓRGÃO GERENCIADOR;

9.1.3 MULTA MORATÓRIA de 0,5% (zero vírgula cinco por cento) do valor mensal do contrato por dia de atraso decorrido **em caso de descumprimento do prazo** estabelecido na cláusula DO CONTINGENCIAMENTO DOS ENCARGOS TRABALHISTAS referente a abertura da conta-depósito vinculada;

9.1.4 MULTA MORATÓRIA de 0,5% (zero vírgula cinco por cento) sobre o valor mensal do contrato por ocorrência em que o **profissional descumprir as exigências de vestimenta**, conforme determinado na PORTARIA CJF-POR-2018/00129 ou norma que vier a sucedê-la;

9.1.5 MULTA MORATÓRIA de 0,5% (zero vírgula cinco por cento) sobre o valor mensal do contrato por ocorrência em que o profissional **descumprir a norma sobre o controle de acesso**, a circulação e a permanência de pessoas no Conselho da Justiça Federal, conforme determinado na Portaria Ministro Presidente nº 34 de 02/02/2017 ou norma que vier a sucedê-la;

9.1.6 MULTA MORATÓRIA – de 1% (um por cento) sobre o valor mensal do contrato, a cada ocorrência em que a DETENTORA:

- a) Substituir profissional sem formalizar o ÓRGÃO GERENCIADOR;
- b) Deixar de afastar profissional que se conduza de modo inconveniente ou que não respeite as normas do CJF ou que não atenda às necessidades, num período de 24 (vinte e quatro) horas corridas a contar da notificação do DETENTOR;



PODER JUDICIÁRIO
CONSELHO DA JUSTIÇA FEDERAL

c) Deixar de alocar um novo profissional em caso de substituição, num período de 5 (cinco) dias úteis a contar da notificação do DETENTOR quando da substituição;

9.1.7 MULTA MORATÓRIA – de 1,5% (um vírgula cinco por cento) sobre o valor mensal do contrato, a cada ocorrência em que a DETENTORA:

a) Por motivo de negligência, imprudência ou imperícia na execução das atividades contratuais, causar qualquer dano físico ou lógico aos equipamentos do ÓRGÃO GERENCIADOR;

b) Descumprir Política, Norma ou Procedimento de Segurança da Informação do ÓRGÃO GERENCIADOR.

c) Deixar de comunicar formalmente ao ÓRGÃO GERENCIADOR sobre o desligamento de prestador de serviço (profissional que prestava serviço nas dependências do CJF e/ ou remotamente).

9.1.8 MULTA MORATÓRIA de 10% (dez por cento) do valor mensal do contrato pelo não atingimento de um mesmo nível de serviço previsto no ANEXO I, do termo de referência, durante 3 (três) meses consecutivos ou 5 (cinco) meses alternados, apurados em um período de 12 (doze meses);

9.1.9 MULTA MORATÓRIA de 20% (vinte por cento) do valor mensal do contrato pelo não atingimento de um mesmo nível de serviço previsto no ANEXO I, do termo de referência, durante 6 (seis) meses consecutivos ou 10 (cinco) meses não consecutivos, apurados em um período de 12 (doze meses);

9.1 10 Os indicadores fora das metas exigidas no ANEXO I do termo de referência – Níveis Mínimos de Serviço serão considerados como INEXECUÇÃO DOS **SERVIÇOS MENSAIS** do contrato conforme a tabela abaixo, sem prejuízo da aplicação da glosa referente ao indicador não atingido:

PORCENTAGEM ALCANÇADA DO NÍVEL DE SERVIÇO EM RELAÇÃO A META EXIGIDA NO ANEXO I do Termo de Referência	TIPO DE INEXECUÇÃO DOS SERVIÇOS MENSAIS
50% A 69,9%	PARCIAL
0% A 49,9%	TOTAL

Será aplicada:

a) **MULTA MORATÓRIA** de 10% (dez por cento) do valor mensal do contrato, em caso de INEXECUÇÃO PARCIAL DOS SERVIÇOS MENSAIS do contrato; ou

b) **MULTA MORATÓRIA** de 20% (vinte por cento) do valor mensal do contrato, em caso de INEXECUÇÃO TOTAL DOS SERVIÇOS MENSAIS do contrato;

9 .2 Pela inexecução total ou parcial o ÓRGÃO GERENCIADOR poderá, nos termos do art. 87 da Lei n. 8.666/1993, aplicar as seguintes sanções:

a) advertência;

b) **MULTA COMPENSATÓRIA** de 10% (dez por cento) do valor total do contrato, em caso de INEXECUÇÃO PARCIAL das obrigações contratuais;



PODER JUDICIÁRIO
CONSELHO DA JUSTIÇA FEDERAL

- c) MULTA COMPENSATÓRIA de 20% (vinte por cento) do valor total do contrato, em caso de inexecução total das obrigações contratuais;
- d) suspensão temporária
- e) declaração de inidoneidade

9.3 Nos termos da Lei n. 10.520/2002, art. 7º, o ÓRGÃO GERENCIADOR poderá aplicar impedimento de licitar àquele que:

Ocorrência	Pena
a) fizer declaração falsa ou apresentar documentação falsa:	Impedimento do direito de licitar e contratar com a União e descredenciamento do Sistema de Cadastramento Unificado de Fornecedores – SICAF, pelo período de 24 (vinte e quatro) meses;
b) falhar na execução do contrato:	Impedimento do direito de licitar e contratar com a União e descredenciamento do SICAF pelo período de 12 (doze) meses;
c) fraudar na execução do contrato:	Impedimento do direito de licitar e contratar com a União e descredenciamento do SICAF pelo período de 30 (trinta) meses;
d) comportar-se de modo inidôneo:	Impedimento do direito de licitar e contratar com a União e descredenciamento do SICAF pelo período de 24 (vinte e quatro) meses;
e) cometer fraude fiscal:	Impedimento do direito de licitar e contratar com a União e descredenciamento do SICAF pelo período de 40 (quarenta) meses;

9.3.1 O ÓRGÃO GERENCIADOR, para aplicação da penalidade prevista no item anterior, adotará os critérios previstos na Instrução Normativa n. 1, de 13/10/2017, da Presidência da República, publicada no DOU, em 16/10/2017 (n. 198, Seção 1, pag. 5).

9.4 A não manutenção das condições de habilitação da DETENTORA ao longo da execução do Contrato, ensejará a rescisão contratual unilateral pelo ÓRGÃO GERENCIADOR, após regular procedimento administrativo e garantido o direito ao contraditório e à ampla defesa, e ainda a aplicação de multa de 10% sobre o valor da prestação inadimplida.

9.5 A reabilitação será concedida sempre que a DETENTORA ressarcir a Administração pelos prejuízos resultantes, e depois de decorrido o prazo de suspensão temporária, se aplicada

9.6 As sanções de multa podem ser aplicadas à DETENTORA juntamente com a de advertência, suspensão temporária do direito de participar de licitação e impedimento de contratar com o Conselho da Justiça Federal e declaração de inidoneidade para licitar ou contratar com a Administração Pública, descontando-a do pagamento a ser efetuado.

9.7 A critério da autoridade competente do ÓRGÃO GERENCIADOR, com fundamento nos princípios da proporcionalidade e razoabilidade, as penalidades poderão ser relevadas ou atenuadas, em razão de circunstâncias fundamentadas, mediante comprovação dos fatos e,



PODER JUDICIÁRIO
CONSELHO DA JUSTIÇA FEDERAL

desde que formuladas por escrito, no prazo máximo de 5 (cinco) dias úteis, contados da data da notificação.

9.8 A aplicação das sanções previstas nesta cláusula será realizada mediante processo administrativo específico, mediante comunicação à DETENTORA da penalidade, sendo assegurado, em todos os casos, o contraditório e a ampla defesa, no prazo de 5 (cinco) dias, contados do recebimento da comunicação.

9.9 Em caso de aplicação de multa, o valor poderá ser descontado da garantia prestada, dos pagamentos eventualmente devidos à DETENTORA, ser recolhido ao Tesouro por meio Guia de Recolhimento da União – GRU, ou cobrado judicialmente, nos termos do § 3º do art. 86 da Lei n. 8.666/1993.

9.10 O atraso no recolhimento de multas será corrigido monetariamente pela variação acumulada do Índice Nacional de Preços ao Consumidor Amplo/IPCA, calculado e divulgado pelo Instituto Brasileiro de Geografia e Estatística/IBGE

9.11 O ÓRGÃO GERENCIADOR promoverá o registro no Sistema de Cadastramento Unificado de Fornecedores - SICAF de toda e qualquer penalidade imposta à DETENTORA.

CLÁUSULA DÉCIMA – DO CADASTRO RESERVA

10.1 O cadastro de reserva, a convocação, a avaliação das condições de habilitação observará o disposto na cláusula X do Edital n. 000/2020, bem como o disposto no parágrafo único do art. 13 e arts. 20 e 21 do Decreto n. 7.892/2013.

CLÁUSULA DÉCIMA PRIMEIRA – DO CONTROLE DE ALTERAÇÃO DE PREÇOS

11.1 Os preços registrados poderão ser revistos em face de:

- a)** eventual redução daqueles praticados no mercado;
- b)** fato que eleve o custo dos serviços ou bens registrados.

11.2 Será realizada, periodicamente, pesquisa de mercado visando à comprovação da vantagem dos preços registrados, exigência contida no inciso XI do art. 9º do Decreto n. 7.892/2013.

11.3 Quando o preço registrado se tornar superior ao preço praticado no mercado, por motivo superveniente, o CJF convocará os fornecedores a negociarem a redução dos preços aos valores de mercado.

11.3.1 Os fornecedores que não aceitarem reduzir seus preços aos valores de mercado serão liberados do compromisso assumido, sem aplicação de penalidade.

11.3.2 A ordem de classificação dos fornecedores que aceitarem reduzir seus preços aos valores de mercado observará a classificação original.

11.4 Quando o preço de mercado se tornar superior aos preços registrados e o FORNECEDOR não puder cumprir o compromisso, o CJF poderá:



PODER JUDICIÁRIO
CONSELHO DA JUSTIÇA FEDERAL

- a)** revisar os preços registrados, mediante comprovação da elevação dos custos pelo FORNECEDOR;
- b)** liberar o fornecedor do compromisso assumido, caso a comunicação ocorra antes do pedido de fornecimento, e sem aplicação da penalidade, se confirmada a veracidade dos motivos e comprovantes apresentados;
- c)** convocar os demais fornecedores para assegurarem igual oportunidade de negociação.

11.5 Não havendo êxito nas negociações, o CJF procederá à revogação da ata de registro de preços, adotando as medidas cabíveis para obtenção da contratação mais vantajosa.

11.6 Serão considerados preços de mercado os que forem iguais ou inferiores à média daqueles apurados pelo CJF.

CLÁUSULA DÉCIMA SEGUNDA– DO CANCELAMENTO DO REGISTRO DE PREÇOS

12.1 O FORNECEDOR terá seu registro cancelado por intermédio de procedimento administrativo específico, assegurados o contraditório e a ampla defesa:

12.1.1 A pedido, quando:

- a)** comprovada a impossibilidade de cumprir as exigências da ata, por ocorrência de caso fortuito ou de força maior;
- b)** o seu preço registrado se tornar, comprovadamente, inexequível em função da elevação dos preços de mercado e dos insumos que compõem os seus custos, desde que a comunicação ocorra antes do pedido de fornecimento.

12.1.2 Por iniciativa do CJF, quando o fornecedor:

- a)** não aceitar reduzir o preço registrado, se este se tornar superior àqueles praticados no mercado;
- b)** não mantiver todas as condições de habilitação e qualificação exigidas na licitação;
- c)** não cumprir as obrigações decorrentes da ata de registro de preços;
- d)** não comparecer ou recusar-se a retirar, no prazo estabelecido, os pedidos decorrentes da ata de registro de preços;
- e)** não retirar a nota de empenho ou instrumento equivalente no prazo estabelecido pelo CJF, sem justificativa aceitável, como previsto no inciso II do art. 20 do Decreto n. 7.892/2013;
- f)** sofrer sanção prevista no inciso IV do *caput* do art. 87 da Lei n. 8.666, de 1993, ou no art. 7º da Lei n. 10.520, de 2002.
- g)** por fato superveniente, decorrente de caso fortuito ou força maior, que prejudique o cumprimento da ata, por razões de interesse público.



PODER JUDICIÁRIO
CONSELHO DA JUSTIÇA FEDERAL

12.2 O cancelamento do preço registrado implica a cessação de todas as atividades do FORNECEDOR relativas ao respectivo registro.

12.3 Nos casos em que o FORNECEDOR sofrer processos de fusão, cisão ou incorporação, será admitida a continuação deste instrumento, desde que a execução desta ata não seja afetada e que o FORNECEDOR mantenha o fiel cumprimento dos termos deste documento e as condições de habilitação.

CLÁUSULA DÉCIMA TERCEIRA - DA CONTRATAÇÃO

13.1 Após a assinatura da ata de registro de preços e autorizado o fornecimento/serviço, o CJF convocará a empresa para, dentro de 5 (cinco) dias úteis, após regular convocação, assinar o contrato, cuja minuta integra o edital de licitação.

**CLÁUSULA DÉCIMA QUARTA -
DA DIVULGAÇÃO DA ATA DE REGISTRO DE PREÇOS**

14.1 Em conformidade com o disposto na Lei n. 8.666/1993, art. 61, parágrafo único, o presente instrumento de aditamento será publicado no Diário Oficial da União, em forma de extrato.

CLÁUSULA DÉCIMA QUINTA – DO FORO

15.1 Para dirimir quaisquer conflitos oriundos desta ata, é competente o foro do Juízo da Seção Judiciária do Distrito Federal, com expressa renúncia a qualquer outro, por mais privilegiado que seja, no que se refere a qualquer ação ou medida judicial originada ou referente a este instrumento.

CLÁUSULA DÉCIMA SEXTA– DAS DISPOSIÇÕES FINAIS

16.1 Nos termos do §1º do art. 12 do Decreto 7.892/2013, é vedado efetuar acréscimos nos quantitativos fixados nesta ata.

16.2 NÃO serão permitidas adesões à ata (caronas), previstas no artigo 22 do Decreto n. 7.892 (de 23 janeiro 2013). (Acórdão TCU n. 1.297/2015 – Plenário, TC 003.377/2015-6, relator Ministro Bruno Dantas, 27.5.2015)

E, por estarem assim de pleno acordo, assinam as partes este instrumento, na forma eletrônica, para todos os fins de direito.

Juíza Federal SIMONE DOS SANTOS LEMOS FERNANDES
Secretária-Geral do Conselho da Justiça Federal

SIGNATÁRIO EMPRESA



PODER JUDICIÁRIO
CONSELHO DA JUSTIÇA FEDERAL

MÓDULO III DO EDITAL 1/2020
MINUTA DE CONTRATO

CONTRATO CJF N. 000/0000

que entre si celebram o **CONSELHO DA JUSTIÇA FEDERAL** e a **(NOME DA EMPRESA)**, para contratação de Serviços Gerenciados de Segurança da Informação para o Conselho de Justiça Federal – CJF.

MINUTA

O CONSELHO DA JUSTIÇA FEDERAL - CJF, órgão integrante do Poder Judiciário, inscrito no CNPJ/MF n. 00.508.903/0001-88, com sede no Setor de Clubes Esportivos Sul, Trecho III, Polo 8, Lote 9, Brasília - DF, doravante denominado **CONTRATANTE**, neste ato representado por sua Secretária-Geral, a Exma. Juíza Federal **SIMONE DOS SANTOS LEMOS FERNANDES**, brasileira, CPF/MF n. 418.381.906-78, Carteira de Identidade n. 1075089 – SSP - MG, residente em Brasília - DF, e a **(NOME DA EMPRESA)**, pessoa jurídica de direito privado, inscrita no CNPJ/MF n. 0000, estabelecida na (endereço), doravante denominada **CONTRATADA**, neste ato representada por seu (sua) (cargo/função), o (a) senhor (a) **(nome SIGNATÁRIO)**, brasileiro (a), CPF/MF n. 0000 e Carteira de Identidade n. 0000 – SSP/00, residente em (domicílio), celebram o presente contrato com fundamento na Lei n. 8.666/1993 e alterações, Lei n. 12.846/2013 em conformidade com as informações constantes do Processo SEI n. 0001989-89.2019.4.90.8000, mediante as cláusulas e condições a seguir:

CLÁUSULA PRIMEIRA - DO OBJETO

- 1.1 Constitui objeto deste contrato a contratação de Serviços Gerenciados de Segurança da Informação para o Conselho de Justiça Federal – CJF de acordo com as especificações técnicas contidas no Termo de Referência e seus anexos, englobando os seguintes serviços:
- a) Serviço de operação e atendimento a requisições.
 - b) Serviço de gestão de incidentes de segurança (CSIRT - Blue Team).
 - c) Serviço de gestão de vulnerabilidades.



PODER JUDICIÁRIO
CONSELHO DA JUSTIÇA FEDERAL

- d) Serviço de monitoramento e visibilidade de ataques cibernéticos.
- e) Serviço de orquestração, automação e resposta de segurança (SOAR).
- f) Serviço de testes de invasão (Red Team).

1.2 As especificações constantes do edital de licitação (Pregão Eletrônico n. 00/0000), do termo de referência e da proposta comercial da CONTRATADA, fazem parte deste instrumento, independentemente de transcrição.

CLÁUSULA SEGUNDA – DA EXECUÇÃO E DOS SERVIÇOS

2.1 Dos prazos e da execução dos serviços:

2.1.1 A CONTRATADA deverá iniciar a prestação dos serviços objeto deste termo, de acordo com o cronograma apresentado no anexo V do Termo de Referência;

2.1.2 Para execução dos serviços, será implementado método de trabalho baseado no conceito de delegação de responsabilidade. Esse conceito define o CONTRATANTE como responsável pela gestão do contrato e pela atestação da aderência aos padrões de qualidade exigidos dos serviços entregues e a CONTRATADA como responsável pela execução dos serviços e gestão dos profissionais a seu cargo;

2.1.3 A CONTRATADA será responsável pela execução dos serviços e pelo acompanhamento diário da qualidade e dos níveis de serviço alcançados com vistas a efetuar eventuais ajustes e correções. Quaisquer problemas que venham a comprometer o bom andamento dos serviços ou o alcance dos níveis de serviço estabelecidos devem ser imediatamente comunicados por escrito ao CONTRATANTE;

2.1.4 Após a assinatura do contrato, será emitida Ordem de Serviço de Transição – OST com o objetivo de viabilizar a transferência de conhecimentos e o repasse dos serviços à nova CONTRATADA;

2.1.5 A CONTRATADA deverá apresentar, no prazo máximo de 10 (dez) dias corridos a partir da emissão da Ordem de Serviço de Transição - OST, carta de apresentação juntamente com os documentos comprobatórios (certificados oficiais) contendo os respectivos dados pessoais e informações quanto à habilitação e qualificação profissional de todos os profissionais que serão alocados na execução dos serviços no CONTRATANTE;

2.1.6 Quando da apresentação dos documentos comprobatórios de qualificação, a CONTRATADA deverá observar atenciosamente à qualificação exigida, conforme descrito no Item 13 do Termo de Referência- Dos perfis profissionais. Caso a documentação não atenda às exigências deste item, a CONTRATADA deverá apresentar documentação de um novo profissional que atenda as exigências, dentro do prazo estabelecido, antes do início das atividades;

2.1.7 Para fins de comprovação de atendimento aos requisitos de qualificação profissional serão aceitos:

- a) Cópia autenticada de certificados ou diplomas que comprovem a conclusão dos cursos exigidos. No caso dos cursos de nível médio e/ou superior deverão ser apresentados os diplomas;



PODER JUDICIÁRIO
CONSELHO DA JUSTIÇA FEDERAL

b) Todos os documentos apresentados estarão sujeitos à diligência do CONTRATANTE para fins de confirmação das informações prestadas;

c) Caso uma certificação não seja mais válida, será aceita a nova certificação que substituiu a anterior;

d) As certificações técnicas exigidas devem estar válidas;

2.1.8 O CJF poderá a qualquer momento recusar o atendimento dos serviços por profissionais que não atendam aos requisitos de qualificação especificados. A CONTRATADA terá o prazo de 2 (dois) dias úteis a contar da data de recusa para apresentar a documentação do novo profissional;

2.1.9 Será considerado como período de transição, os 10 (dez) dias corridos contados a partir da entrega da documentação completa da equipe de profissionais na forma dos subitens anteriores. Neste período a CONTRATADA antecessora atuará conjuntamente com a recém-CONTRATADA, priorizando a documentação e retenção de conhecimento para a continuidade dos serviços de TI e a mitigação de impacto nas atividades dos usuários de tais serviços;

2.1.10 A CONTRATADA deverá iniciar a prestação dos serviços em; no máximo; 20 (vinte) dias corridos após a emissão da Ordem de Serviço – OS.

2.1.11 Não ocorrerá período de transição caso não ocorra a substituição da empresa prestadora de serviços. A prestação dos serviços deverá seguir o Cronograma de Atividades, conforme Anexo V do Termo de Referência.

2.1.12 O período inicial de 90 (noventa) dias após a emissão da Ordem de Serviço Rotineira - OSR, será considerado como período de estabilização da operação dos serviços, durante o qual os indicadores de serviço não atingidos terão aplicadas as glosas da tabela do Anexo I do termo de referência, conforme os seguintes critérios:

a) Nos primeiros 30 (trinta) dias: aplicar-se-á efetivamente 25% (vinte e cinco por cento) dos pontos previstos na tabela do Anexo I do termo de referência, para cada ocorrência de indicador de serviço não atingido;

b) Do 31º ao 60º dia: aplicar-se-á efetivamente 50% (cinquenta por cento) dos pontos previstos na tabela do Anexo I do termo de referência, para cada ocorrência de indicador de serviço não atingido;

c) Do 61º ao 90º dia: aplicar-se-á efetivamente 75% (setenta e cinco por cento) dos pontos previstos na tabela do Anexo I do termo de referência, para cada ocorrência de indicador de serviço não atingido;

d) Após 90 (noventa): aplicar-se-ão integralmente os pontos previstos na tabela do Anexo I do termo de referência, para cada ocorrência de indicador de serviço não atingido.

2.1.13 Caso haja prorrogação da vigência contratual, não haverá novo período de estabilização;

2.1.14 Ao final do contrato de prestação dos serviços, a empresa CONTRATADA deverão fornecer, pelo período 90 (noventa) dias corridos, todas as informações necessárias à transição para a nova CONTRATADA, além de elaborar e atualizar toda a documentação que por ventura não tenha sido devidamente gerada ou atualizada durante o período de vigência do contrato;

2.1.15 A CONTRATADA deverá responsabilizar-se pela transição inicial e final dos serviços, absorvendo as atividades de forma a documentá-las minuciosamente para que os repasses de



PODER JUDICIÁRIO
CONSELHO DA JUSTIÇA FEDERAL

informações, conhecimentos e procedimentos, no final dos contratos, aconteçam de forma precisa e responsável;

2.1.16 Quando houver necessidade de qualquer alteração na equipe de profissionais que prestam o serviço no CONTRATANTE, a CONTRATADA deverá apresentar os documentos comprobatórios de qualificação deste(s) profissional(ais) antes do início de suas atividades no CONTRATANTE.

2.1.17 Em conformidade com a Instrução Normativa CJF-INN-2016/00001 e as Resoluções CNJ nº 169/2013 e nº 183/2013, o gestor do contrato irá acompanhar a presença dos funcionários da CONTRATADA alocados para prestar serviço nas dependências do CJF. Para tal, será utilizado um sistema de ponto eletrônico da CONTRATADA. O registro do ponto neste sistema será obrigatório para todos os funcionários da CONTRATADA que prestarem serviço nas dependências do Conselho;

2.1.18 Para a realização da monitoração proativa do ambiente tecnológico, a CONTRATADA deverá oferecer serviço SMS (Short Message Service) ou mensageria instantânea (WHATSAPP), para que sejam enviadas mensagens aos prestadores de serviço e aos gestores de TI conforme a geração de alertas dos softwares de monitoração. É de responsabilidade da CONTRATADA o custo da contratação deste serviço;

2.1.19 Todos os profissionais da CONTRATADA alocados para a prestação dos serviços objeto do Termo de Referência deverão ter vínculo com a CONTRATADA, baseado na CLT.

2.2 Encaminhamento de Demandas

2.2.1 Os serviços deverão ser executados somente após a emissão de Ordens de Serviços, com a obrigatoria autorização pelo CONTRATANTE;

2.2.2 As Ordens de Serviços deverão ser classificadas pelo CONTRATANTE, conforme nível e continuidade de execução:

- a) Transição: entendida como o processo de transferência dos conhecimentos e competências necessárias para prover a continuidade dos serviços contratados ou executados;
- b) Rotineira: atividades contínuas, realizáveis periodicamente, emitidas para execução durante a vigência do contrato. Podendo, mediante realinhamento, ter novas atividades inseridas ou excluídas no decorrer da vigência contratual, quando passará a vigorar nova versão de OSR;
- c) Exclusiva: atividades de natureza não contínua, emitidas a partir da demanda do CONTRATANTE.

2.2.3 Nas Ordens de Serviços deverão constar:

- a) Número de controle: identificação em ordem sequencial;
- b) Área demandante: que deverá assinar a solicitação e o aceite e contabilização periódica das atividades, para efeito dos pagamentos;
- c) Objetivo da tarefa: definição das expectativas e justificativas para realização das atividades;



PODER JUDICIÁRIO
CONSELHO DA JUSTIÇA FEDERAL

- d) Data de início e conclusão das atividades (exceto rotineira): definição do período de realização, inclusive dos períodos e horários realizáveis para serviços que impactem com os trabalhos de usuários;
- e) Listagem das atividades a serem realizadas, especificadas, quantificadas e classificadas conforme complexidade;
- f) Resultado e Nível de Qualidade definido para a tarefa;
- g) Glosa e Penalidades, em caso de descumprimento, e de acordo com a previsão contratual;
- h) Responsáveis pela fiscalização e autorização no CONTRATANTE;
- i) Responsável pelo aceite na CONTRATADA.

2.2.4 Atestação técnica:

- a) A Ordem de Serviço somente poderá ser encerrada quanto todos os objetivos propostos forem plenamente atingidos, e todos os produtos e serviços realizados e entregues com a qualidade demandada e devidamente atestada pelo demandante e pelo gestor do CONTRATANTE;
- b) Antes do fechamento de cada OS a CONTRATADA consultará o representante indicado pelo CONTRATANTE, que avaliará e atestará o serviço realizado;
- c) Uma requisição de serviço ou incidente encerrado sem anuência do CONTRATANTE ou sem que tenha sido de fato resolvido será reaberto e os prazos serão contados a partir da abertura original da requisição de serviço ou incidente, inclusive para efeito de aplicação das sanções previstas.

2.3 Níveis Mínimos de Serviços Exigidos

2.3.1 Os níveis mínimos de serviços são critérios objetivos e mensuráveis que visam aferir e avaliar diversos fatores relacionados com os serviços contratados, quais sejam: qualidade, desempenho, disponibilidade, abrangência/cobertura e segurança;

2.3.2 Os níveis mínimos de serviços estão detalhados no Anexo I do termo de referência – Níveis Mínimos de Serviço;

2.3.3 O não atingimento de um mesmo nível de serviços durante 3 (três) meses consecutivos ou 5 (cinco) meses intervalados, em um período de 12 (doze) meses, ensejará a execução das Sanções Administrativas previstas no contrato;

2.3.4 A CONTRATADA sofrerá glosa de 1% (um por cento), sobre o valor da fatura, a cada 15 pontos ou percentual proporcional ao número de pontos, levando em consideração a relação: glosa de 1% a cada 15 pontos;

2.3.5 As metas devem ser medidas do primeiro ao último dia de cada mês;

2.3.6 A meta exigida representa o parâmetro de valor exato (=), limite máximo (<=) ou limite mínimo (>=) que deve ser alcançado pela CONTRATADA para cada um dos indicadores;

2.3.7 Os tempos serão contados a partir do recebimento da solicitação do cliente. No caso da contagem em dias, a contagem é efetuada dia a dia, incluindo o primeiro e o último dia;



PODER JUDICIÁRIO
CONSELHO DA JUSTIÇA FEDERAL

2.3.8 No caso da resolução de incidentes, se o mesmo não tiver a sua causa raiz conhecida, ou seja, existe um problema a ser resolvido, a CONTRATADA é obrigada a aplicar uma solução de contorno na resolução do incidente para que o serviço volte à sua operação padrão;

2.3.9 Os níveis de serviço serão mensurados de forma automatizada e não poderão ser manipulados pela CONTRATADA;

2.3.10 A CONTRATADA se responsabilizará somente pelos índices que reflitam as requisições de serviços e incidentes designados a ela, não poderá ser responsabilizada por chamados pendentes de fornecedores/prestadores de serviços externos ou encaminhados a outros níveis, ou situações que dependam de terceiros, que, desta forma, não poderão ser computados;

2.3.11 O termo “Hora do restabelecimento” refere-se a hora em que o incidente de indisponibilidade foi efetivamente resolvido;

2.3.12 Por requisições de serviço e incidentes reabertos entende-se que são requisições de serviço ou incidentes que foram dados como resolvidos, porém os mesmos ainda permanecem pendentes de resolução;

2.3.13 Por horário normal de produção entende-se sendo o período entre 09:00 e 20:00, de segunda à sexta-feira, excetuando-se os feriados;

2.3.14 Sobre o índice de supervisão e intervenção proativa:

a) A manutenção proativa visa detectar com antecedência os possíveis problemas que possam vir a ocorrer devido à necessidade de suporte, como aplicação de patches, correções de firmware, ou algum outro dispositivo que possa impactar no desempenho ou disponibilidade dos Sistemas Monitorados pela CONTRATADA, podendo ser visualizados mediante acompanhamento e análise diária de desempenho e produção dos recursos e também através de testes rotineiros de stress e carga;

b) Deverão ser analisados em tempo real os desempenhos dos serviços críticos inserindo as manutenções e os suportes necessários de maneira a proporcionar a continuidade e disponibilidade dos serviços. Diariamente deverão ser analisados os registros internos dos hardwares e softwares para avaliação e detecção de intervenções necessárias, submetendo-os à CONTRATANTE para programação das intervenções que permitirem agendamento;

c) É obrigação da CONTRATADA efetuar as intervenções necessárias em tempo de produção para sanar os erros apresentados nesta fase e que sejam de sua competência. Se as intervenções propostas forem para melhoria de desempenho ou compatibilização de ambiente e permitirem agendamento deverão ser submetidas para aprovação da CONTRATANTE antes de execução.

2.4 Os serviços gerenciados de segurança, serão executados conforme os itens 6.1 a 6.26 da cláusula 6 do Termo de Referência.

2.5 Os serviços de operação e atendimento a requisições, serão executados conforme os itens 7.1 a 7.9 da cláusula 7 do Termo de Referência.

2.6 Os serviços de gestão de incidentes de segurança (CSIRT - Blue Team), serão executados conforme os itens 8.1 a 8.23 da cláusula 8 do Termo de Referência.



PODER JUDICIÁRIO
CONSELHO DA JUSTIÇA FEDERAL

2.7 Os serviços de gestão de vulnerabilidades, serão executados conforme os itens 9.1 a 9.26 da cláusula 9 do Termo de Referência.

2.8 Os serviços de monitoramento e visibilidade de ataques cibernéticos, serão executados conforme os itens 10.3 e 10.4 da cláusula 10 do Termo de Referência.

2.9 Os serviços de orquestração, automação e resposta de segurança (**SOAR**), serão executados conforme os itens 11.3 a 11.5 da cláusula 11 do Termo de Referência.

2.10 Os serviços de testes de invasão (RED TEAM), serão executados conforme os itens 12.2 a 12.16 da cláusula 12 do Termo de Referência.

CLÁUSULA TERCEIRA – DO RECEBIMENTO

3.1 O recebimento e a aceitação obedecerão ao disposto nos arts. 73 a 76 da Lei n. 8.666/1993.

3.2 Caso o CONTRATANTE constate que os serviços foram prestados em desacordo com o contrato, com defeito, fora de especificação ou incompletos, a CONTRATADA será formalmente notificada, sendo interrompidos os prazos de recebimento, e os pagamentos suspensos, até que a situação seja sanada.

3.3 O recebimento definitivo não exclui a responsabilidade civil da CONTRATADA pela solidez e segurança do serviço, nem a ético-profissional pela perfeita execução do contrato, dentro dos limites estabelecidos pela lei ou por este instrumento.

CLÁUSULA QUARTA – DOS PROFISSIONAIS

4.1 A CONTRATADA deverá dimensionar adequadamente a sua equipe de profissionais de forma a atingir os níveis de serviço estabelecidos no contrato;

4.2 Todos os profissionais deverão possuir qualificação plena e conhecimento técnico compatível com a complexidade das demandas a serem atendidas;

4.3 A formação da equipe de profissionais é de exclusiva responsabilidade da CONTRATADA e serão gerenciados exclusivamente pelo PREPOSTO da empresa;

4.4 Os profissionais deverão conhecer o funcionamento dos negócios internos da STI, e respectivas áreas do CJF, bem como executar os procedimentos de acordo com as regras de segurança da informação;

4.5 Os profissionais deverão utilizar vestimenta compatível com a utilizada pelos servidores do CJF e portar crachá de identificação durante toda a prestação de serviço;

4.6 Durante a execução dos serviços, a CONTRATADA se obriga, durante a execução do Contrato, a manter todos os profissionais com as qualificações abaixo especificadas:

4.6.1 Formação:

a) 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.

4.6.2 Certificações:

a) Serviço de Operação e Atendimento a Requisições:



PODER JUDICIÁRIO
CONSELHO DA JUSTIÇA FEDERAL

- CompTIA Security+;
- Fortinet Network Security Expert 4 – NSE4;
- FortiWeb Specialist Exam;
- Certificação ITILv3 Foundation.

b) Serviço de Gestão de Incidentes de Segurança:

- CompTIA Cybersecurity Analyst (CySA+);
- Certified Ethical Hacker – CEH;
- Fortinet Network Security Expert 4 – NSE4;
- FortiWeb Specialist Exam;
- Certificação ITILv3 Foundation.

c) Serviço de Gestão de Vulnerabilidades:

- Certificação dos produtos ofertados;
- Certificação ITILv3 Foundation.

d) Serviço de Monitoramento e Visibilidade de Ataques Cibernéticos:

- Certificação dos produtos ofertados;
- Certificação ITILv3 Foundation.

e) Serviço de Automação de Processos e Fluxos de Trabalho:

- Certificação dos produtos ofertados;
- Certificação ITILv3 Foundation.

g) Serviço de Testes de Invasão:

- EC-Concil Licensed Penetration Tester – LPT ou IACRB Certified Expert Penetration Tester – CEPT ou GIAC Exploit Researcher and Advanced Penetration Tester – GXPN ou Offensive Security Certified Professional – OSCP;
- Certificação ITILv3 Foundation.

4.6.3 Capacitação:

a) Serviço de Operação e Atendimento a Requisições e Serviço de Gestão de Incidentes de Segurança:

- Trend Micro Deep Security, com certificado de participação em curso oficial do fabricante de no mínimo 16 (dezesesseis) horas;
- Trend Micro OfficeScan ou Apex One, com certificado de participação em curso oficial do fabricante de no mínimo 16 (dezesesseis) horas;

4.7 A comprovação dos requisitos deverá ser composta de:

4.7.1 Documento digitalizado com apresentação documento original, cópia autenticada ou documento digital em que seja possível comprovar a autenticidade em site do emissor.



PODER JUDICIÁRIO
CONSELHO DA JUSTIÇA FEDERAL

4.7.2 Todos os documentos apresentados estarão sujeitos à diligência do CONTRATANTE para fins de confirmação das informações prestadas;

4.8 A CONTRATADA deverá promover, no prazo máximo de 3 (três) meses, a atualização das certificações de seus profissionais caso haja 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.

4.9 Caso uma certificação não seja mais válida, será aceita a nova certificação que substituiu a anterior.

CLÁUSULA QUINTA – DO ACOMPANHAMENTO E DA FISCALIZAÇÃO

5.1 O CONTRATANTE designará, na forma da Lei n. 8.666/1993, art. 67, um servidor com autoridade para exercer, como seu representante, toda e qualquer ação de orientação geral, acompanhamento e fiscalização da execução contratual.

5.2 A Subsecretaria de Segurança da Tecnologia da Informação - SUSTI acompanhará a execução do contrato (Gestor do Contrato), devendo proceder à orientação, fiscalização e interdição da execução do contrato, se necessário, a fim de garantir o exato cumprimento das condições estabelecidas em contrato;

5.3 A Seção de Segurança de Rede – SESERE atuará na fiscalização (Fiscal Técnico) e acompanhamento da execução técnica do contrato a fim de garantir o exato cumprimento das condições estabelecidas em contrato;

5.4 O representante da Área Administrativa (Fiscal Administrativo do Contrato), indicado pela autoridade competente dessa área, fiscalizará o contrato quanto aos aspectos administrativos, tais como a verificação de regularidades fiscais, trabalhistas e previdenciárias para fins de pagamento.

5.5 Também cabe ao representante da Área Administrativa, conforme definido na Instrução Normativa CJF-INN-2016/00001, a verificação dos percentuais das rubricas, o acompanhamento, o controle, a conferência dos cálculos efetuados, a confirmação dos valores e da documentação apresentada e demais verificações pertinentes, bem como a autorização para movimentar a conta-depósito vinculada – bloqueada para movimentação.

5.6 O CONTRATANTE reserva-se o direito de atuar orientando, fiscalizando e intervindo no interesse da Administração Pública sem que, de qualquer forma, restrinja a plenitude da responsabilidade da CONTRATADA de exercer a mais ampla e completa fiscalização sobre os serviços, diretamente ou por preposto designado.

5.7 A existência e a atuação da fiscalização pelo CONTRATANTE em nada restringem a responsabilidade única, integral e exclusiva da CONTRATADA, no que concerne à execução do objeto contratado.

CLÁUSULA SEXTA - DAS OBRIGAÇÕES DA CONTRATADA

6.1 Além das obrigações assumidas neste contrato, a CONTRATADA compromete-se a:



PODER JUDICIÁRIO
CONSELHO DA JUSTIÇA FEDERAL

6.1.1 Requisitos Internos:

- a) Atender aos Níveis Mínimos de Serviço estabelecidos pelos indicadores contidos no Anexo I do Termo de Referência;
- b) Executar excepcionalmente, os serviços nas dependências da Gráfica, nos casos em que o CJF entender como conveniente;
- c) Cumprir os normativos e os procedimentos definidos pelo CONTRATANTE;
- d) Primar pelo bom planejamento das atividades, utilizar as boas práticas técnicas e de governança, avaliar previamente a viabilidade técnica, os riscos e os impactos de suas ações, planejar e documentar adequadamente as mudanças de configuração dos ativos de Segurança da Informação – SI;
- e) Criar documentação técnica, operacional e de análise e controle, execução de rotinas pró-ativas e reativas, análise de desempenho, monitoramento e operação dos serviços;
- f) Efetuar a transferência de conhecimento para a equipe técnica do CONTRATANTE, de todos os novos serviços implantados ou modificados, mediante documentação técnica em repositório adotado pelo CJF para esse fim;
- g) Executar todos os serviços, tarefas e atividades demandadas pelo CONTRATANTE dentro do prazo contratado, atendendo o padrão de qualidade exigido;
- h) Apresentar no 1º (primeiro) dia útil de cada mês a relação dos profissionais que prestarão os serviços no mês corrente;
- i) Formalizar ao CONTRATANTE a substituição de profissional, antes de sua efetiva substituição;
- j) Realizar os serviços em conformidade com os horários e períodos determinados pelo CONTRATANTE;
- k) Documentar as atividades, que não possuam rotinas e procedimentos definidos, após a sua realização como condição para a aceitação do serviço;
- l) Elaborar relatório gerencial de serviços, apresentando-o ao CONTRATANTE, até o terceiro dia útil do mês subsequente ao da prestação dos serviços, devendo constar dentre outras informações:
 - Os indicadores e níveis de serviços alcançados em relação ao previsto no Anexo I do termo de referência;
 - Relatório de análise e diagnóstico das causas (causa raiz) dos incidentes e problemas ocorridos;
 - Manutenções evolutivas e corretivas realizadas;
 - Erros operacionais;
 - Sugestões de melhorias;
 - Painel de volumetria de chamados (requisições de serviço, incidentes, problemas etc.) divididos por grupos solucionadores e responsáveis, demonstrando graficamente a evolução destas informações;



PODER JUDICIÁRIO
CONSELHO DA JUSTIÇA FEDERAL

- Indicadores de aferição da qualidade de novos produtos e/ou serviços que venham a ser implantados no decorrer da vigência contratual;
- Demais informações relevantes para as atividades demandadas nas Ordens de Serviços.
- Estatísticas de tratamento de e-mails suspeitos, spam etc.;
- Estatísticas de tratamento de malware (vírus, worms, trojan horses, spyware etc.);
- Relatório de resultados obtidos em testes de invasão;
- Relatório de vulnerabilidades de segurança nos sistemas de informação, aplicativos e serviços de TI;
- Sugestões de mitigação das vulnerabilidades de segurança encontradas;
- Eventos de segurança;
- Ações tomadas em reação aos eventos de segurança;
- Sugestões de mitigação de riscos.

m) Submeter seus profissionais aos regulamentos de segurança e disciplina instituídos pelo CONTRATANTE, durante o tempo de permanência nas suas dependências;

n) Solicitar o credenciamento e descredenciamento de acesso físico e lógico às dependências do CONTRATANTE bem como assumir quaisquer prejuízos porventura causados por seus profissionais;

o) Promover o afastamento, no prazo máximo de 24 (vinte e quatro) horas, após a notificação de que qualquer dos seus profissionais que não estejam realizando as atividades com a devida competência técnica e/ou postura profissional exigidos para a prestação dos serviços no CONTRATANTE;

p) Prestar os serviços de forma ininterrupta, portanto o afastamento mencionado no subitem o, não poderá prejudicar a qualidade dos serviços e nem descumprir quaisquer cláusulas contratuais;

q) Comunicar às unidades do CONTRATANTE responsáveis pela fiscalização do contrato, por escrito, qualquer anormalidade, bem como atender prontamente o que lhe for solicitado e exigido;

r) Manter um Diário de Ocorrências que conste nos registros as eventuais ocorrências diárias relativas à execução dos trabalhos;

s) Selecionar e treinar adequadamente os profissionais alocados para prestação dos serviços, observando a boa conduta e a idoneidade moral destes;

t) Manter os seus profissionais atualizados tecnologicamente, promovendo treinamentos e participação em eventos de caráter técnico que permitam a boa execução dos serviços, sem qualquer ônus para o CONTRATANTE, com carga horária mínima de 20 (vinte) horas anuais. O CONTRATANTE poderá indicar áreas de conhecimento em que os serviços necessitem de aperfeiçoamento;

u) Manter os seus profissionais qualificados nas ferramentas, metodologias, processos e tecnologias utilizados pelo CONTRATANTE durante toda a vigência do contrato;



PODER JUDICIÁRIO
CONSELHO DA JUSTIÇA FEDERAL

- v) Realizar os serviços, durante toda a vigência do contrato, por profissionais com as competências e certificações exigidas nas descrições dos serviços, bem como capacitados nas tecnologias que eventualmente venham a ser utilizadas durante sua execução. Tal qualificação sempre que exigida pelo CJF, deverá ser comprovada por currículos e certificados oficiais;
- w) A seleção, a designação e a manutenção do quadro de profissionais alocados ao contrato são de exclusiva responsabilidade da CONTRATADA;
- x) Fiscalizar regularmente os seus profissionais designados para a prestação dos serviços verificando as condições em que as atividades estão sendo realizadas;
- y) Refazer todos os serviços que, a juízo do representante do CONTRATANTE, não forem considerados satisfatórios, sem que caiba qualquer acréscimo no custo contratado, independentemente das penalidades previstas do Termo de Referência;
- z) A CONTRATADA e seus profissionais deverão assinar o Termo de Responsabilidade conforme modelo Anexo IV do Termo de Referência, e manter em caráter confidencial, mesmo após o término do prazo de vigência ou rescisão do contrato, as informações relativas:
- As políticas e procedimentos de segurança da informação adotados pelo CONTRATANTE;
 - As configurações de hardwares, de softwares, produtos, ferramentas e equipamentos;
 - Aos processos internos do CONTRATANTE;
 - As vulnerabilidades dos ativos de informação do CJF;
 - Mecanismos de criptografia e autenticação.
- aa) Assinar, juntamente com seus profissionais que prestarão os serviços, o Termo de Responsabilidade e se responsabilizar pelos atos de seus profissionais que estiverem prestando serviço no CONTRATANTE, conforme modelo do Anexo IV do Termo de Referência;
- bb) Acatar as determinações feitas pela fiscalização do CONTRATANTE no que tange ao cumprimento do objeto deste contrato;
- cc) Prestar, de imediato, todos os esclarecimentos solicitados pela fiscalização do CONTRATANTE no que diz respeito a execução do objeto contratado;
- dd) Responder por escrito, no prazo máximo de 48 (quarenta e oito) horas, a quaisquer esclarecimentos de ordem técnica pertinentes à execução dos serviços que venham porventura a ser solicitados pelo CONTRATANTE;
- ee) Permitir auditoria pelo CONTRATANTE, ou terceiro por ela designado, inclusive com a possibilidade dos atendimentos serem monitorados para verificação de procedimentos;
- ff) Seguir as melhores práticas preconizadas pelo framework ITIL v3, garantindo a aplicação dos processos de Gerenciamento da Configuração e de Ativo de Serviço, Gerenciamento de Requisição, Gerenciamento de Incidente, Gerenciamento de Problema, Gerenciamento de Mudança, Gerenciamento do Conhecimento e o Gerenciamento de Níveis de Serviço, Gerenciamento da Disponibilidade, Gerenciamento do Catálogo de



PODER JUDICIÁRIO
CONSELHO DA JUSTIÇA FEDERAL

Serviço e o Gerenciamento de liberação e Implantação, garantindo a manutenção de uma base de dados de configuração e mudanças;

gg) A realização dos processos ITIL significa seguir os processos descritos naquela metodologia, manter equipe capacitada para aplicar os conceitos, utilizar as ferramentas que implementem o ITIL e gerar relatórios com as informações pertinentes à metodologia;

hh) Manter atualizada a Base de Dados de Gerenciamento de Configuração dos ativos que fazem parte do objeto do seu contrato;

ii) Participar, dentro do período compreendido entre a assinatura do contrato e o início da prestação dos serviços, de reunião de alinhamento de expectativas contratuais com uma equipe de técnicos da STI;

jj) Indicar formalmente, quando da assinatura do contrato, PREPOSTO que tenha capacidade gerencial para tratar de todos os assuntos previstos no instrumento contratual e coordenação da equipe para a execução dos serviços contratados. O preposto deverá, entre outras atividades, promover os contatos com o gestor do contrato bem como deverá prestar atendimento aos profissionais em serviço, tais como:

- Executar os procedimentos administrativos referentes aos profissionais alocados para execução dos serviços contratados, tais como: entregar-lhes contracheques, auxílio-transporte e auxílio-alimentação, acompanhar e controlar a apuração do ponto;
- Assegurar de que as determinações do CJF sejam disseminadas junto aos profissionais alocados com vistas à execução dos serviços contratados;
- Informar ao gestor do contrato sobre problemas de qualquer natureza que possam impedir o bom andamento dos serviços contratados;
- Desenvolver outras atividades administrativas de responsabilidade da CONTRATADA, principalmente quanto ao controle de informações relativas ao seu faturamento mensal e apresentação de documentos quando solicitado;
- O preposto não poderá ser contabilizado como profissional para execução dos serviços contratados.
- Após a assinatura do contrato, conhecer o parque tecnológico e as atividades em andamento, visando à preparação da equipe que irá prestar os serviços, conhecer os modelos de serviços realizados, as normas internas, procedimentos de segurança e a definição dos requisitos necessários;
- Deverá estar disponível, de segunda a sexta-feira, das 09 (nove) às 19 (dezenove) horas, e acessível por contato telefônico em qualquer outro horário;
- A CONTRATADA deverá indicar um substituto eventual para substituir o PREPOSTO nos casos de afastamento imprevisto, tais como por motivo de saúde, limitado a 5 (cinco) dias corridos;
- A CONTRATADA deverá indicar um substituto com, no mínimo 10 (dez) dias corridos de antecedência, nos casos previsíveis de ausência do PREPOSTO, tais como por férias, treinamentos etc.;

kk) Os profissionais deverão atender as exigências de vestimenta feitas aos servidores do CJF e portar crachá de identificação durante toda a prestação do serviço;



PODER JUDICIÁRIO
CONSELHO DA JUSTIÇA FEDERAL

- ll) Manter o serviço de suporte técnico das soluções ofertadas com a finalidade de garantir a plena utilização dos produtos durante toda a vigência do contrato;
- mm) Implantar as novas versões, patches, releases, e service packs relativos a esses produtos de segurança utilizados no ambiente. Quando houver contrato de suporte técnico com terceiro, deverá ser aberto chamado de suporte técnico para a execução coordenada destes serviços;
- nn) Auxiliar o CONTRATANTE na comunicação junto aos fabricantes dos produtos utilizados pelo CONTRATANTE;

6.1.2 Requisitos Externos

- a) Manter sigilo, sob pena de responsabilidade civil, penal e administrativa, sobre todo e qualquer assunto de interesse do CONTRATANTE ou de terceiros de que tomar conhecimento em razão da execução do objeto deste contrato, devendo orientar seus profissionais nesse sentido; observar o cumprimento das normas relacionadas com a segurança e higiene no trabalho;
- b) Manter a limpeza e a conservação dos ambientes onde desempenhe seus serviços;
- c) Cuidar materiais, produtos, ferramentas e equipamentos disponibilizados para a execução dos serviços, inclusive por perdas decorrentes de roubo, furto ou outros fatos que possam vir a ocorrer;
- d) Prestar os serviços dentro dos parâmetros e rotinas estabelecidos pelo CONTRATANTE, com observância às recomendações aceitas pela boa técnica, normas e legislação, bem como observar conduta adequada na utilização dos materiais, equipamentos, ferramentas e utensílios;
- e) Responsabilizar-se por danos causados ao patrimônio do CONTRATANTE, ou de terceiros, ocasionados por seus profissionais, em virtude de dolo ou culpa, durante a execução do objeto contratado;
- f) Manter durante todo o período de vigência do ajuste todas as condições, inclusive de habilitação, que ensejaram sua contratação;
- g) Prestar os serviços de forma ininterrupta, em conformidade com o demandado pelas Ordens de Serviço;
- h) Assumir todas as despesas relativas à execução dos serviços, tais como taxas, emolumentos, encargos sociais;
- i) Arcar com as despesas decorrentes de qualquer infração cometida por seus profissionais, inclusive com as glosas previstas, quando da execução dos serviços especificados nas Ordens de Serviço;
- j) Responder por todo e qualquer dano ou prejuízo eventualmente causado ao CONTRATANTE como consequência de atos e fatos imputáveis a seus profissionais;
- k) Cumprir às suas próprias expensas todas as cláusulas contratuais que definam suas obrigações;
- l) Assinar, juntamente com seus profissionais que prestarão os serviços, a declaração de não nepotismo, conforme modelo do Anexo IV do Termo de Referência;



PODER JUDICIÁRIO
CONSELHO DA JUSTIÇA FEDERAL

- m) Responsabilizar-se por todos os encargos previdenciários e obrigações sociais previstas na legislação social e trabalhista em vigor, obrigando-se a saldá-las na época própria, vez que os seus profissionais não manterão nenhum vínculo empregatício com o CONTRATANTE;
- n) Responsabilizar-se por todas as providências e obrigações estabelecidas na legislação específica de acidentes de trabalho, quando, em ocorrência da espécie, forem vítimas os seus profissionais durante a execução deste contrato, ainda que acontecido em dependência do CONTRATANTE;
- o) Responsabilizar-se por todos os encargos de possível demanda trabalhista, civil ou penal, relacionada à execução deste contrato, originariamente ou vinculada por prevenção, conexão ou continência;
- p) Responsabilizar-se por todos os encargos fiscais e comerciais resultantes desta contratação;
- q) Responsabilizar-se pelo pagamento de eventuais multas aplicadas por quaisquer autoridades federais, estaduais e municipais, em consequência de fato a ela imputável e relacionada com a execução do objeto do contrato;
- r) Responsabilizar-se por todos os prejuízos advindos de perdas e danos, incluindo despesas judiciais e honorários advocatícios, resultantes de ações judiciais a que o CONTRATANTE for compelido a responder por força desta contratação.

CLÁUSULA SÉTIMA - DAS OBRIGAÇÕES DO CONTRATANTE

7.1 Constituem obrigações do CONTRATANTE, além de outras estabelecidas ou decorrentes deste contrato:

- a) Nomear um gestor e equipe de fiscais técnicos para acompanhar a execução do contrato, que se tornará responsável pelo fiel cumprimento do mesmo e seus elementos integrantes;
- b) Receber e atestar as notas fiscais de faturamento dos serviços prestados, bem como, verificar a qualidade dos serviços por meio de relatórios que comprovem o cumprimento dos níveis mínimos de serviço estabelecidos. O gestor será também responsável por encaminhar as notas fiscais para pagamento segundo os procedimentos internos do CJF;
- c) Nomear um Fiscal Administrativo do contrato que irá fiscalizar periodicamente os recolhimentos do FGTS, por empregado, o fornecimento de vale transporte e auxílio alimentação, o pagamento de 13º salário, a concessão de férias e o correspondente pagamento do adicional de 1/3, a realização de exames admissionais e demissionais e periódicos, os eventuais cursos de treinamento e reciclagem, a comprovação de encaminhamento ao Ministério do Trabalho e Emprego da RAIS e CAGED, do cumprimento das convenções, acordos e dissídios coletivos, e do efetivo pagamento dos valores salariais lançados na proposta da CONTRATADA, mediante a verificação das folhas de pagamento referentes aos meses de realização dos serviços, de cópias de carteiras de trabalho dos empregados, dos recibos e dos respectivos documentos bancários, entre outros meios de fiscalização cabíveis;



PODER JUDICIÁRIO
CONSELHO DA JUSTIÇA FEDERAL

- d) Solicitar a substituição do profissional que tenha infringido às normas do CJF, ainda que em parte, dos itens indicados na cláusula 6 - “Obrigações da CONTRATADA”;
- e) Permitir acesso dos prestadores de serviço da CONTRATADA às suas dependências, aos equipamentos, softwares e sistemas de informação para a execução dos serviços contratados;
- f) Prestar as informações e os esclarecimentos pertinentes que venham a ser solicitados pelos prestadores de serviço da CONTRATADA ou por seu preposto;
- g) Efetuar o pagamento mensal devido pela execução dos serviços, desde que cumpridas as formalidades e exigências do contrato;
- h) Exercer a fiscalização dos serviços prestados;
- i) Comunicar oficialmente à CONTRATADA, quaisquer falhas verificadas no cumprimento do contrato;
- g) Avaliar mensalmente o relatório gerencial de serviços, observando os indicadores e metas de níveis de serviço alcançados;
- h) Observar o cumprimento dos requisitos de qualificação profissional exigidos no edital e seus módulos, solicitando à CONTRATADA as substituições e os treinamentos que se verificarem necessários;
- i) Fornecer as normas, rotinas, procedimentos e processos desenvolvidos pelo CJF para que a CONTRATADA promova os devidos ajustes e implementações adicionais;

CLÁUSULA OITAVA – DO CONTINGENCIAMENTO DOS ENCARGOS TRABALHISTAS

8.1 Os encargos sociais trabalhistas serão contingenciados pelos percentuais abaixo, incidentes sobre a remuneração mensal dos profissionais alocados no CONTRATANTE para execução do contrato.

Percentuais para contingenciamento de encargos trabalhistas a serem aplicados sobre a NF

Título	VARIAÇÃO RAT AJUSTADO 0,50% A 6,00%			
	EMPRESAS		SIMPLES	
Grupo A SUBMÓDULO 4.1 - DA IN 1/2016 – CJF: RAT:	Mínimo 34,30% 0,50%	Máximo 39,80% 6,00%	Mínimo 28,50% 0,50%	Máximo 34,00% 6,00%
13º salário	9,09	9,09	9,09	9,09
Férias	9,09	9,09	9,09	9,09
1/3 Constitucional	3,03	3,03	3,03	3,03
Subtotal	21,21	21,21	21,21	21,21
Incidência do Grupo A (*)	7,28	8,44	6,04	7,21
Multa do FGTS	4,36	4,36	4,36	4,36
Encargos a contingenciar	32,85	34,01	31,61	32,78



PODER JUDICIÁRIO
CONSELHO DA JUSTIÇA FEDERAL

Taxa da conta corrente vinculada (inciso III, artigo 2º IN) (**)				
Total a contingenciar				

(*) A incidência recai sobre as verbas de 13º salário, férias e 1/3 constitucional, variando de acordo com o RAT Ajustado da contratada.

(**) Caso o contrato firmado entre a empresa e o banco oficial tenha previsão de desconto da taxa de abertura e manutenção diretamente na conta vinculada, esse valor deverá ser retido da fatura e devolvido à conta vinculada, nos termos do inciso VIII do artigo 17 da Resolução CNJ n. 169/2013.

8.2 O contingenciamento será feito mensalmente, mediante depósito em conta-depósito vinculada – bloqueada para movimentação -, cujo saldo será remunerado pelo índice da poupança ou outro definido com a instituição financeira, recaiando a opção sempre pelo de maior rentabilidade, na forma estabelecida pela Instrução Normativa CJF nº 01/2016;

8.3 As parcelas correspondentes a Férias e 13º salário serão liberadas ao longo da execução do contrato na medida em que os eventos ocorrerem.

8.4 A CONTRATADA deverá providenciar a assinatura dos documentos relativos à abertura e movimentação da conta-depósito vinculada (bloqueada para movimentação), em até 20 (vinte) dias a contar da notificação do CONTRATANTE;

8.5 Eventuais despesas com abertura e manutenção da conta-depósito vinculada deverão ser suportadas pela CONTRATADA e integrarão os custos com taxa de administração, constante da proposta comercial da empresa;

8.6 Sempre que necessário, o gestor do contrato poderá requerer à CONTRATADA a apresentação dos documentos comprobatórios da remuneração dos profissionais alocados na execução deste contrato, bem como daqueles necessários à apuração do RAT ajustado;

8.7 O valor das rubricas indicadas no item 8.1, será destacado do valor mensal do contrato e depositados em conta-depósito vinculada–bloqueada para movimentação, aberta em nome da CONTRATADA, em banco público oficial, e deixarão de compor o valor mensal a ser pago à CONTRATADA.

8.7.1 Os valores provisionados serão obtidos pela aplicação de percentuais e valores constantes da proposta comercial da CONTRATADA.

8.8 Os valores provisionados só poderão ser movimentados mediante autorização do CONTRATANTE e exclusivamente para o pagamento das rubricas vinculadas.

8.8.1 A liberação deverá obedecer ao disposto nos artigos 12, 13 e 14 da IN CJF 001/2016, no que se refere aos procedimentos e documentos necessários à autorização de liberação.

8.9 Os saldos da conta-depósito vinculada – bloqueada para movimentação serão remunerados diariamente pelo índice da poupança ou outro definido no Acordo de Cooperação Técnica, sempre escolhido o de maior rentabilidade.

8.10 O saldo remanescente da conta-depósito vinculada – bloqueada para movimentação será liberado à CONTRATADA no encerramento do contrato, após a quitação de todas as verbas trabalhistas dos empregados.

8.11 A fim de cumprir o disposto no artigo 147 do Decreto-lei n. 5.452/1943 – Consolidação das Leis do Trabalho – CLT (férias proporcionais), bem como o disposto no parágrafo único do artigo 1º do Decreto n. 57.155/1965 (13º proporcional), o CONTRATANTE deverá reter



PODER JUDICIÁRIO
CONSELHO DA JUSTIÇA FEDERAL

integralmente a parcela relativa a estes encargos quando a prestação de serviços for igual ou superior a 15 (quinze) dias.

8.12 No caso em que o banco oficial promova o débito do valor das despesas com a cobrança de abertura e de manutenção diretamente na conta-depósito vinculada - bloqueada para movimentação, o referido montante será retido do pagamento do valor mensal devido à CONTRATADA e depositado na conta-depósito vinculada - bloqueada, na forma estabelecida no parágrafo único do art. 1º da Resolução CNJ n.169/2013.

8.13 Deverão ser precedidos, para o início das atividades de prestação de serviços, os seguintes atos:

- a) Solicitação pelo Tribunal ou pelo Conselho contratante ao Banco, mediante ofício, de abertura de conta-depósito vinculada – bloqueada para movimentação -, no nome da empresa, conforme modelo constante no termo de cooperação, devendo o banco público oficial ao Conselho sobre a abertura da referida conta- depósito vinculada – bloqueada para movimentação-, na forma do modelo consignado no supracitado termo de cooperação;
- b) Assinatura, pela empresa contratada, no prazo de vinte dias, a contar da notificação da CONTRATADA, dos documentos de abertura da conta-deposito vinculada – bloqueada para movimentação – e de termo específico da instituição financeira oficial que permita ao Conselho ter acesso ao saldos e extratos, e vincule a movimentação dos valores depositados à autorização do Conselho, conforme modelo indicado no termo de cooperação.

CLÁUSULA NONA – DA VIGÊNCIA

9.1 O prazo de vigência deste contrato é de 24 (vinte e quatro) meses, contados da data de assinatura pelo CONTRATANTE, podendo ser prorrogado, por mútuo acordo entre as partes, mediante termo aditivo, por iguais e sucessivos períodos, observado o limite máximo de 60 (sessenta) meses.

9.2 Caso ocorra a prorrogação da vigência do Contrato, observadas as disposições constantes no art. 57, da Lei n.º 8.666/1993, a CONTRATADA deverá providenciar a devida renovação da garantia prestada, com validade de 3 (três) meses após o término da vigência contratual, tomando-se por base o valor atualizado do Contrato.

9.3 A prorrogação da vigência do Contrato, em exercícios subsequentes ficará condicionada à avaliação dos serviços prestados, à comprovação da compatibilidade dos preços conforme o mercado, à existência, em cada ano, de dotação orçamentária para suportar as despesas dele decorrentes, bem como a manutenção das condições de habilitação.

CLÁUSULA DÉCIMA – DO VALOR

10.1 O valor total contratado fica estimado em **R\$ 00,00 (extenso)**, referente aos lotes, conforme especificado no Anexo II do Termo de Referência- Planilha de Preços.

10.2 Os valores estabelecidos nesta cláusula incluem todos os tributos, contribuições fiscais e parafiscais previstos na legislação em vigor, incidentes direta ou indiretamente, bem como as despesas de quaisquer naturezas decorrentes da execução do contrato, sendo os valores fixos e irredutíveis.



PODER JUDICIÁRIO
CONSELHO DA JUSTIÇA FEDERAL

10.3 O CONTRATANTE poderá promover alterações contratuais, observada as limitações constantes na Lei n. 8.666/1993, art. 65, §1º.

CLÁUSULA DÉCIMA PRIMEIRA – DA DOTAÇÃO ORÇAMENTÁRIA

11.1 As despesas com a execução correrão à conta de recursos orçamentários da União destinados ao CONTRATANTE, consignados no Programa de Trabalho Resumido - PTRES: _____, Natureza de Despesa - ND: _____, Nota de Empenho n._____.

CLÁUSULA DÉCIMA SEGUNDA – DA REPACTUAÇÃO E DO REAJUSTE

12.1 Do reajuste dos serviços e dos insumos

12.1.1 Em caso de prorrogação do contrato será adotada, para fins de reajuste para os serviços em que **não houver a alocação continuada de profissionais**, bem como os preços de eventuais equipamentos, softwares e demais insumos utilizados para a prestação dos serviços previstos no contrato e que tenham sido declarados nas planilhas de custos e formação de preços, poderão ser reajustados mediante negociação entre as partes, tendo como limite máximo a variação do IPCA – IBGE, conforme a seguir:

12.1.1.1 Na primeira prorrogação de vigência, as partes observarão para que o percentual a ser aplicado não seja superior à variação acumulada, no período compreendido entre a data da apresentação da proposta e aquela em que se verificar o aniversário da celebração do contrato, conforme estabelece a Lei n. 8.666/1993, art. 40, inciso XI.

12.1.1.2 Nas prorrogações seguintes, o reajuste será calculado considerando-se a variação acumulada dos 12 (doze) últimos meses, contados do aniversário do contrato.

12.1.1.3 Caso o índice estabelecido para delimitar o reajustamento dos preços seja extinto ou, de qualquer forma, não possa mais ser utilizado para esse fim, as partes desde já concordam que em substituição seja adotado o que vier a ser determinado pela legislação então em vigor.

12.1.1.4 Na ausência de previsão legal quanto ao índice substituto, as partes elegerão novo índice para delimitar o reajustamento dos preços.

12.2 Da Repactuação DOS SERVIÇOS:

12.2.1 Os valores referentes aos serviços gerenciados de segurança, **quando houver à alocação continuada de profissionais** da CONTRATADA nas dependências do CONTRATANTE, previstos no contrato poderão ser repactuados, observado o interregno mínimo de um ano, a contar da data do orçamento a que a proposta se referir, cabendo à CONTRATADA apresentar, junto à solicitação, a devida justificativa e demonstração analítica da variação dos componentes de custo do Contrato, de acordo com planilha de custos e formação de preços, acordo, convenção ou dissídio coletivo de trabalho ou equivalente, registrado no Sistema de Negociações Coletivas de Trabalho - Mediador, entre outros, visando à análise e aprovação pelo CONTRATANTE;

12.3 A repactuação para fazer face à elevação dos custos da contratação, respeitada a anualidade disposta no item anterior e que vier a ocorrer durante a vigência do Contrato, é direito da CONTRATADA, e não poderá alterar o equilíbrio econômico e financeiro do Contrato, conforme estabelece o art. 37, inciso XXI da Constituição da República Federativa



PODER JUDICIÁRIO
CONSELHO DA JUSTIÇA FEDERAL

do Brasil, sendo assegurado à CONTRATADA receber pagamento mantidas as condições efetivas da proposta;

12.4 A repactuação poderá ser dividida em tantas parcelas quanto forem necessárias em respeito ao princípio da anualidade do reajuste dos preços da contratação, podendo ser realizada em momentos distintos para discutir a variação de custos que tenham sua anualidade resultante em datas diferenciadas, tais como os custos decorrentes da mão de obra e os custos decorrentes dos insumos necessários à execução do serviço;

12.5 A repactuação, em razão de novo acordo, dissídio ou convenção coletiva deve repassar integralmente o aumento de custos da mão de obra decorrente desses instrumentos;

12.6 O interregno mínimo de 1 (um) ano para a primeira repactuação será contado a partir da data do acordo, convenção ou dissídio coletivo de trabalho ou equivalente, vigente à época da apresentação da proposta, quando a variação dos custos for decorrente da mão de obra e estiver vinculada às datas-bases destes instrumentos;

12.7 Nas repactuações subsequentes à primeira, a anualidade será contada a partir da data do fato gerador que deu ensejo à última repactuação;

12.8 As repactuações serão precedidas de solicitação da CONTRATADA, acompanhada de demonstração analítica da alteração dos custos, por meio de apresentação da planilha de custos e formação de preços ou do novo acordo convenção ou dissídio coletivo que fundamenta a repactuação, conforme for a variação de custos objeto da repactuação;

12.9 A proposta de repactuação dependerá de iniciativa da CONTRATADA, devendo ser apresentada ao CONTRATANTE em até 30 (trinta) dias da ocorrência do fato ensejador da variação dos componentes de custos do Contrato, ou até a prorrogação contratual ou o encerramento do contrato, se esses eventos ocorrerem antes daquele prazo;

12.10 A CONTRATADA apresentará justificativa expressa, nos mesmos prazos indicados no item anterior, caso não seja possível a apresentação da proposta de repactuação;

12.11 Caso o CONTRATANTE concorde com a justificativa, a CONTRATADA, para fazer jus à repactuação retroativa, deverá solicitá-la até a prorrogação contratual ou o encerramento do contrato, pois serão objeto de preclusão com a assinatura da prorrogação contratual ou com o fim de vigência do ajuste;

12.12 É vedada a inclusão, por ocasião da repactuação, de benefícios não previstos na proposta inicial, exceto quando se tornarem obrigatórios por força de instrumento legal, sentença normativa, acordo coletivo ou convenção coletiva;

12.13 A decisão sobre o pedido de repactuação deve ser feita no prazo máximo de sessenta dias, contados a partir da solicitação e da entrega dos comprovantes de variação dos custos;

12.14 Na hipótese de iminente prorrogação do contrato, não havendo concessão do pedido até a assinatura do termo aditivo respectivo, a CONTRATADA deverá deixar consignado o seu direito expressamente nesse instrumento;

12.15 O prazo referido subitem anterior ficará suspenso enquanto a CONTRATADA não cumprir os atos ou apresentar a documentação solicitada pelo CONTRATANTE para a comprovação da variação dos custos;



PODER JUDICIÁRIO
CONSELHO DA JUSTIÇA FEDERAL

12.16 O CONTRATANTE poderá realizar diligências para conferir a variação de custos alegada pela CONTRATADA;

12.17 Os novos valores contratuais decorrentes das repactuações terão suas vigências iniciadas observando-se o seguinte:

12.17.1 A partir da ocorrência do fato gerador que deu causa à repactuação;

12.17.2 Em data futura, desde que acordada entre as partes, sem prejuízo da contagem de periodicidade para concessão das próximas repactuações futuras; ou

12.17.3 Em data anterior à ocorrência do fato gerador, exclusivamente quando a repactuação envolver revisão do custo de mão de obra em que o próprio fato gerador, na forma de acordo, convenção ou sentença normativa, contemplar data de vigência retroativa, podendo esta ser considerada para efeito de compensação do pagamento devido, assim como para a contagem da anualidade em repactuações futuras.

12.18 Os efeitos financeiros da repactuação deverão ocorrer exclusivamente para os itens que a motivaram, e apenas em relação à diferença porventura existente;

12.19 As repactuações não interferem no direito das partes de solicitar, a qualquer momento, a manutenção do equilíbrio econômico dos contratos com base no disposto no art. 65 da Lei n. 8.666. de 1993;

12.20 A CONTRATADA para a execução de remanescente de serviço tem direito à repactuação nas mesmas condições e prazos a que fazia jus a empresa anteriormente contratada, devendo os seus preços serem corrigidos antes do início da contratação, conforme determina o art. 24, inciso XI da Lei n. 8.666, de 1993;

12.21 As repactuações poderão ser formalizadas por meio de apostilamento, e não poderão alterar o equilíbrio econômico e financeiro do Contrato, exceto quando coincidirem com a prorrogação contratual, em que deverão ser formalizadas por aditamento.

12.22 Em decorrência da variação anual do Fator Acidentário de Prevenção - FAP (cf. Decreto n. 6.957/2009), a CONTRATADA deverá apresentar, com o pedido de repactuação a documentação comprobatória acerca da alteração/manutenção da alíquota do FAP.

CLÁUSULA DÉCIMA TERCEIRA – DO PAGAMENTO

13.1 Os pagamentos 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;

13.2 As notas fiscais deverão ser emitidas com número raiz do CNPJ qualificado no preâmbulo e encaminhadas ao gestor do contrato pelos e-mails : xx@cjf.jus.br e xx@cjf.jus.br .

13.2.1 No corpo da nota fiscal deverá ser especificado o objeto contratado e o período faturado no formato dia/mês/ano.

13.3 A fim de que o CONTRATANTE possa efetuar o pagamento, a CONTRATADA deverá apresentar nota fiscal constando a indicação do banco, da agência e do número da conta corrente onde deverá ser efetuado o crédito;

13.4 A nota fiscal deverá apresentada até o quinto dia útil do mês subsequente à prestação do serviço;



PODER JUDICIÁRIO
CONSELHO DA JUSTIÇA FEDERAL

13.5 O CONTRATANTE, deverá efetuar a análise dos relatórios gerenciais de serviços em até cinco dias úteis do recebimento destes. Após manifestação formal do Contratante, a CONTRATADA deverá emitir as notas fiscais de cobrança em até 10 (dez) dias úteis da manifestação

13.6 A nota de cobrança emitida pela CONTRATADA deverá ser atestada em até 7 (sete) dias úteis pelo Gestor do contrato e encaminhada para a área financeira efetuar o pagamento, acompanhada dos relatórios gerenciais de serviços e documentação comprobatória do não atendimento dos resultados ou níveis de serviço exigidos;

13.7 Apresentada a nota fiscal de cobrança na forma aqui estabelecida, terá o CONTRATANTE o prazo máximo de 10 (dez) dias úteis para efetuar o pagamento, contados a partir do atesto.

13.8 Deverá ser encaminhado mensalmente, em conjunto com a fatura, a seguinte documentação que será analisada e aprovada pelo representante da área administrativa (Fiscal Administrativo do Contrato). Os documentos comprobatórios listados nos itens abaixo são necessários apenas para os colaboradores que prestaram serviço nas dependências do CJF por mais de 15 (quinze) dias no mês em questão:

13.8.1 Comprovação de pagamento de salários do mês da prestação dos serviços objeto de faturamento, mediante apresentação de folha de pagamento específica, em que conste como tomador o Conselho da Justiça Federal, acompanhada de cópias dos recibos de depósitos bancários ou contracheques assinados pelos profissionais;

13.8.2 Planilha formadora de custos de mão-de-obra, nos termos da IN n.05/2017 e IN n.07/2018 do Ministério do Planejamento, Desenvolvimento e Gestão;

13.8.3 Guia de Recolhimento do Fundo de Garantia do Tempo de Serviço e Informações à Previdência Social – GFIP específica, em que conste como tomador o CJF, relativa ao mês da prestação de serviço;

13.8.4 Comprovante de entrega de benefícios suplementares (vale transporte, vale-alimentação etc.), a que estiver obrigada, por força de lei ou de convenção ou acordo coletivo de trabalho;

13.8.5 Comprovação do pagamento do 13º salário, quando houver;

13.8.6 Relação mensal de prestadores referente ao mês da prestação dos serviços, na qual constem todos os empregados que atuaram no Conselho, mesmo que transitoriamente em substituição à mão de obra faltante, com discriminação do período de atuação;

13.8.7 Folha de pagamento do mês de referência constando todos os funcionários que prestaram serviço no Conselho, ou contracheque individual de cada funcionário, e comprovante de depósito nominal.

13.8.8 Guia de Recolhimento do FGTS e Informações à Previdência Social (GFIP), referente ao mês da prestação dos serviços, individualizada por tomador (CJF);

13.8.9 Quando ocorrer demissão de pessoal, será necessário o encaminhamento dos Termos de Rescisão de Contrato de Trabalho, integrando-se à documentação exigida para pagamento da nota fiscal.

13.8.10 Quando exigível em Convenção Coletiva de Trabalho, os Termos de Rescisão deverão estar homologados pelo sindicato que assiste a categoria profissional do trabalhador.



PODER JUDICIÁRIO
CONSELHO DA JUSTIÇA FEDERAL

13.9 Dos valores a serem pagos à CONTRATADA, serão abatidos, na fonte, os tributos federais, estaduais e municipais, na forma da lei.

13.9.1 Caso a CONTRATADA goze de algum benefício fiscal, deverá, juntamente com a nota fiscal, encaminhar documentação hábil, ou, no caso de optante pelo Simples Nacional - Lei Complementar n. 123/2006, declaração nos termos do modelo constante de instrução normativa da Secretaria da Receita Federal.

13.10 Poderá o CONTRATANTE, após efetuar a análise das notas fiscais, realizar glosas dos valores cobrados indevidamente.

13.11 Obedecendo a pontuação atribuída no Anexo I do Termo de Referência para cada inadimplemento, o CONTRATANTE aplicará glosa de 1% (um por cento) sobre o valor da nota fiscal a cada 15 pontos, limitada a glosa total ao percentual máximo de 30% (trinta por cento) do valor mensal previsto em contrato, devendo o CONTRATANTE cientificar à CONTRATADA sobre as razões que ensejaram o desconto;

13.12 No caso de discordância das glosas aplicadas, a CONTRATADA deverá apresentar o recurso que será analisado pela área administrativa. Se a decisão da Administração for favorável ao recurso da CONTRATADA, esta emitirá a nota de cobrança adicional para que seja efetuado o pagamento referente ao valor glosado;

13.13 A impugnação à glosa, deverá ocorrer no prazo de 3 (três) dias úteis, contados da data do recebimento da notificação.

13.14 Caso a CONTRATADA não apresente a impugnação, ou caso o CONTRATANTE não acolha as razões da impugnação, o valor será deduzido da respectiva nota fiscal.

13.15 Para os inadimplementos que não estão previstos no Anexo I do Termo de Referência, o CONTRATANTE abrirá processo administrativo e seguirá o rito definido nas SANÇÕES ADMINISTRATIVAS;

13.16 Em conformidade com a Instrução Normativa CJF-INN-2016/00001 e as Resoluções nº 169/2013 e nº 183/2013, do Conselho Nacional de Justiça (CNJ), na ocasião do pagamento mensal, serão retidos da CONTRATADA, e transferidos para conta-depósito bloqueada para movimentação os custos relativos às provisões de férias e adicional de férias; ao 13º salário; à multa do FGTS por dispensa sem justa causa; à incidência dos encargos previdenciários e FGTS sobre férias, 1/3 constitucional e 13º salário; e ao valor das despesas com a cobrança de abertura e de manutenção da referida conta vinculada, caso necessário.

13.16.1 Os valores depositados na conta-depósito, bloqueada para movimentação, deixarão de compor o valor mensal devido à empresa.

13.16.2 Os valores retidos da CONTRATADA, referentes às provisões com férias e abono de férias, 13º salário, multa do FGTS, e incidência dos encargos previdenciários e FGTS sobre férias, 1/3 constitucional e 13º salário, serão liberados somente quando da ocorrência e do pagamento das verbas trabalhistas, com prévia autorização do CONTRATANTE, na forma prevista na pela Instrução Normativa CJF-INN-2016/00001 e nas Resoluções CNJ nº 169/2013, 183/2013 e 248/2018.

13.17 Para fins de conformidade com a Instrução Normativa CJF-INN-2016/00001 e as Resoluções CNJ nº 169/2013 e alterações como mão de obra residente e, portanto, suscetível à



PODER JUDICIÁRIO
CONSELHO DA JUSTIÇA FEDERAL

retenção tratada no item anterior, todos os funcionários da CONTRATADA que prestem serviço nas dependências do CJF;

13.18 Os valores retidos na conta-depósito bloqueada para movimentação serão liberados na forma prevista na Instrução Normativa CJF-INN-2016/00001 e nas Resoluções CNJ nº 169/2013, 183/2013 e 248/2018.

13.19 O prazo de pagamento será interrompido nos casos em que haja necessidade de regularização do documento fiscal, o que será devidamente apontado pelo CONTRATANTE.

13.20 A contagem do prazo previsto para pagamento será iniciada a partir da respectiva regularização.

13.21 Nenhum pagamento será efetuado enquanto pendente o cumprimento de qualquer obrigação imposta à CONTRATADA, inclusive em virtude de penalidade ou inadimplência.

13.22 O depósito bancário produzirá os efeitos jurídicos da quitação da prestação devida.

CLÁUSULA DÉCIMA QUARTA - DA ATUALIZAÇÃO MONETÁRIA

14.1 No caso de eventual atraso no pagamento e, desde que a CONTRATADA não tenha concorrido de alguma forma para tanto, haverá incidência de atualização monetária, sobre o valor devido, *pro rata temporis*, ocorrida entre a data limite estipulada para pagamento e a da efetiva realização.

14.1.1 para esse fim, será utilizada a variação acumulada do Índice Nacional de Preços ao Consumidor Amplo/IPCA, calculado e divulgado pelo Instituto Brasileiro de Geografia e Estatística/IBGE.

14.2 O mesmo critério de correção será adotado em relação à devolução dos valores recebidos indevidamente pela CONTRATADA.

CLÁUSULA DÉCIMA QUINTA - DAS PENALIDADES

15.1 O atraso injustificado no cumprimento do objeto, sujeitará a CONTRATADA a multa, sobre o valor mensal do contrato, a título de mora, quais sejam:

15.1.1 MULTA MORATÓRIA de 0,5% (zero vírgula cinco por cento) sobre o valor mensal do contrato, por dia de atraso **na apresentação da nota fiscal de faturamento**, de acordo com os níveis de serviços e eventuais glosas apuradas pelo CONTRATANTE;

15.1.2 MULTA MORATÓRIA de 0,5% (zero vírgula cinco por cento) sobre o valor mensal do contrato, por dia de atraso **na apresentação da relação de profissionais** que prestarão os serviços alocados no CONTRATANTE;

15.1.3 MULTA MORATÓRIA de 0,5% (zero vírgula cinco por cento) do valor mensal do contrato por dia de atraso decorrido **em caso de descumprimento do prazo** estabelecido na cláusula DO CONTINGENCIAMENTO DOS ENCARGOS TRABALHISTAS referente a abertura da conta-depósito vinculada;

15.1.4 MULTA MORATÓRIA de 0,5% (zero vírgula cinco por cento) sobre o valor mensal do contrato por ocorrência em que o **profissional descumprir as exigências de vestimenta**, conforme determinado na PORTARIA CJF-POR-2018/00129 ou norma que vier a sucedê-la;



PODER JUDICIÁRIO
CONSELHO DA JUSTIÇA FEDERAL

15.1.5 MULTA MORATÓRIA de 0,5% (zero vírgula cinco por cento) sobre o valor mensal do contrato por ocorrência em que o profissional **descumprir a norma sobre o controle de acesso**, a circulação e a permanência de pessoas no Conselho da Justiça Federal, conforme determinado na Portaria Ministro Presidente nº 34 de 02/02/2017 ou norma que vier a sucedê-la;

15.1.6 MULTA MORATÓRIA – de 1% (um por cento) sobre o valor mensal do contrato, a cada ocorrência em que a CONTRATADA:

- a) Substituir profissional sem formalizar à CONTRATANTE;
- b) Deixar de afastar profissional que se conduza de modo inconveniente ou que não respeite as normas do CJF ou que não atenda às necessidades, num período de 24 (vinte e quatro) horas corridas a contar da notificação do CONTRATANTE;
- c) Deixar de alocar um novo profissional em caso de substituição, num período de 5 (cinco) dias úteis a contar da notificação do CONTRATANTE quando da substituição;

15.1.7 MULTA MORATÓRIA – de 1,5% (uma vírgula cinco por cento) sobre o valor mensal do contrato, a cada ocorrência em que a CONTRATADA:

- a) Por motivo de negligência, imprudência ou imperícia na execução das atividades contratuais, causar qualquer dano físico ou lógico aos equipamentos da CONTRATANTE;
- b) Descumprir Política, Norma ou Procedimento de Segurança da Informação do CONTRATANTE
- c) Deixar de comunicar formalmente à CONTRATANTE sobre o desligamento de prestador de serviço (profissional que prestava serviço nas dependências do CJF e/ ou remotamente).

15.1.8 MULTA MORATÓRIA de 10% (dez por cento) do valor mensal do contrato pelo não atingimento de um mesmo nível de serviço previsto no ANEXO I, do termo de referência, durante 3 (três) meses consecutivos ou 5 (cinco) meses alternados, apurados em um período de 12 (doze meses);

15.1.9 MULTA MORATÓRIA de 20% (vinte por cento) do valor mensal do contrato pelo não atingimento de um mesmo nível de serviço previsto no ANEXO I, do termo de referência, durante 6 (seis) meses consecutivos ou 10 (cinco) meses não consecutivos, apurados em um período de 12 (doze meses);

15.1.10 Os indicadores fora das metas exigidas no ANEXO I do termo de referência – Níveis Mínimos de Serviço serão considerados como INEXECUÇÃO DOS **SERVIÇOS MENSAIS** do contrato conforme a tabela abaixo, sem prejuízo da aplicação da glosa referente ao indicador não atingido:

PORCENTAGEM ALCANÇADA DO NÍVEL DE SERVIÇO EM RELAÇÃO A META EXIGIDA NO ANEXO I do Termo de Referência	TIPO DE INEXECUÇÃO DOS SERVIÇOS MENSAIS
50% A 69,9%	PARCIAL
0% A 49,9%	TOTAL

Será aplicada:



PODER JUDICIÁRIO
CONSELHO DA JUSTIÇA FEDERAL

- a) MULTA MORATÓRIA de 10% (dez por cento) do valor mensal do contrato, em caso de INEXECUÇÃO PARCIAL DOS SERVIÇOS MENSAIS do contrato; ou
- b) MULTA MORATÓRIA de 20% (vinte por cento) do valor mensal do contrato, em caso de INEXECUÇÃO TOTAL DOS SERVIÇOS MENSAIS do contrato;

15.2 Pela inexecução total ou parcial o CONTRATANTE poderá, nos termos do art. 87 da Lei n. 8.666/1993, aplicar as seguintes sanções:

- a) advertência;
- b) MULTA COMPENSATÓRIA de 10% (dez por cento) do valor total do contrato, em caso de INEXECUÇÃO PARCIAL das obrigações contratuais;
- c) MULTA COMPENSATÓRIA de 20% (vinte por cento) do valor total do contrato, em caso de inexecução total das obrigações contratuais;
- d) suspensão temporária
- e) declaração de inidoneidade

15.3 Nos termos da Lei n. 10.520/2002, art. 7º, o CONTRATANTE poderá aplicar impedimento de licitar àquele que:

Ocorrência	Pena
a) fizer declaração falsa ou apresentar documentação falsa:	Impedimento do direito de licitar e contratar com a União e descredenciamento do Sistema de Cadastramento Unificado de Fornecedores – SICAF, pelo período de 24 (vinte e quatro) meses;
b) falhar na execução do contrato:	Impedimento do direito de licitar e contratar com a União e descredenciamento do SICAF pelo período de 12 (doze) meses;
c) fraudar na execução do contrato:	Impedimento do direito de licitar e contratar com a União e descredenciamento do SICAF pelo período de 30 (trinta) meses;
d) comportar-se de modo inidôneo:	Impedimento do direito de licitar e contratar com a União e descredenciamento do SICAF pelo período de 24 (vinte e quatro) meses;
e) cometer fraude fiscal:	Impedimento do direito de licitar e contratar com a União e descredenciamento do SICAF pelo período de 40 (quarenta) meses;

15.3.1 O CONTRATANTE, para aplicação da penalidade prevista no item anterior, adotará os critérios previstos na Instrução Normativa n. 1, de 13/10/2017, da Presidência da República, publicada no DOU, em 16/10/2017 (n. 198, Seção 1, pag. 5).



PODER JUDICIÁRIO
CONSELHO DA JUSTIÇA FEDERAL

15.4 A não manutenção das condições de habilitação da CONTRATADA ao longo da execução do Contrato, ensejará a rescisão contratual unilateral pelo CONTRATANTE, após regular procedimento administrativo e garantido o direito ao contraditório e à ampla defesa, e ainda a aplicação de multa de 10% sobre o valor da prestação inadimplida.

15.5 A reabilitação será concedida sempre que a CONTRATADA ressarcir a Administração pelos prejuízos resultantes, e depois de decorrido o prazo de suspensão temporária, se aplicada

15.6 As sanções de multa podem ser aplicadas à CONTRATADA juntamente com a de advertência, suspensão temporária do direito de participar de licitação e impedimento de contratar com o Conselho da Justiça Federal e declaração de inidoneidade para licitar ou contratar com a Administração Pública, descontando-a do pagamento a ser efetuado.

15.7 A critério da autoridade competente do CONTRATANTE, com fundamento nos princípios da proporcionalidade e razoabilidade, as penalidades poderão ser relevadas ou atenuadas, em razão de circunstâncias fundamentadas, mediante comprovação dos fatos e, desde que formuladas por escrito, no prazo máximo de 5 (cinco) dias úteis, contados da data da notificação.

15.8 A aplicação das sanções previstas nesta cláusula será realizada mediante processo administrativo específico, mediante comunicação à CONTRATADA da penalidade, sendo assegurado, em todos os casos, o contraditório e a ampla defesa, no prazo de 5 (cinco) dias, contados do recebimento da comunicação.

15.9 Em caso de aplicação de multa, o valor poderá ser descontado da garantia prestada, dos pagamentos eventualmente devidos à CONTRATADA, ser recolhido ao Tesouro por meio Guia de Recolhimento da União – GRU, ou cobrado judicialmente, nos termos do § 3º do art. 86 da Lei n. 8.666/1993.

15.10 O atraso no recolhimento de multas será corrigido monetariamente pela variação acumulada do Índice Nacional de Preços ao Consumidor Amplo/IPCA, calculado e divulgado pelo Instituto Brasileiro de Geografia e Estatística/IBGE

15.11 O CONTRATANTE promoverá o registro no Sistema de Cadastramento Unificado de Fornecedores - SICAF de toda e qualquer penalidade imposta à CONTRATADA.

CLÁUSULA DÉCIMA SEXTA – DA GARANTIA CONTRATUAL

16.1 A CONTRATADA apresentará, nos termos do art. 56 da Lei n. 8.666/1993, em até 20 (vinte) dias úteis, contados da assinatura deste instrumento, garantia de execução do contrato no valor de **R\$ 000** _____(extenso), correspondente a 3% (cinco por cento) do valor total estimado da contratação, tendo como beneficiário o CONTRATANTE, quais sejam:

- a) Caução em dinheiro ou títulos da dívida pública; ou
- b) Seguro – garantia; ou
- c) Fiança bancária.

16.1.1 A CONTRATADA, caso opte pela modalidade de garantia caução, declara que manterá conta de caução específica para o depósito de valores oferecidos em garantia/caução referentes exclusivamente a contratos firmados com o CONTRATANTE.



PODER JUDICIÁRIO
CONSELHO DA JUSTIÇA FEDERAL

16.1.2 No caso de a CONTRATADA optar pela caução em dinheiro, esta deverá ser feita na Caixa Econômica Federal, conforme Decreto-lei n. 1.737, de 21/12/1979.

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

- a) prejuízos advindos do não cumprimento do objeto do contrato;
- b) prejuízos diretos causados ao CONTRATANTE, decorrentes de culpa ou dolo durante a execução do contrato;
- c) multas moratórias e punitivas aplicadas à CONTRATADA;
- d) obrigações trabalhistas e previdenciárias de qualquer natureza, não adimplidas pela CONTRATADA, quando couber;

16.2.1 Caso o valor da garantia venha a ser utilizado em pagamento de qualquer obrigação atribuída à CONTRATADA, esta se obriga a efetuar a respectiva reposição no prazo máximo de 10 (dez) dias úteis, a contar da data do recebimento da comunicação pelo CONTRATANTE.

16.2.2 Prorrogado o prazo de vigência ou alterado o valor do contrato, fica a CONTRATADA obrigada a renovar a garantia, no mesmo percentual e modalidades constantes desta cláusula, em até 20 (vinte) dias úteis, contados da data de assinatura do respectivo instrumento contratual.

16.2.3 A garantia apresentada em desacordo com os requisitos e coberturas previstos neste instrumento será devolvida à CONTRATADA, que disporá do prazo improrrogável de 10 (dez) dias úteis para a regularização da pendência.

16.2.4 O CONTRATANTE poderá executar a garantia para ressarcimento dos valores que a CONTRATADA passe a lhe dever em virtude da ocorrência de qualquer das situações expressamente previstas neste contrato e na legislação pertinente, após a instauração de procedimento administrativo específico.

16.2.5 O valor da garantia reverterá, integralmente, em favor do CONTRATANTE, ou pelo saldo que apresentar, no caso de rescisão contratual por culpa exclusiva da CONTRATADA, sem prejuízo das perdas e danos porventura verificados.

16.2.6 O CONTRATANTE poderá utilizar o valor da garantia prestada para descontar, entre outros, os valores referentes a eventuais multas aplicadas à CONTRATADA, bem como nos casos decorrentes de inadimplemento contratual, e de indenização por danos causados ao Patrimônio da União ou de terceiros, ocorridos nas suas dependências.

16.2.7 A garantia deverá ser prestada com validade de 3 (três) meses após o término da vigência do contrato e será liberada ou restituída ante a comprovação do adimplemento total das obrigações contratuais, desde que não haja pendências.

16.2.8 O termo da garantia será restituído à CONTRATADA após o cumprimento integral de todas as obrigações contratuais.

16.2.9 Na ocorrência de qualquer inadimplemento das obrigações contratadas, o CONTRATANTE notificará a empresa seguradora da expectativa de sinistro com vistas a resguardar a administração de possíveis prejuízos, mediante provocação da unidade gestora responsável pelo acompanhamento da execução contratual, durante a vigência da apólice.



PODER JUDICIÁRIO
CONSELHO DA JUSTIÇA FEDERAL

CLÁUSULA DÉCIMA SÉTIMA – DA RESCISÃO

17.1 Este contrato poderá ser rescindido a juízo do CONTRATANTE, com base nos arts. 77 a 80 da Lei n. 8.666/1993, especialmente quando entender que a CONTRATADA não está cumprindo de forma satisfatória as avenças estabelecidas, independentemente da aplicação das penalidades estabelecidas.

Parágrafo único: Nos casos em que a CONTRATADA sofrer processo de fusão, cisão ou incorporação, será admitida a continuação da contratação desde que a execução deste a execução dos serviços não seja afetada e que a CONTRATADA mantenha o fiel cumprimento dos termos contratuais e as condições de habilitação.

CLÁUSULA DÉCIMA OITAVA – DA PUBLICAÇÃO

18.1 Em conformidade com o disposto na Lei n. 8.666/1993, art.61, parágrafo único, o contrato será publicado no Diário Oficial da União, em forma de extrato.

CLÁUSULA DÉCIMA NONA – DO FORO

19.1 Para dirimir quaisquer conflitos oriundos deste contrato, é competente o foro do Juízo da Seção Judiciária do Distrito Federal, com expressa renúncia a qualquer outro, por mais privilegiado que seja, no que se refere a qualquer ação ou medida judicial originada ou referente ao instrumento contratual.

CLÁUSULA VIGÉSIMA – DAS DISPOSIÇÕES FINAIS

20.1 As partes contratantes ficarão exoneradas do cumprimento das obrigações assumidas neste instrumento, quando ocorrerem motivos de força maior ou caso fortuito, assim definidos no parágrafo único do art. 393 do Código Civil.

20.2 Os casos omissos serão resolvidos à luz das disposições contidas na Lei n. 8.666/1993, bem como dos princípios de direito público.

20.3 É defeso à CONTRATADA utilizar-se deste contrato para caucionar qualquer dívida ou títulos por ela emitidos, seja qual for a natureza.

20.4 A CONTRATADA assumirá, de forma exclusiva, todas as dívidas que venha a contrair com vistas ao cumprimento das obrigações oriundas deste contrato, ficando certo, desde já, que o CONTRATANTE não será responsável solidário.

20.5 A documentação necessária para pagamento, pedido de prorrogação de prazo, recursos, defesa prévia e outros inerentes à contratação deverão ser encaminhados diretamente ao gestor do contrato pelos e-mails: (inserir e-mail gestor, substituto e da unidade).

20.5.1 Alterações nos e-mails apresentados no item anterior, serão comunicados, por escrito, pelo gestor, não acarretando a necessidade de alteração contratual.

E por estarem assim de pleno acordo, assinam as partes este instrumento, na forma eletrônica, para todos os fins de direito.

Juíza Federal SIMONE DOS SANTOS LEMOS FERNANDES



PODER JUDICIÁRIO
CONSELHO DA JUSTIÇA FEDERAL

Secretária-Geral do Conselho da Justiça Federal

SIGNATÁRIO CONTRATADA

MINUTA



PODER JUDICIÁRIO
CONSELHO DA JUSTIÇA FEDERAL

Anexos ao Contrato CJF n. 000/0000,
celebrado entre o **CONSELHO DA JUSTIÇA
FEDERAL** e a **(NOME DA EMPRESA)**, para
a (objeto resumido).

ANEXO I - PLANILHA DE PREÇOS

EXCEL. SERÃO JUNTADAS NO SEI NO MOMENTO DE ENVIO PARA ASSINATURA DAS PARTES

MINUTA

Anexo IV - SEI MJSP 13624102 - Ata_do_pregao_CFJ. pdf

90026.12020.28657.4500.2784290740



CONSELHO DA JUSTIÇA FEDERAL DO DF

Ata de Realização do Pregão Eletrônico
Nº 00001/2020 (SRP)

Às 10:08 horas do dia 05 de fevereiro de 2020, reuniram-se o Pregoeiro Oficial deste Órgão e respectivos membros da Equipe de Apoio, designados pelo instrumento legal 607 de 08/11/2019, em atendimento às disposições contidas na Lei nº 10.520 de 17 de julho de 2002 e no Decreto nº 10.024 de 20 de setembro de 2019, referente ao Processo nº sei 1989-89.19, para realizar os procedimentos relativos ao Pregão nº 00001/2020. Modo de disputa: Aberto. Objeto: Objeto: Pregão Eletrônico - Serviços Gerenciados de Segurança da Informação para atender ao Conselho da Justiça Federal CJF.. O Pregoeiro abriu a Sessão Pública em atendimento às disposições contidas no edital, divulgando as propostas recebidas. Abriu-se em seguida a fase de lances para classificação dos licitantes relativamente aos lances ofertados.

Item: 1 - GRUPO 1**Descrição:** Sustentação de Software**Descrição Complementar:** Serviço de Operação e Atendimento à Requisições**Tratamento Diferenciado:** -**Quantidade:** 24**Unidade de fornecimento:** Unidade**Valor Estimado:** R\$ 67.125,8900**Situação:** Aceito e Habilitado**Intervalo mínimo entre lances:** 1,00 %**Aceito para:** ISH TECNOLOGIA S/A, pelo melhor lance de R\$ 56.520,0000 e a quantidade de 24 Unidade .**Item: 2 - GRUPO 1****Descrição:** Sustentação de Software**Descrição Complementar:** Serviço de gestão de incidentes de segurança (CSIRT - Blue Team)**Tratamento Diferenciado:** -**Quantidade:** 24**Unidade de fornecimento:** Unidade**Valor Estimado:** R\$ 26.200,4100**Situação:** Aceito e Habilitado**Intervalo mínimo entre lances:** 1,00 %**Aceito para:** ISH TECNOLOGIA S/A, pelo melhor lance de R\$ 18.443,6500 e a quantidade de 24 Unidade .**Item: 3 - GRUPO 1****Descrição:** Sustentação de Software**Descrição Complementar:** Serviço de Gestão De Vulnerabilidades.**Tratamento Diferenciado:** -**Quantidade:** 24**Unidade de fornecimento:** Unidade**Valor Estimado:** R\$ 19.994,0900**Situação:** Aceito e Habilitado**Intervalo mínimo entre lances:** 1,00 %**Aceito para:** ISH TECNOLOGIA S/A, pelo melhor lance de R\$ 17.040,6500 e a quantidade de 24 Unidade .**Item: 4 - GRUPO 1****Descrição:** Sustentação de Software**Descrição Complementar:** Serviço de Monitoramento e Visibilidade de Ataques Cibernéticos**Tratamento Diferenciado:** -**Quantidade:** 24**Unidade de fornecimento:** Unidade**Valor Estimado:** R\$ 45.784,6900**Situação:** Aceito e Habilitado**Intervalo mínimo entre lances:** 1,00 %**Aceito para:** ISH TECNOLOGIA S/A, pelo melhor lance de R\$ 26.217,3400 e a quantidade de 24 Unidade .**Item: 5 - GRUPO 1****Descrição:** Sustentação de Software**Descrição Complementar:** Serviço de Orquestração, Automação e Resposta de Segurança (SOAR)**Tratamento Diferenciado:** -**Quantidade:** 24**Unidade de fornecimento:** Unidade**Valor Estimado:** R\$ 24.921,4200**Situação:** Aceito e Habilitado**Intervalo mínimo entre lances:** 1,00 %**Aceito para:** ISH TECNOLOGIA S/A, pelo melhor lance de R\$ 24.670,0000 e a quantidade de 24 Unidade .**Item: 6 - GRUPO 1**

Descrição: Sustentação de Software**Descrição Complementar:** Serviço de Testes de Invasão (Red Team)**Tratamento Diferenciado:** -**Quantidade:** 15**Unidade de fornecimento:** Unidade**Valor Estimado:** R\$ 14.703,6700**Situação:** Aceito e Habilitado**Intervalo mínimo entre lances:** 1,00 %**Aceito para:** ISH TECNOLOGIA S/A, pelo melhor lance de R\$ 11.508,4000 e a quantidade de 15 Unidade .**Relação de Grupos****GRUPO 1****Tratamento Diferenciado:** -**Aplicabilidade Margem de Preferência:** Não**Critério de Valor:** R\$ 4.637.191,0500**Situação:** Aceito e Habilitado com intenção de recurso**Aceito para:** ISH TECNOLOGIA S/A, pelo melhor lance de R\$ 3.602.025,3600 .**Itens do grupo:**

- 1 - Sustentação de Software
- 2 - Sustentação de Software
- 3 - Sustentação de Software
- 4 - Sustentação de Software
- 5 - Sustentação de Software
- 6 - Sustentação de Software

Histórico**Item: 1 - GRUPO 1 - Sustentação de Software****Propostas** Participaram deste item as empresas abaixo relacionadas, com suas respectivas propostas.

(As propostas com * na frente foram desclassificadas)

CNPJ/CPF	Fornecedor	Porte ME/EPP	Declaração ME/EPP/COOP	Quantidade	Valor Unit.	Valor Global	Data/Hora Registro
15.690.857/0002-39	APURA COMERCIO DE SOFTWARES E ASSESSORIA EM TECNOLOGIA	Não	Não	24	R\$ 61.125,8900	R\$ 1.467.021,3600	04/02/2020 20:11:43
Descrição Detalhada do Objeto Ofertado: Serviço de Operação e Atendimento à Requisições							
01.707.536/0001-04	ISH TECNOLOGIA S/A	Não	Não	24	R\$ 67.124,0000	R\$ 1.610.976,0000	05/02/2020 00:23:34
Descrição Detalhada do Objeto Ofertado: Serviço de Operação e Atendimento à Requisições							
03.017.428/0001-35	NCT INFORMATICA LTDA	Não	Não	24	R\$ 67.125,8900	R\$ 1.611.021,3600	05/02/2020 09:04:36
Descrição Detalhada do Objeto Ofertado: Serviço de Operação e Atendimento a Requisições, 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 íntegro, conforme proposta de preços anexa a esse termo.							
03.970.788/0001-57	CIPHER S.A.	Não	Não	24	R\$ 94.524,1200	R\$ 2.268.578,8800	05/02/2020 00:18:48

Descrição Detalhada do Objeto Ofertado: Serviço de Operação e Atendimento à Requisições**Lances** (Obs: lances com * na frente foram excluídos pelo pregoeiro)

Valor do Lance	CNPJ/CPF	Data/Hora Registro
R\$ 94.524,1200	03.970.788/0001-57	05/02/2020 10:08:00:357
R\$ 67.125,8900	03.017.428/0001-35	05/02/2020 10:08:00:357
R\$ 67.124,0000	01.707.536/0001-04	05/02/2020 10:08:00:357
R\$ 61.125,8900	15.690.857/0002-39	05/02/2020 10:08:00:357
R\$ 61.358,7900	01.707.536/0001-04	05/02/2020 10:18:04:393
R\$ 65.000,0000	03.017.428/0001-35	05/02/2020 10:20:51:357
R\$ 63.000,0000	03.017.428/0001-35	05/02/2020 10:22:05:810
R\$ 60.312,4000	01.707.536/0001-04	05/02/2020 10:23:49:077
R\$ 50.000,0000	03.017.428/0001-35	05/02/2020 10:25:47:273
R\$ 57.219,9400	01.707.536/0001-04	05/02/2020 10:38:37:970

R\$ 56.520,0000

01.707.536/0001-04

05/02/2020 10:39:56:187

R\$ 60.000,0000

15.690.857/0002-39

05/02/2020 10:48:23:293

Não existem lances de desempate ME/EPP para o item**Eventos do Item**

Evento	Data	Observações
Recusa	11/02/2020 15:37:46	Recusa da proposta. Fornecedor: NCT INFORMATICA LTDA, CNPJ/CPF: 03.017.428/0001-35, pelo melhor lance de R\$ 50.000,0000. Motivo: Por não atender requisitos técnicos exigidos em edital
Recusa	11/02/2020 15:59:32	Recusa da proposta. Fornecedor: APURA COMERCIO DE SOFTWARES E ASSESSORIA EM TECNOLOGIA, CNPJ/CPF: 15.690.857/0002-39, pelo melhor lance de R\$ 60.000,0000. Motivo: Por não apresentar documentos de habilitação, juntamente com proposta, de acordo com o art. 26 do Decreto 10.024/2019
Aceite	14/02/2020 15:28:01	Aceite individual da proposta. Fornecedor: ISH TECNOLOGIA S/A, CNPJ/CPF: 01.707.536/0001-04, pelo melhor lance de R\$ 56.520,0000.
Habilitado	14/02/2020 15:29:06	Habilitação em grupo de propostas. Fornecedor: ISH TECNOLOGIA S/A - CNPJ/CPF: 01.707.536/0001-04

Para consultar intenção de recurso do item, verificar histórico do GRUPO 1.**Item: 2 - GRUPO 1 - Sustentação de Software**

Propostas Participaram deste item as empresas abaixo relacionadas, com suas respectivas propostas.
(As propostas com * na frente foram desclassificadas)

CNPJ/CPF	Fornecedor	Porte ME/EPP	Declaração ME/EPP/COOP	Quantidade	Valor Unit.	Valor Global	Data/Hora Registro
01.707.536/0001-04	ISH TECNOLOGIA S/A	Não	Não	24	R\$ 26.000,0000	R\$ 624.000,0000	05/02/2020 00:23:34
Descrição Detalhada do Objeto Ofertado: Serviço de gestão de incidentes de segurança (CSIRT - Blue Team)							
15.690.857/0002-39	APURA COMERCIO DE SOFTWARES E ASSESSORIA EM TECNOLOGIA	Não	Não	24	R\$ 26.200,4100	R\$ 628.809,8400	04/02/2020 20:11:43
Descrição Detalhada do Objeto Ofertado: Serviço de Gestão de Incidentes de Segurança (CSIRT - Blue Team)							
03.017.428/0001-35	NCT INFORMATICA LTDA	Não	Não	24	R\$ 26.200,4100	R\$ 628.809,8400	05/02/2020 09:04:36
Descrição Detalhada do Objeto Ofertado: Serviço de gestão de incidentes de segurança (CSIRT - Blue Team) com a finalidade de 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, conforme proposta de preços anexa a esse termo.							
03.970.788/0001-57	CIPHER S.A.	Não	Não	24	R\$ 31.300,4100	R\$ 751.209,8400	05/02/2020 00:18:48
Descrição Detalhada do Objeto Ofertado: Serviço de Gestão de Incidentes de Segurança (CSIRT - Blue Team)							

Lances (Obs: lances com * na frente foram excluídos pelo pregoeiro)

Valor do Lance	CNPJ/CPF	Data/Hora Registro
R\$ 31.300,4100	03.970.788/0001-57	05/02/2020 10:08:00:357
R\$ 26.200,4100	03.017.428/0001-35	05/02/2020 10:08:00:357
R\$ 26.200,4100	15.690.857/0002-39	05/02/2020 10:08:00:357
R\$ 26.000,0000	01.707.536/0001-04	05/02/2020 10:08:00:357
R\$ 25.000,0000	03.017.428/0001-35	05/02/2020 10:20:31:777
R\$ 25.033,8200	01.707.536/0001-04	05/02/2020 10:20:38:967
R\$ 23.603,4500	01.707.536/0001-04	05/02/2020 10:24:36:053
R\$ 20.938,2400	01.707.536/0001-04	05/02/2020 10:25:34:683
R\$ 20.410,5600	01.707.536/0001-04	05/02/2020 10:27:04:603
R\$ 18.769,5300	01.707.536/0001-04	05/02/2020 10:28:12:437
R\$ 18.443,6500	01.707.536/0001-04	05/02/2020 10:28:17:507
R\$ 20.000,0000	03.017.428/0001-35	05/02/2020 10:29:41:803
R\$ 18.000,0000	03.017.428/0001-35	05/02/2020 10:39:32:217

Não existem lances de desempate ME/EPP para o item**Eventos do Item**

Evento	Data	Observações

Recusa	11/02/2020 15:37:46	Recusa da proposta. Fornecedor: NCT INFORMATICA LTDA, CNPJ/CPF: 03.017.428/0001-35, pelo melhor lance de R\$ 18.000,0000. Motivo: Por não atender requisitos técnicos exigidos em edital
Recusa	11/02/2020 15:59:32	Recusa da proposta. Fornecedor: APURA COMERCIO DE SOFTWARES E ASSESSORIA EM TECNOLOGIA, CNPJ/CPF: 15.690.857/0002-39, pelo melhor lance de R\$ 26.200,4100. Motivo: Por não apresentar documentos de habilitação, juntamente com proposta, de acordo com o art. 26 do Decreto 10.024/2019
Aceite	14/02/2020 15:28:01	Aceite individual da proposta. Fornecedor: ISH TECNOLOGIA S/A, CNPJ/CPF: 01.707.536/0001-04, pelo melhor lance de R\$ 18.443,6500.
Habilitado	14/02/2020 15:29:06	Habilitação em grupo de propostas. Fornecedor: ISH TECNOLOGIA S/A - CNPJ/CPF: 01.707.536/0001-04

Para consultar intenção de recurso do item, verificar histórico do GRUPO 1.

Item: 3 - GRUPO 1 - Sustentação de Software

Propostas Participaram deste item as empresas abaixo relacionadas, com suas respectivas propostas.

(As propostas com * na frente foram desclassificadas)

CNPJ/CPF	Fornecedor	Porte ME/EPP	Declaração ME/EPP/COOP	Quantidade	Valor Unit.	Valor Global	Data/Hora Registro
01.707.536/0001-04	ISH TECNOLOGIA S/A	Não	Não	24	R\$ 19.990,0000	R\$ 479.760,0000	05/02/2020 00:23:34
Descrição Detalhada do Objeto Ofertado: Serviço de Gestão De Vulnerabilidades.							
15.690.857/0002-39	APURA COMERCIO DE SOFTWARES E ASSESSORIA EM TECNOLOGIA	Não	Não	24	R\$ 19.994,0900	R\$ 479.858,1600	04/02/2020 20:11:43
Descrição Detalhada do Objeto Ofertado: Serviço de Gestão de Vulnerabilidades							
03.017.428/0001-35	NCT INFORMATICA LTDA	Não	Não	24	R\$ 19.994,0900	R\$ 479.858,1600	05/02/2020 09:04:36
Descrição Detalhada do Objeto Ofertado: Serviço de gestão de vulnerabilidades, para, de forma proativa e recorrente, identificar possíveis vulnerabilidades de segurança da informação no ambiente a fim de evitar que ataques cibernéticos obtenham sucesso explorando, conforme proposta de preços anexa a esse termo. vulnerabilidades conhecidas, conforme proposta de preços anexa a esse termo.							
03.970.788/0001-57	CIPHER S.A.	Não	Não	24	R\$ 45.130,1500	R\$ 1.083.123,6000	05/02/2020 00:18:48

Descrição Detalhada do Objeto Ofertado: Serviço de Gestão de Vulnerabilidades

Lances (Obs: lances com * na frente foram excluídos pelo pregoeiro)

Valor do Lance	CNPJ/CPF	Data/Hora Registro
R\$ 45.130,1500	03.970.788/0001-57	05/02/2020 10:08:00:357
R\$ 19.994,0900	15.690.857/0002-39	05/02/2020 10:08:00:357
R\$ 19.994,0900	03.017.428/0001-35	05/02/2020 10:08:00:357
R\$ 19.990,0000	01.707.536/0001-04	05/02/2020 10:08:00:357
R\$ 18.000,0000	03.017.428/0001-35	05/02/2020 10:20:14:463
R\$ 18.414,0100	01.707.536/0001-04	05/02/2020 10:20:55:183
R\$ 18.161,9800	01.707.536/0001-04	05/02/2020 10:21:05:190
R\$ 18.959,0000	15.690.857/0002-39	05/02/2020 10:22:30:860
R\$ 15.500,0000	03.017.428/0001-35	05/02/2020 10:23:46:170
R\$ 17.265,3800	01.707.536/0001-04	05/02/2020 10:24:56:227
R\$ 17.040,6500	01.707.536/0001-04	05/02/2020 10:25:50:780

Não existem lances de desempate ME/EPP para o item

Eventos do Item

Evento	Data	Observações
Recusa	11/02/2020 15:37:46	Recusa da proposta. Fornecedor: NCT INFORMATICA LTDA, CNPJ/CPF: 03.017.428/0001-35, pelo melhor lance de R\$ 15.500,0000. Motivo: Por não atender requisitos técnicos exigidos em edital
Recusa	11/02/2020 15:59:32	Recusa da proposta. Fornecedor: APURA COMERCIO DE SOFTWARES E ASSESSORIA EM TECNOLOGIA, CNPJ/CPF: 15.690.857/0002-39, pelo melhor lance de R\$ 18.959,0000. Motivo: Por não apresentar documentos de habilitação, juntamente com proposta, de acordo com o art. 26 do Decreto 10.024/2019
Aceite	14/02/2020 15:28:01	Aceite individual da proposta. Fornecedor: ISH TECNOLOGIA S/A, CNPJ/CPF: 01.707.536/0001-04, pelo melhor lance de R\$ 17.040,6500.
Habilitado	14/02/2020 15:29:06	Habilitação em grupo de propostas. Fornecedor: ISH TECNOLOGIA S/A - CNPJ/CPF: 01.707.536/0001-04

Para consultar intenção de recurso do item, verificar histórico do GRUPO 1.

Item: 4 - GRUPO 1 - Sustentação de Software

Propostas Participaram deste item as empresas abaixo relacionadas, com suas respectivas propostas.

(As propostas com * na frente foram desclassificadas)

CNPJ/CPF	Fornecedor	Porte ME/EPP	Declaração ME/EPP/COOP	Quantidade	Valor Unit.	Valor Global	Data/Hora Registro
01.707.536/0001-04	ISH TECNOLOGIA S/A	Não	Não	24	R\$ 45.760,0000	R\$ 1.098.240,0000	05/02/2020 00:23:34
Descrição Detalhada do Objeto Ofertado: Serviço de Monitoramento e Visibilidade de Ataques Cibernéticos							
15.690.857/0002-39	APURA COMERCIO DE SOFTWARES E ASSESSORIA EM TECNOLOGIA	Não	Não	24	R\$ 45.784,6900	R\$ 1.098.832,5600	04/02/2020 20:11:43
Descrição Detalhada do Objeto Ofertado: Serviço de Monitoramento e Visibilidade de Ataques Cibernéticos							
03.017.428/0001-35	NCT INFORMATICA LTDA	Não	Não	24	R\$ 45.784,6900	R\$ 1.098.832,5600	05/02/2020 09:04:36
Descrição Detalhada do Objeto Ofertado: Serviço de monitoramento e visibilidade de ataques cibernéticos, para 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, conforme proposta de preços anexa a esse termo. da informação.							
03.970.788/0001-57	CIPHER S.A.	Não	Não	24	R\$ 85.428,2700	R\$ 2.050.278,4800	05/02/2020 00:18:48
Descrição Detalhada do Objeto Ofertado: Serviço de Monitoramento e Visibilidade de Ataques Cibernético, incluindo SIEM, UEBA e NTA							

Lances (Obs: lances com * na frente foram excluídos pelo pregoeiro)

Valor do Lance	CNPJ/CPF	Data/Hora Registro
R\$ 85.428,2700	03.970.788/0001-57	05/02/2020 10:08:00:357
R\$ 45.784,6900	15.690.857/0002-39	05/02/2020 10:08:00:357
R\$ 45.784,6900	03.017.428/0001-35	05/02/2020 10:08:00:357
R\$ 45.760,0000	01.707.536/0001-04	05/02/2020 10:08:00:357
R\$ 45.000,0000	03.017.428/0001-35	05/02/2020 10:19:47:793
R\$ 43.755,7000	01.707.536/0001-04	05/02/2020 10:22:08:710
R\$ 40.000,0000	15.690.857/0002-39	05/02/2020 10:23:42:183
R\$ 38.000,0000	15.690.857/0002-39	05/02/2020 10:24:53:477
R\$ 42.568,5700	01.707.536/0001-04	05/02/2020 10:24:56:570
R\$ 35.000,0000	15.690.857/0002-39	05/02/2020 10:25:30:323
R\$ 36.445,5800	01.707.536/0001-04	05/02/2020 10:25:51:107
R\$ 30.000,0000	15.690.857/0002-39	05/02/2020 10:26:42:703
R\$ 35.540,5100	01.707.536/0001-04	05/02/2020 10:27:42:303
R\$ 29.000,0000	15.690.857/0002-39	05/02/2020 10:28:38:643
R\$ 34.509,7700	01.707.536/0001-04	05/02/2020 10:28:42:533
R\$ 34.069,9400	01.707.536/0001-04	05/02/2020 10:29:46:353
R\$ 28.500,0000	15.690.857/0002-39	05/02/2020 10:30:39:980
R\$ 43.500,0000	03.017.428/0001-35	05/02/2020 10:31:11:263
R\$ 32.541,9300	01.707.536/0001-04	05/02/2020 10:31:14:613
R\$ 28.000,0000	15.690.857/0002-39	05/02/2020 10:31:51:743
R\$ 27.000,0000	15.690.857/0002-39	05/02/2020 10:32:20:207
R\$ 32.025,7000	01.707.536/0001-04	05/02/2020 10:32:26:840
R\$ 31.529,3700	01.707.536/0001-04	05/02/2020 10:32:47:303
R\$ 31.162,1200	01.707.536/0001-04	05/02/2020 10:33:29:687
R\$ 42.000,0000	03.017.428/0001-35	05/02/2020 10:33:49:780
R\$ 30.500,0000	01.707.536/0001-04	05/02/2020 10:34:10:023
R\$ 26.000,0000	15.690.857/0002-39	05/02/2020 10:34:30:367
R\$ 29.655,4600	01.707.536/0001-04	05/02/2020 10:34:35:527
R\$ 29.300,0000	01.707.536/0001-04	05/02/2020 10:35:52:413

R\$ 25.500,0000	15.690.857/0002-39	05/02/2020 10:36:05:783
R\$ 29.000,0000	01.707.536/0001-04	05/02/2020 10:36:42:377
R\$ 28.602,7000	01.707.536/0001-04	05/02/2020 10:37:00:153
R\$ 28.264,8500	01.707.536/0001-04	05/02/2020 10:38:13:983
R\$ 40.000,0000	03.017.428/0001-35	05/02/2020 10:38:32:383
R\$ 27.957,8300	01.707.536/0001-04	05/02/2020 10:39:09:187
R\$ 27.206,1300	01.707.536/0001-04	05/02/2020 10:39:56:913
R\$ 24.500,0000	15.690.857/0002-39	05/02/2020 10:40:13:133
R\$ 26.900,0000	01.707.536/0001-04	05/02/2020 10:40:52:987
R\$ 23.500,0000	15.690.857/0002-39	05/02/2020 10:41:03:467
R\$ 26.217,3400	01.707.536/0001-04	05/02/2020 10:41:07:367
R\$ 22.500,0000	15.690.857/0002-39	05/02/2020 10:42:51:357
R\$ 38.000,0000	03.017.428/0001-35	05/02/2020 10:44:13:517
R\$ 21.000,0000	15.690.857/0002-39	05/02/2020 10:44:38:957
R\$ 20.000,0000	15.690.857/0002-39	05/02/2020 10:46:06:940
R\$ 35.000,0000	03.017.428/0001-35	05/02/2020 10:47:25:247
R\$ 19.000,0000	15.690.857/0002-39	05/02/2020 10:47:42:607
R\$ 18.000,0000	15.690.857/0002-39	05/02/2020 10:47:56:820
R\$ 32.000,0000	03.017.428/0001-35	05/02/2020 10:49:15:183
R\$ 17.000,0000	15.690.857/0002-39	05/02/2020 10:49:37:380
R\$ 16.000,0000	15.690.857/0002-39	05/02/2020 10:52:22:980
R\$ 30.000,0000	03.017.428/0001-35	05/02/2020 10:52:57:093

Não existem lances de desempate ME/EPP para o item

Eventos do Item

Evento	Data	Observações
Recusa	11/02/2020 15:37:46	Recusa da proposta. Fornecedor: NCT INFORMATICA LTDA, CNPJ/CPF: 03.017.428/0001-35, pelo melhor lance de R\$ 30.000,0000. Motivo: Por não atender requisitos técnicos exigidos em edital
Recusa	11/02/2020 15:59:32	Recusa da proposta. Fornecedor: APURA COMERCIO DE SOFTWARES E ASSESSORIA EM TECNOLOGIA, CNPJ/CPF: 15.690.857/0002-39, pelo melhor lance de R\$ 16.000,0000. Motivo: Por não apresentar documentos de habilitação, juntamente com proposta, de acordo com o art. 26 do Decreto 10.024/2019
Aceite	14/02/2020 15:28:01	Aceite individual da proposta. Fornecedor: ISH TECNOLOGIA S/A, CNPJ/CPF: 01.707.536/0001-04, pelo melhor lance de R\$ 26.217,3400.
Habilitado	14/02/2020 15:29:06	Habilitação em grupo de propostas. Fornecedor: ISH TECNOLOGIA S/A - CNPJ/CPF: 01.707.536/0001-04

Para consultar intenção de recurso do item, verificar histórico do GRUPO 1.

Item: 5 - GRUPO 1 - Sustentação de Software

Propostas Participaram deste item as empresas abaixo relacionadas, com suas respectivas propostas.
(As propostas com * na frente foram desclassificadas)

CNPJ/CPF	Fornecedor	Porte ME/EPP	Declaração ME/EPP/COOP	Quantidade	Valor Unit.	Valor Global	Data/Hora Registro
01.707.536/0001-04	ISH TECNOLOGIA S/A	Não	Não	24	R\$ 24.920,0000	R\$ 598.080,0000	05/02/2020 00:23:34
Descrição Detalhada do Objeto Ofertado: Serviço de Orquestração, Automação e Resposta de Segurança (SOAR)							
15.690.857/0002-39	APURA COMERCIO DE SOFTWARES E ASSESSORIA EM TECNOLOGIA	Não	Não	24	R\$ 24.921,4200	R\$ 598.114,0800	04/02/2020 20:11:43
Descrição Detalhada do Objeto Ofertado: Serviço de Orquestração, Automação e Resposta de Segurança (SOAR)							
03.017.428/0001-35	NCT INFORMATICA LTDA	Não	Não	24	R\$ 24.921,4200	R\$ 598.114,0800	05/02/2020 09:04:36
Descrição Detalhada do Objeto Ofertado: Serviço de orquestração, para a automação e resposta de segurança (SOAR), com o objetivo de automatizar os processos e fluxos de trabalho, a aplicação de atividades rotineiras ou de difícil execução e a orquestração das diversas ferramentas de segurança, sem necessidade de atuação humana, conforme proposta de preços anexa a esse termo.							
03.970.788/0001-57	CIPHER S.A.	Não	Não	24	R\$ 84.250,0000	R\$ 2.022.000,0000	05/02/2020

Descrição Detalhada do Objeto Ofertado: Serviço de Orquestração, Automação e Resposta de Segurança (SOAR)

Lances (Obs: lances com * na frente foram excluídos pelo pregoeiro)

Valor do Lance	CNPJ/CPF	Data/Hora Registro
R\$ 84.250,0000	03.970.788/0001-57	05/02/2020 10:08:00:357
R\$ 24.921,4200	03.017.428/0001-35	05/02/2020 10:08:00:357
R\$ 24.921,4200	15.690.857/0002-39	05/02/2020 10:08:00:357
R\$ 24.920,0000	01.707.536/0001-04	05/02/2020 10:08:00:357
R\$ 24.000,0000	03.017.428/0001-35	05/02/2020 10:18:35:147
R\$ 23.000,0000	15.690.857/0002-39	05/02/2020 10:24:34:803
R\$ 21.000,0000	15.690.857/0002-39	05/02/2020 10:26:57:240
R\$ 20.000,0000	15.690.857/0002-39	05/02/2020 10:27:39:687
R\$ 18.000,0000	15.690.857/0002-39	05/02/2020 10:28:07:200
R\$ 17.500,0000	15.690.857/0002-39	05/02/2020 10:32:04:787
R\$ 17.000,0000	15.690.857/0002-39	05/02/2020 10:32:42:540
R\$ 16.500,0000	15.690.857/0002-39	05/02/2020 10:33:25:003
R\$ 16.000,0000	15.690.857/0002-39	05/02/2020 10:34:22:697
R\$ 22.000,0000	03.017.428/0001-35	05/02/2020 10:35:49:687
R\$ 15.500,0000	15.690.857/0002-39	05/02/2020 10:36:55:613
R\$ 24.670,0000	01.707.536/0001-04	05/02/2020 10:37:42:173
R\$ 15.000,0000	15.690.857/0002-39	05/02/2020 10:37:51:647
R\$ 12.000,0000	15.690.857/0002-39	05/02/2020 10:38:32:737
R\$ 11.500,0000	15.690.857/0002-39	05/02/2020 10:38:59:817
R\$ 20.000,0000	03.017.428/0001-35	05/02/2020 10:39:48:730
R\$ 11.000,0000	15.690.857/0002-39	05/02/2020 10:40:22:430
R\$ 18.000,0000	03.017.428/0001-35	05/02/2020 10:42:32:007
R\$ 10.800,0000	15.690.857/0002-39	05/02/2020 10:44:54:397
R\$ 10.500,0000	15.690.857/0002-39	05/02/2020 10:45:07:613
R\$ 10.000,0000	15.690.857/0002-39	05/02/2020 10:46:15:003
R\$ 9.000,0000	15.690.857/0002-39	05/02/2020 10:47:35:113
R\$ 8.000,0000	15.690.857/0002-39	05/02/2020 10:49:28:130
R\$ 17.500,0000	03.017.428/0001-35	05/02/2020 10:50:32:900

Não existem lances de desempate ME/EPP para o item

Eventos do Item

Evento	Data	Observações
Recusa	11/02/2020 15:37:46	Recusa da proposta. Fornecedor: NCT INFORMATICA LTDA, CNPJ/CPF: 03.017.428/0001-35, pelo melhor lance de R\$ 17.500,0000. Motivo: Por não atender requisitos técnicos exigidos em edital
Recusa	11/02/2020 15:59:32	Recusa da proposta. Fornecedor: APURA COMERCIO DE SOFTWARES E ASSESSORIA EM TECNOLOGIA, CNPJ/CPF: 15.690.857/0002-39, pelo melhor lance de R\$ 8.000,0000. Motivo: Por não apresentar documentos de habilitação, juntamente com proposta, de acordo com o art. 26 do Decreto 10.024/2019
Aceite	14/02/2020 15:28:01	Aceite individual da proposta. Fornecedor: ISH TECNOLOGIA S/A, CNPJ/CPF: 01.707.536/0001-04, pelo melhor lance de R\$ 24.670,0000.
Habilitado	14/02/2020 15:29:06	Habilitação em grupo de propostas. Fornecedor: ISH TECNOLOGIA S/A - CNPJ/CPF: 01.707.536/0001-04

Para consultar intenção de recurso do item, verificar histórico do GRUPO 1.

Item: 6 - GRUPO 1 - Sustentação de Software

Propostas Participaram deste item as empresas abaixo relacionadas, com suas respectivas propostas.

(As propostas com * na frente foram desclassificadas)

CNPJ/CPF	Fornecedor	Porte ME/EPP	Declaração ME/EPP/COOP	Quantidade	Valor Unit.	Valor Global	Data/Hora Registro
01.707.536/0001-04	ISH TECNOLOGIA S/A	Não	Não	15	R\$ 14.700,0000	R\$ 220.500,0000	05/02/2020 00:23:34
Descrição Detalhada do Objeto Ofertado: Serviço de Testes de Invasão (Red Team)							
15.690.857/0002-39	APURA COMERCIO DE SOFTWARES E	Não	Não	15	R\$ 14.703,6700	R\$ 220.555,0500	04/02/2020 20:11:43

ASSESSORIA
EM
TECNOLOGIA**Descrição Detalhada do Objeto Ofertado:** Serviço de Testes de Invasão (Red Team)

03.017.428/0001-35	NCT INFORMATICA LTDA	Não	Não	15	R\$ 14.703,6700	R\$ 220.555,0500	05/02/2020 09:04:36

Descrição Detalhada do Objeto Ofertado: Serviço de testes de invasão (Red Team), com a finalidade de 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, conforme proposta de preços anexa a esse termo.

03.970.788/0001-57	CIPHER S.A.	Não	Não	15	R\$ 20.835,0000	R\$ 312.525,0000	05/02/2020 00:18:48

Descrição Detalhada do Objeto Ofertado: Serviço de Testes de Invasão (Red Team)**Lances** (Obs: lances com * na frente foram excluídos pelo pregoeiro)

Valor do Lance	CNPJ/CPF	Data/Hora Registro
R\$ 20.835,0000	03.970.788/0001-57	05/02/2020 10:08:00:357
R\$ 14.703,6700	03.017.428/0001-35	05/02/2020 10:08:00:357
R\$ 14.703,6700	15.690.857/0002-39	05/02/2020 10:08:00:357
R\$ 14.700,0000	01.707.536/0001-04	05/02/2020 10:08:00:357
R\$ 12.000,0000	03.017.428/0001-35	05/02/2020 10:17:53:117
R\$ 12.223,4400	01.707.536/0001-04	05/02/2020 10:23:46:807
R\$ 11.633,3200	01.707.536/0001-04	05/02/2020 10:25:32:397
R\$ 11.508,4000	01.707.536/0001-04	05/02/2020 10:27:02:270
R\$ 10.000,0000	03.017.428/0001-35	05/02/2020 10:45:29:743

Não existem lances de desempate ME/EPP para o item**Eventos do Item**

Evento	Data	Observações
Recusa	11/02/2020 15:37:46	Recusa da proposta. Fornecedor: NCT INFORMATICA LTDA, CNPJ/CPF: 03.017.428/0001-35, pelo melhor lance de R\$ 10.000,0000. Motivo: Por não atender requisitos técnicos exigidos em edital
Recusa	11/02/2020 15:59:32	Recusa da proposta. Fornecedor: APURA COMERCIO DE SOFTWARES E ASSESSORIA EM TECNOLOGIA, CNPJ/CPF: 15.690.857/0002-39, pelo melhor lance de R\$ 14.703,6700. Motivo: Por não apresentar documentos de habilitação, juntamente com proposta, de acordo com o art. 26 do Decreto 10.024/2019
Aceite	14/02/2020 15:28:01	Aceite individual da proposta. Fornecedor: ISH TECNOLOGIA S/A, CNPJ/CPF: 01.707.536/0001-04, pelo melhor lance de R\$ 11.508,4000.
Habilitado	14/02/2020 15:29:06	Habilitação em grupo de propostas. Fornecedor: ISH TECNOLOGIA S/A - CNPJ/CPF: 01.707.536/0001-04

Para consultar intenção de recurso do item, verificar histórico do GRUPO 1.**HISTÓRICO DO GRUPO 1**

Propostas Participaram deste grupo as empresas abaixo relacionadas, com suas respectivas propostas.
(As propostas com * na frente foram desclassificadas)

CNPJ/CPF	Fornecedor	Porte ME/EPP	Declaração ME/EPP/COOP	Quantidade	Valor Global	Data/Hora Registro
15.690.857/0002-39	APURA COMERCIO DE SOFTWARES E ASSESSORIA EM TECNOLOGIA	Não	Não	-	R\$ 4.493.191,0500	04/02/2020 20:11:43
01.707.536/0001-04	ISH TECNOLOGIA S/A	Não	Não	-	R\$ 4.631.556,0000	05/02/2020 00:23:34
03.017.428/0001-35	NCT INFORMATICA LTDA	Não	Não	-	R\$ 4.637.191,0500	05/02/2020 09:04:36
03.970.788/0001-57	CIPHER S.A.	Não	Não	-	R\$ 8.487.715,8000	05/02/2020 00:18:48

Eventos do Grupo

Evento	Data	Observações
Aberto	05/02/2020 10:16:33	Item Aberto.
Encerrado	05/02/2020 10:54:57	Item encerrado.
Abertura do prazo de Convocação - Anexo	05/02/2020 11:28:28	Convocado para envio de anexo o fornecedor NCT INFORMATICA LTDA, CNPJ/CPF: 03.017.428/0001-35.

Encerramento do prazo de Convocação - Anexo	05/02/2020 12:30:59	Encerrado o prazo de Convocação de Anexo pelo fornecedor NCT INFORMATICA LTDA, CNPJ/CPF: 03.017.428/0001-35.
Abertura do prazo de Convocação - Anexo	07/02/2020 14:03:36	Convocado para envio de anexo o fornecedor NCT INFORMATICA LTDA, CNPJ/CPF: 03.017.428/0001-35.
Encerramento do prazo de Convocação - Anexo	07/02/2020 14:10:33	Encerrado o prazo de Convocação de Anexo pelo fornecedor NCT INFORMATICA LTDA, CNPJ/CPF: 03.017.428/0001-35.
Abertura do prazo de Convocação - Anexo	07/02/2020 18:19:03	Convocado para envio de anexo o fornecedor NCT INFORMATICA LTDA, CNPJ/CPF: 03.017.428/0001-35.
Encerramento do prazo de Convocação - Anexo	10/02/2020 12:38:25	Encerrado o prazo de Convocação de Anexo pelo fornecedor NCT INFORMATICA LTDA, CNPJ/CPF: 03.017.428/0001-35.
Abertura do prazo de Convocação - Anexo	11/02/2020 16:04:29	Convocado para envio de anexo o fornecedor ISH TECNOLOGIA S/A, CNPJ/CPF: 01.707.536/0001-04.
Encerramento do prazo de Convocação - Anexo	11/02/2020 17:22:36	Encerrado o prazo de Convocação de Anexo pelo fornecedor ISH TECNOLOGIA S/A, CNPJ/CPF: 01.707.536/0001-04.
Abertura do prazo de Convocação - Anexo	12/02/2020 16:05:32	Convocado para envio de anexo o fornecedor ISH TECNOLOGIA S/A, CNPJ/CPF: 01.707.536/0001-04.
Encerramento do prazo de Convocação - Anexo	13/02/2020 12:31:22	Encerrado o prazo de Convocação de Anexo pelo fornecedor ISH TECNOLOGIA S/A, CNPJ/CPF: 01.707.536/0001-04.
Habilitado	14/02/2020 15:29:06	Habilitação em grupo de propostas. Fornecedor: ISH TECNOLOGIA S/A - CNPJ/CPF: 01.707.536/0001-04
Registro Intenção de Recurso	14/02/2020 15:32:07	Registro de Intenção de Recurso. Fornecedor: NCT INFORMATICA LTDA CNPJ/CPF: 03017428000135. Motivo: Manifestamos intenção de interposição de recurso contra a desclassificação da empresa NCT e declaração de vitória da licitante ISH. Conforme será exposto nas razões de recurso, a inabilitação da NCT s
Intenção de Recurso Aceita	14/02/2020 16:11:11	Intenção de recurso aceita. Fornecedor: NCT INFORMATICA LTDA, CNPJ/CPF: 03017428000135. Motivo: Por atender os requisitos de admissibilidade

Intenções de Recurso para o Grupo

CNPJ/CPF	Data/Hora do Recurso	Data/Hora Admissibilidade	Situação
03.017.428/0001-35	14/02/2020 15:32	14/02/2020 16:11	Aceito
Motivo Intenção: Manifestamos intenção de interposição de recurso contra a desclassificação da empresa NCT e declaração de vitória da licitante ISH. Conforme será exposto nas razões de recurso, a inabilitação da NCT se deu por razões técnicas inconsistentes, tendo em vista que a documentação atende integralmente o estabelecido em edital. Ademais, há inconsistências na documentação da ISH, o que será devidamente demonstrado na peça recursal.			
Motivo Aceite ou Recusa: Por atender os requisitos de admissibilidade			

Troca de Mensagens

	Data	Mensagem
Pregoeiro	05/02/2020 10:08:56	Boa tarde senhores fornecedores, informo que a sessão encontra-se aberta, pregoeiro Márcio Gomes
Pregoeiro	05/02/2020 10:16:33	O item G1 foi aberto. Solicitamos o envio de lances.
Pregoeiro	05/02/2020 10:49:36	Senhores fornecedores, solicito observar a exequibilidade das propostas
Sistema	05/02/2020 10:54:57	O item G1 está encerrado.
Sistema	05/02/2020 10:54:57	Todos os itens estão encerrados. Será iniciada a etapa de Julgamento de Propostas. Favor acompanhar através da funcionalidade "Acompanhar julgamento/habilitação/admissibilidade".
Pregoeiro	05/02/2020	Para NCT INFORMATICA LTDA - Caro fornecedor, solicito o envio da proposta atualizada

	11:28:13	de acordo com o valor oferecido, em planilha de Excel, Ressaltando que de acordo com o edital, Item VI - Da Proposta Eletrônica de Preços, subitem 4.1.2 que valores maiores ou menores do previsto na nossa nota técnica deverá ser justificado, até as 14h de hoje. obrigado.
Sistema	05/02/2020 11:28:28	Senhor fornecedor NCT INFORMATICA LTDA, CNPJ/CPF: 03.017.428/0001-35, solicito o envio do anexo referente ao grupo G1.
03.017.428/0001-35	05/02/2020 11:29:02	Bom dia
03.017.428/0001-35	05/02/2020 11:31:56	Encaminharemos conforme solicitado
Pregoeiro	05/02/2020 11:34:48	ok, obrigado
Sistema	05/02/2020 12:30:59	Senhor Pregoeiro, o fornecedor NCT INFORMATICA LTDA, CNPJ/CPF: 03.017.428/0001-35, enviou o anexo para o grupo G1.
Pregoeiro	05/02/2020 14:01:44	Boa tarde
Pregoeiro	05/02/2020 14:19:29	Informo que estamos analisando a proposta e demais documentos, junto com a área técnica
Pregoeiro	05/02/2020 16:44:17	Informo que foi feito pedido de diligência a empresa NCT e que a sessão será suspensão e reaberta amanhã, 06/02/2020, às 14 horas
Pregoeiro	06/02/2020 14:03:20	Boa tarde senhores fornecedores, informo que a sessão encontra-se reaberta pregoeiro Márcio Gomes
Pregoeiro	06/02/2020 14:53:05	Informo que o pedido de diligência se resume em: comprovação do RAT ajustado Comprovante de recolhimento do Incra Ajuste no vale transporte Verificação da alíquota do ISS e do substituto de férias maiores detalhes em relação aos atestados técnicos
Pregoeiro	06/02/2020 14:54:40	Informo que a empresa NCT enviou, via e-mail, resposta ao pedido de diligência e estamos analisado.
Pregoeiro	06/02/2020 16:44:57	Para NCT INFORMATICA LTDA - Informo que para o Serviço de Operação e Atendimento a Requisições há a possibilidade de horas extras, mas não consta tal previsão na planilha de custos.
Pregoeiro	06/02/2020 16:47:56	Para NCT INFORMATICA LTDA - Em análise dos documentos de habilitação apresentados pela empresa NCT, foi verificado pela equipe de planejamento da contratação, que nas planilhas de composição do salário apresentadas pela empresa licitante, levando em consideração os quantitativos dos serviços, a qualificação exigida, bem como os salários praticados no mercado de trabalho local,
Pregoeiro	06/02/2020 16:49:13	Para NCT INFORMATICA LTDA - observa-se que tais valores encontram-se em desacordo com a média salarial do mercado. Dessa forma, solicito demonstração comprobatória de que já tenha contratado ou tenha condições reais de contratar, pelos valores propostos, profissionais com QUALIFICAÇÃO IGUAL OU SUPERIOR À EXIGIDA NO ITEM 13 _ PERFIS DOS PROFISSIONAIS, DO TERMO DE REFERÊNCIA
03.017.428/0001-35	06/02/2020 16:53:42	Boa tarde
03.017.428/0001-35	06/02/2020 16:55:12	Qual prazo para envio da comprovação solicitada?
Pregoeiro	06/02/2020 16:56:13	Para NCT INFORMATICA LTDA - Qual seria o tempo necessário?
03.017.428/0001-35	06/02/2020 17:04:54	Em razão do término do expediente da área de RH, solicitamos até amanhã 11h. Agradecemos.
Pregoeiro	06/02/2020 17:07:37	Para NCT INFORMATICA LTDA - Prazo concedido até as 13h30 do dia 07/02
Pregoeiro	06/02/2020 17:08:15	Informo que a sessão será suspensão e reaberta amanhã, 07/02/2020, às 14h.
Pregoeiro	07/02/2020 14:03:04	Boa tarde senhores fornecedores, informo que a sessão encontra-se reaberta, pregoeiro Márcio Gomes
Sistema	07/02/2020 14:03:36	Senhor fornecedor NCT INFORMATICA LTDA, CNPJ/CPF: 03.017.428/0001-35, solicito o envio do anexo referente ao grupo G1.
Sistema	07/02/2020 14:10:33	Senhor Pregoeiro, o fornecedor NCT INFORMATICA LTDA, CNPJ/CPF: 03.017.428/0001-35, enviou o anexo para o grupo G1.
Pregoeiro	07/02/2020 14:45:11	Para NCT INFORMATICA LTDA - segue pedido de diligência por parte da área técnica: "Solicito que a licitante apresente comprovação que os componentes da ofertada para o Serviço de Gestão de Vulnerabilidades, incluindo gerência, atende ao item 9.15 do Termo de Referência: "As soluções de prestação dos Serviços de Gestão de Vulnerabilidades deverão ser instaladas no CONTRATANTE, ...
Pregoeiro	07/02/2020 14:45:28	Para NCT INFORMATICA LTDA - ... de modo a prover varredura, identificação e gestão de vulnerabilidades do parque computacional do CONTRATANTE."
03.017.428/0001-35	07/02/2020 14:48:47	Boa tarde.
Pregoeiro	07/02/2020 14:50:56	Para NCT INFORMATICA LTDA - e mais um pedido de diligência por parte da área técnica: Com relação à resposta sobre a diligência 5, que trata sobre o item 10.3.48 do Termo de Referência, foram enviados alguns links referenciando documentação do fabricante, sendo que: ...

Pregoeiro	07/02/2020 14:51:10	Para NCT INFORMATICA LTDA - 1. Em vários documentos do fabricante consta a seguinte informação: "This functionality is experimental and may be changed or removed completely in a future release. Elastic will take a best effort approach to fix any issues, but experimental features are not subject to the support SLA of official GA features".
Pregoeiro	07/02/2020 14:51:24	Para NCT INFORMATICA LTDA - Evidenciando que trata-se funcionalidade experimental e em desenvolvimento, que pode haver descontinuidade a qualquer momento. Além de não possuir nível de serviço para atendimento (SLA) do fabricante nem desenvolvimento de novas funcionalidades.
Pregoeiro	07/02/2020 14:51:37	Para NCT INFORMATICA LTDA - 2. Não foi encontrado de forma inequívoca a informação de que o produto é capaz de realizar o correlacionamento de eventos complexos (conceito em inglês "Complex Event Processing - CEP), conforme é exigido pelo item 10.3.48 do EDITAL PE N.1/2020.
Pregoeiro	07/02/2020 14:51:49	Para NCT INFORMATICA LTDA - 3. Observou-se que o produto faz Machine Learning para a análise preditiva de eventos e padrões, não inteligência artificial.
03.017.428/0001-35	07/02/2020 14:55:23	Sr pregoeiro, mais alguma consideração?
03.017.428/0001-35	07/02/2020 14:56:10	E dentro do apresentado, qual o prazo para entrega das respostas?
03.017.428/0001-35	07/02/2020 15:04:29	Aguardamos.
Pregoeiro	07/02/2020 15:12:20	Para NCT INFORMATICA LTDA - a principio somente estas
Pregoeiro	07/02/2020 15:12:50	Para NCT INFORMATICA LTDA - Quanto tempo necessário?
03.017.428/0001-35	07/02/2020 15:15:04	Em razão da demanda técnica, até às 13h do próximo dia útil. Agradecemos.
Pregoeiro	07/02/2020 15:38:49	Para NCT INFORMATICA LTDA - ok
Pregoeiro	07/02/2020 18:06:05	Para NCT INFORMATICA LTDA - Em análise a resposta da diligência feita aos documentos de habilitação apresentados, foi verificado pela equipe de planejamento da contratação, que nas planilhas de composição do salário apresentadas pela empresa licitante, levando em consideração: os quantitativos dos serviços, a qualificação exigida, ...
Pregoeiro	07/02/2020 18:07:20	Para NCT INFORMATICA LTDA - em edital e com o salário proposto pela empresa na PLANILHA DE CUSTOS. Tal solicitação está exigida nos seguintes itens do edital 4.3 e 9
Pregoeiro	07/02/2020 18:08:40	Para NCT INFORMATICA LTDA - 4.3 Caso sejam apresentadas propostas de preços consideradas inexequíveis, levando-se em conta os quantitativos dos serviços, a qualificação exigida, bem como os salários praticados no mercado de trabalho local, o CJF poderá realizar diligências junto à licitante, consultando a planilha de formação de preços, para verificar a capacidade ...
Pregoeiro	07/02/2020 18:09:04	Para NCT INFORMATICA LTDA - de cumprir com a proposta de prestação de serviços apresentada.
Pregoeiro	07/02/2020 18:09:20	Para NCT INFORMATICA LTDA - 9 Os preços deverão ser finais, acrescidos de todas as despesas e conter somente duas casas decimais, não sendo admitidos valores simbólicos, irrisórios ou de valor zero, incompatíveis com os preços dos insumos e salários de mercado, acrescidos dos respectivos encargos, conforme definido no §3º do art. 44 da Lei n. 8.666/93
Pregoeiro	07/02/2020 18:10:18	Para NCT INFORMATICA LTDA - Para fins da demonstração comprobatória exigida, solicitamos a apresentação de cópias da carteira de trabalho (CTPS), do contrato de trabalho ou instrumento similar, de profissionais que já prestaram serviços equivalentes para a licitante mediante salário igual ou inferior ao de sua proposta; ...
Pregoeiro	07/02/2020 18:10:33	Para NCT INFORMATICA LTDA - ou, ainda, declarações de profissionais que se comprometam a prestar os serviços objeto desta contratação, mediante o salário constante da proposta da licitante. ESSES PROFISSIONAIS DEVERÃO ATENDER AOS REQUISITOS DE QUALIFICAÇÃO ESTIPULADOS NO ITEM 13 DO TERMO DE REFERÊNCIA - PERFS DOS PROFISSIONAIS.
03.017.428/0001-35	07/02/2020 18:12:51	Boa noite.
Pregoeiro	07/02/2020 18:13:41	Para NCT INFORMATICA LTDA - NCT, segue mais esta diligência, por favor responder no prazo já concedido, 10/02/2020
03.017.428/0001-35	07/02/2020 18:16:55	Procederemos conforme solicitado.
Pregoeiro	07/02/2020 18:18:07	Para NCT INFORMATICA LTDA - ok
Pregoeiro	07/02/2020 18:18:52	Para NCT INFORMATICA LTDA - Informo que a sessão será suspensa e reaberta na segunda-feira, 10/02/2020, às 14h
Sistema	07/02/2020 18:19:03	Senhor fornecedor NCT INFORMATICA LTDA, CNPJ/CPF: 03.017.428/0001-35, solicito o envio do anexo referente ao grupo G1.
Sistema	10/02/2020 12:38:25	Senhor Pregoeiro, o fornecedor NCT INFORMATICA LTDA, CNPJ/CPF: 03.017.428/0001-35, enviou o anexo para o grupo G1.
Pregoeiro	10/02/2020 14:01:48	Boa tarde senhores fornecedores, informo que a sessão encontra-se reaberta, pregoeiro Márcio Gomes

Pregoeiro	10/02/2020 14:59:57	Informo que os documentos recebidos por parte da NCT estão sendo analisados
Pregoeiro	10/02/2020 18:04:40	Informo que devido ao horário, a sessão será suspensa e reaberta amanhã, 11/02/2020, às 15h
Pregoeiro	11/02/2020 15:02:54	Boa tarde senhores fornecedores informo que a sessão encontra-se reaberta, pregoeiro Márcio Gomes
Pregoeiro	11/02/2020 15:16:30	Para NCT INFORMATICA LTDA - Caro fornecedor, após análise criteriosa pela área técnica foi verificado que esta empresa não atendeu o requisito de qualificação técnica, subitem m.3 do Edital: Experiência na prestação de serviços de administração de solução de antimalware para ambiente de datacenter utilizando plataforma de virtualização de rede VMware NSX com, no mínimo, 200 (duzentos)
Pregoeiro	11/02/2020 15:17:10	Para NCT INFORMATICA LTDA - servidores de rede.
Pregoeiro	11/02/2020 15:18:09	Para NCT INFORMATICA LTDA - A atestado apresentado por esta empresa é relativo à virtualização de servidores, o que não guarda similaridade com o requisito exigido pelo do edital, a saber, administração de solução de segurança para data center utilizando plataforma de virtualização de rede
Pregoeiro	11/02/2020 15:18:28	Para NCT INFORMATICA LTDA - Cabe salientar que à época da emissão dos atestados apresentados, o produto de virtualização de rede sequer existia.
Pregoeiro	11/02/2020 15:19:05	Para NCT INFORMATICA LTDA - Desta forma, a proposta será recusada
03.017.428/0001-35	11/02/2020 15:19:05	Boa tarde.
03.017.428/0001-35	11/02/2020 15:25:25	Prezado Pregoeiro, não concordamos com a recusa, oportunidade em que apresentaremos nossos argumentos em petição.
Pregoeiro	11/02/2020 15:29:54	Para NCT INFORMATICA LTDA - ok, obrigado pela atenção
Pregoeiro	11/02/2020 15:39:28	Informo que a empresa NCT teve sua proposta recusada, por não atender requisitos técnicos, já informados no chat
Pregoeiro	11/02/2020 15:44:42	Para APURA COMERCIO DE SOFTWARES E ASSESSORIA EM TECNOLOGIA - Caro fornecedor, em análise a sua proposta de preços, não localizei a planilha de preços, Anexo II do Termo de Referência
15.690.857/0002-39	11/02/2020 15:46:11	Prezado Sr. pregoeiro, boa tarde.
15.690.857/0002-39	11/02/2020 15:49:32	Solicitamos prazo para encaminhamento da proposta reajustada aos valores finais do pregão, com respectiva planilha de preços.
Pregoeiro	11/02/2020 15:56:10	Para APURA COMERCIO DE SOFTWARES E ASSESSORIA EM TECNOLOGIA - Infelizmente não será possível, pois de acordo com o art. 26 do Decreto 10.024/2019 os documentos de habilitação exigidos em edital serão encaminhados concomitante com a proposta (observar item VI da proposta eletrônica de preço e dos documentos de habilitação, do edital)
Pregoeiro	11/02/2020 16:00:36	Informo que a empresa Apura teve sua proposta recusada por não apresentar documentos de habilitação, juntamente com proposta, de acordo com o art. 26 do Decreto 10.024/2019
Sistema	11/02/2020 16:04:29	Senhor fornecedor ISH TECNOLOGIA S/A, CNPJ/CPF: 01.707.536/0001-04, solicito o envio do anexo referente ao grupo G1.
Pregoeiro	11/02/2020 16:06:01	Para ISH TECNOLOGIA S/A - Caro fornecedor, solicito o envio da proposta atualizada, de acordo com o valor oferecido na fase de lances, e planilha de preços, em Excel, por favor, no prazo de até duas horas
01.707.536/0001-04	11/02/2020 16:52:00	Sr. Pregoeiro, boa tarde. Enviaremos no prazo solicitado.
Pregoeiro	11/02/2020 17:02:07	Para ISH TECNOLOGIA S/A - ok, obrigado
Sistema	11/02/2020 17:22:36	Senhor Pregoeiro, o fornecedor ISH TECNOLOGIA S/A, CNPJ/CPF: 01.707.536/0001-04, enviou o anexo para o grupo G1.
Pregoeiro	11/02/2020 17:46:16	Informo que devido ao horário, a sessão será suspensa e reaberta amanhã, 12/02/2020, às 14h
Pregoeiro	12/02/2020 14:00:42	Boa tarde senhores fornecedores, informo que a sessão encontra-se reaberta, pregoeiro Márcio Gomes
Pregoeiro	12/02/2020 15:11:48	Para ISH TECNOLOGIA S/A - Caro fornecedor postarei aqui alguns pedidos de esclarecimentos: Que seja apresentada a topologia proposta para a prestação do Serviço de Operação e Atendimento à Requisições envolvendo os produtos ServiceNOW ITSM + SECOPS, considerando que o CJF já utiliza o ITSM da ServiceNOW
Pregoeiro	12/02/2020 15:12:01	Para ISH TECNOLOGIA S/A - Que seja apresentada a topologia proposta para a prestação do Serviço de Gestão de Vulnerabilidades envolvendo os produtos Tenable Nexus pro, Acunetix, e RSA Archer VM
Pregoeiro	12/02/2020 15:12:11	Para ISH TECNOLOGIA S/A - Que seja apresentada a topologia proposta para a prestação do Serviço de Análise de Comportamento de Usuário (UBA) envolvendo os produtos RSA UEBA Essentials + Analytics
Pregoeiro	12/02/2020 15:12:28	Para ISH TECNOLOGIA S/A - Que a licitante detalhe quais módulos ou modelos de licenciamento dos produtos ServiceNOW ITSM + SECOPS, RSA ACHER ISSUE, Tanable

Nexus pro, Acunetix, RSA Archer VM, RSA Netwitness Logs, RSA UEBA Essentials + Analytics, RSA Netwitness Packets, RSA Netwitness Orchestrator estão sendo ofertados

Pregoeiro	12/02/2020 15:13:20	Para ISH TECNOLOGIA S/A - Solicito que a licitante apresente comprovação que os componentes da ofertada para o Serviço de Gestão de Vulnerabilidades, incluindo gerência, atende ao item 9.15 do Termo de Referência: "As soluções de prestação dos Serviços de Gestão de Vulnerabilidades deverão ser instaladas no CONTRATANTE, de modo a prover varredura, identificação e gestão ...
Pregoeiro	12/02/2020 15:13:47	Para ISH TECNOLOGIA S/A - ... de vulnerabilidades do parque computacional do CONTRATANTE
Pregoeiro	12/02/2020 15:15:04	Para ISH TECNOLOGIA S/A - Que seja apresentada comprovação que a solução ofertada para o Serviço de Visibilidade de Logs, Fluxos e Informações é capaz de atender ao item 10.3.48 do Termo de Referência: "A solução deve possuir a capacidade de análise avançada de eventos em tempo real através de regras de correlacionamento e eventos complexos em dados correlacionados através da ...
Pregoeiro	12/02/2020 15:15:22	Para ISH TECNOLOGIA S/A - linguagem EPL (Event Processing Language) ou inteligência artificial
Pregoeiro	12/02/2020 15:19:42	Não há previsão de vale transporte?
Pregoeiro	12/02/2020 15:20:40	Qual foi a base para cálculo do auxílio-refeição, assistência médica e odontológica?
Pregoeiro	12/02/2020 15:21:59	Enviar o comprovante do RAT ajustado e do recolhimento do INCRA
Pregoeiro	12/02/2020 15:22:58	Envio de comprovante de tributação do lucro presumido
Pregoeiro	12/02/2020 15:23:14	no Submódulo 4.1, alínea A substituto na cobertura de férias o nosso percentual é 0,69
Pregoeiro	12/02/2020 15:45:01	em relação ao ISS, por favor observar a Lei Complementar n. 963, de 03/01/2020, do GDF, com a alíquota de 2%
Pregoeiro	12/02/2020 15:45:38	Para ISH TECNOLOGIA S/A - Os questionamentos postados foram para a ISH,
01.707.536/0001-04	12/02/2020 15:48:01	Sr. Pregoeiro, Boa tarde, Confirmo o recebimento dos questionamentos. Solicitamos um prazo até amanhã, dia 13/02/2020 às 18:00h para resposta.
Pregoeiro	12/02/2020 15:49:30	Para ISH TECNOLOGIA S/A - solicito o envio dos esclarecimentos e/ou documentos até amanhã, 13/02, às 15h
01.707.536/0001-04	12/02/2020 15:52:56	ok
Pregoeiro	12/02/2020 16:05:10	Informo que a sessão será suspensa e reaberta amanhã, 13/02/2020, às 15h
Sistema	12/02/2020 16:05:32	Senhor fornecedor ISH TECNOLOGIA S/A, CNPJ/CPF: 01.707.536/0001-04, solicito o envio do anexo referente ao grupo G1.
Sistema	13/02/2020 12:31:22	Senhor Pregoeiro, o fornecedor ISH TECNOLOGIA S/A, CNPJ/CPF: 01.707.536/0001-04, enviou o anexo para o grupo G1.
Pregoeiro	13/02/2020 15:05:32	Senhores fornecedores, informo que a sessão encontra-se reaberta, pregoeiro Márcio Gomes
Pregoeiro	13/02/2020 18:49:54	Devido ao horário, informo que a sessão será suspensa e reaberta amanhã, 14/02/2020, às 14h
Pregoeiro	14/02/2020 14:03:57	Boa tarde senhores fornecedores, informo que a sessão encontra-se reaberta, pregoeiro Márcio Gomes
Pregoeiro	14/02/2020 14:34:51	Para ISH TECNOLOGIA S/A - Caro fornecedor, solicito verificar e informar a possibilidade de redução no valor da proposta, obrigado
01.707.536/0001-04	14/02/2020 14:36:42	Sr. Pregoeiro, Infelizmente não temos possibilidade de redução do valor.
Pregoeiro	14/02/2020 15:17:00	Para ISH TECNOLOGIA S/A - ok
Sistema	14/02/2020 15:29:06	Srs. Fornecedores, está aberto o prazo para registro de intenção de recursos para os itens/grupos na situação de 'aceito e habilitado' ou 'cancelado no julgamento'.
Pregoeiro	14/02/2020 15:29:49	Foi informado o prazo final para registro de intenção de recursos: 14/02/2020 às 16:05:00.

Eventos do Pregão

Evento	Data/Hora	Observações
Alteração de Pregoeiro/Equipe de Apoio	03/02/2020 17:12:49	Pregoeiro Anterior: 42794633368-ANTONIO ANTUNES DE OLIVEIRA . Pregoeiro Atual: 41767659172-MARCIO GOMES DA SILVA . Justificativa: retorno de férias
Alteração de Pregoeiro/Equipe de Apoio	07/02/2020 13:22:15	Pregoeiro Anterior: 41767659172-MARCIO GOMES DA SILVA . Pregoeiro Atual: 42794633368-ANTONIO ANTUNES DE OLIVEIRA . Justificativa: Necessidade de acesso.

Alteração de Pregoeiro/Equipe de Apoio	07/02/2020 13:24:30	Pregoeiro Anterior: 42794633368-ANTONIO ANTUNES DE OLIVEIRA . Pregoeiro Atual: 41767659172-MARCIO GOMES DA SILVA . Justificativa: Pregoeiro titular da licitação retornou.
Abertura de Prazo	14/02/2020 15:29:06	Abertura de prazo para intenção de recurso
Informado Fechamento de Prazo	14/02/2020 15:29:49	Fechamento de prazo para registro de intenção de recurso: 14/02/2020 às 16:05:00.

Data limite para registro de recurso: 19/02/2020.
Data limite para registro de contrarrazão: 26/02/2020.
Data limite para registro de decisão: 11/03/2020.

Após encerramento da Sessão Pública, os licitantes melhores classificados foram declarados vencedores dos respectivos itens. Foi divulgado o resultado da Sessão Pública e foi concedido o prazo recursal conforme preconiza o artigo 45, do Decreto 10.024 de 20 de setembro de 2019. Nada mais havendo a declarar, foi encerrada a sessão às 16:32 horas do dia 14 de fevereiro de 2020, cuja ata foi lavrada e assinada pelo Pregoeiro e Equipe de Apoio.

MARCIO GOMES DA SILVA
Pregoeiro Oficial

LEUMAISE APARECIDA DOS SANTOS
Equipe de Apoio

TAMIRES HANIERY DE SOUZA SILVA
Equipe de Apoio



[Voltar](#)



Anexo V - SEI MJSP 14781049 - Despacho 333.pdf



14781049



08006.000401/2021-54



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

DESPACHO Nº 333/2021/CGISE/DTIC/SE/MJ

CDestino: **DTIC**

Assunto: **Informática: Planos e Projetos**

Interessado(a): **CRS/CGGOV**

1. Em complemento ao DESPACHO Nº 320/2021/CGISE/DTIC/SE/MJ (14756341), deve ser salientado ainda que o MJSP está na eminência da assinatura do novo contrato de serviços de computação em nuvem decorrente da Ata de Registro de Preços 1/2021 (14056156), cujo dimensionamento é suficiente para atendimento da demanda de análise e correlação de logs no volume mencionado (200 GB/dia) por meio da ferramenta Azure Sentinel, sem que para isso seja necessária a aquisição em separado de licenciamento adicional.

Atenciosamente,



Documento assinado eletronicamente por **Leonardo Garcia Greco, Coordenador(a)-Geral de Infraestrutura e Serviços**, em 27/05/2021, às 16:42, conforme o § 1º do art. 6º e art. 10 do Decreto nº 8.539/2015.



A autenticidade do documento pode ser conferida no site <http://sei.autentica.mj.gov.br> informando o código verificador **14781049** e o código CRC **847F0F68**.
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 08006.000401/2021-54

SEI nº 14781049

Anexo VI - SEI MJSP 14612910 - Despacho 80.pdf



14612910



08006.000401/2021-54



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

DESPACHO Nº 80/2021/CRS/CGGOV/DTIC/SE/MJ

Destino: **CGGOV, CGISE, DTIC**

Assunto: **Volume de Logs e Uso da Nuvem para armazenamento**

Interessado(a): **MJSP**

1. Considerando que a Coordenação de Riscos e Segurança de TIC está a frente da confecção dos documentos necessários à contratação do 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 abrangendo: aplicativos, equipamentos, infraestrutura física e pessoal, Serviço de tratamento e resposta aos incidentes cibernéticos - CSIRT - Blue Team e Serviço de teste de invasão - Red Team a ser licitado por essa DTIC.
2. Considerando que após o levantamento realizado junto à contratada responsável pela sustentação tecnológica de infraestrutura do Ministério, obteve-se um volume de 137 GB/Dia, como montante atual de coleta de registros e eventos de segurança gerados pelos equipamentos de TIC.
3. Considerando que a CRS realizou avaliação similar por meio dos quantitativos de equipamentos de TIC em produção, ao todo 557 equipamentos entre: servidores de aplicação, servidores de rede, ativos de rede, firewalls e demais ativos de TIC, utilizando uma ferramenta online de calculadora de Eventos por Segundo - EPS, no site [LogPoint](#), obtendo um total de 187 GB/Dia ou 4.783 Eventos por Segundo (EPS), conforme tabela abaixo:

Equipamentos	Quantitativo	Central IT (GB/Dia)	Estimativa LogPoint (GB/Dia)	Estimativa LogPoint (EPS)
Servidores Windows HIGH_END (1)	59	19,2	23,26	413
Servidores Windows MID_END	88	28,8	14,87	264
Linux Servers	160	5	11,59	480

Network Routers	14	1	0,28	14
Network Switches	16	0,5	0,26	32
Network Flows (NetFlow/SFlow)	2	2	1,93	60
Network Wireless LAN	2	0,5	0,12	10
Network Load-Balancers	4		0,24	20
Other Network Devices	150	11	30,17	1500
Network Firewalls (Layer 7 - DMZ)	10	46	40,23	1000
Network IPS/IDS	2	11	4,83	200
Network Web Proxy	8	11	8,37	160
HyperVisor (ESXi, Hyper-V etc)	42	0,1	50,69	630
Total	557	136,1	186,84	4783

Tabela 1: Estimativa de Logs e EPS comparativa.

4. Considerando que após pesquisa em documentações oficiais da Microsoft a respeito do produto de nuvem Azure Sentinel, especificamente quanto à residência dos dados armazenados pela ferramenta identificou-se, conforme endereço eletrônico <https://azure.microsoft.com/en-us/global-infrastructure/data-residency/>, que a Microsoft não armazenará ou processará dados do cliente fora da área geográfica especificada pelo cliente sem sua permissão, exceto para alguns produtos e dentre a relação consta o Azure Sentinel.

5. Considerando que diante dessa informação a CRS entrou em contato com a gerente de contas da Microsoft para o Ministério no sentido de obter melhores esclarecimentos quanto a residência dos dados de log de segurança do Ministério e, após esse contato, obtivemos como resposta os seguintes esclarecimentos por meio do e-mail abaixo:

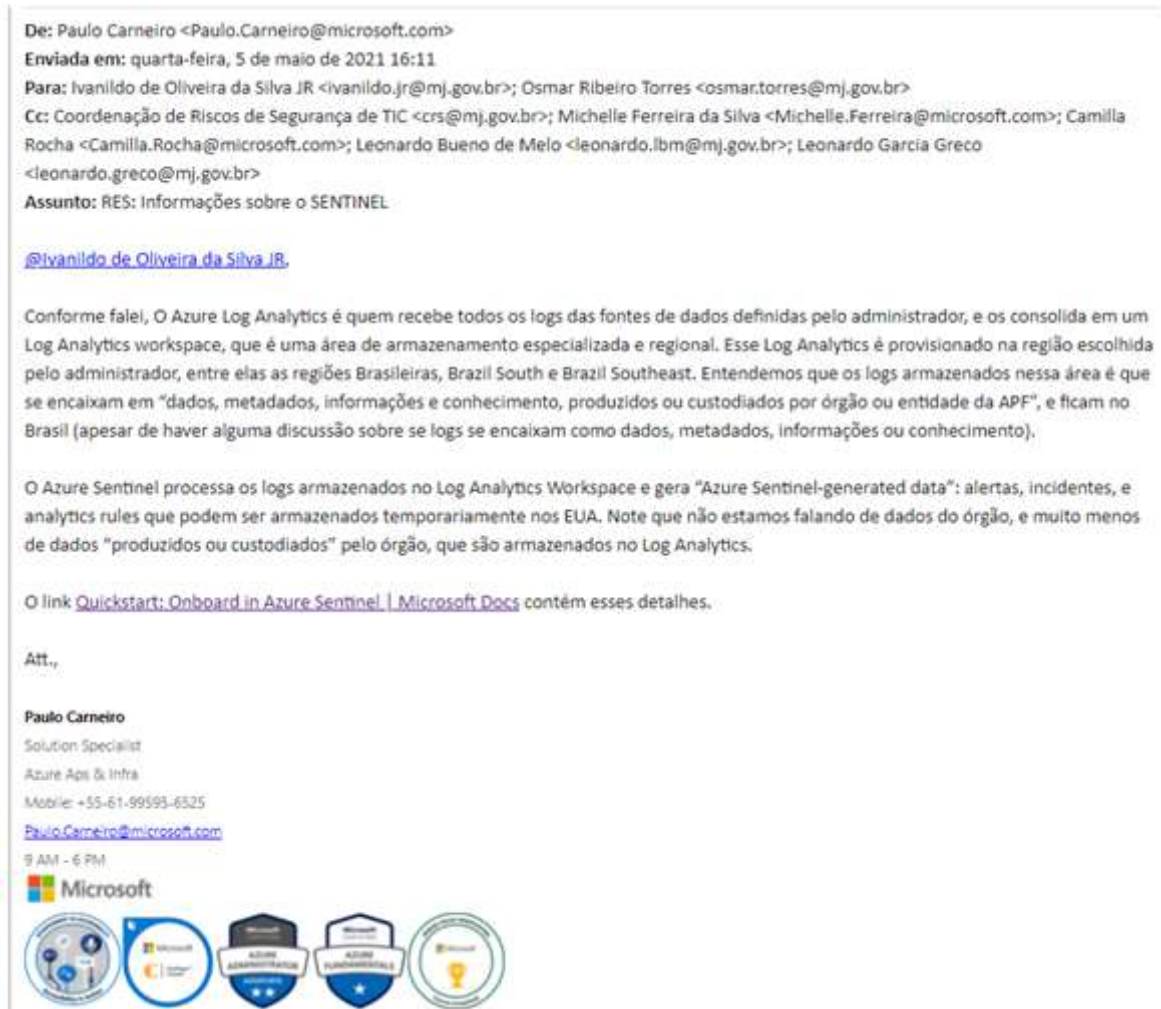


Figura 1 - Resposta da Microsoft acerca da utilização do Microsoft Azure Sentinel.

6. Diante do exposto, e visando à adequada instrução do processo de contratação em epígrafe, solicita-se encaminhar as considerações supracitadas:

6.1. Ao Coordenador-Geral de Infraestrutura e Serviços de TIC, para manifestação quanto à capacidade da DTIC para processar e armazenar o volume diário estimado de logs de segurança da ordem de 200 GB por dia no contexto das operações do Security Operations Center - SOC; e

6.2. Ao Diretor de Tecnologia da Informação e Comunicação, para avaliação quanto à conformidade da ferramenta citada no item 4 às presentes restrições normativas acerca do armazenamento de dados em nuvem por órgãos governamentais, considerando as informações trazidas no item 5, bem como para autorizar a continuidade do processo por parte da Equipe de Planejamento da Contratação.

7. Por fim, encaminhamos à CGGOV para análise e demais encaminhamentos conforme solicitado.

Respeitosamente,



Documento assinado eletronicamente por **IVANILDO DE OLIVEIRA DA SILVA JUNIOR**, **Coordenador(a) de Riscos e Segurança de TIC**, em 07/05/2021, às 19:56, conforme o § 1º do art. 6º e art. 10 do Decreto nº 8.539/2015.

A autenticidade do documento pode ser conferida no site <http://sei.autentica.mj.gov.br> informando o código verificador **14612910** e o código CRC **B5959618**

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 08006.000401/2021-54

SEI nº 14612910

Anexo VII - SEI MJSP 14424141 - PDTIC_2021_2023.pdf



MINISTÉRIO DA JUSTIÇA
E SEGURANÇA PÚBLICA

PLANO DIRETOR DE TECNOLOGIA DA INFORMAÇÃO E COMUNICAÇÃO DO MJSP

PDTIC 2021-2023

Ministro de Estado da Justiça e Segurança Pública

André Luiz de Almeida Mendonça

Secretário-Executivo

Tercio Issami Tokano

Secretário-Executivo Adjunto

Washington Leonardo Guanaes Bonini

Diretor de Tecnologia da Informação e Comunicação

Rodrigo Lange

Equipe Responsável pela Elaboração do PDTIC

(Portaria nº 1.162, de 8 de setembro de 2020)

Bárbara Silveira Matsuura
Leonardo Ayodele Cardoso Santos Costa
Cláudio Antônio de Almeida Py
Carlos Alberto dos Santos Silva
Paula Regina Teixeira Lamounier
Thúlio de Andrade Novais Dantas
Rodrigo Barros de Souza
Roberto Domingos Taufick
Caroline Barbosa Muniz
Paula Marques Ferreira
Rodrigo Cesar de Melo
Lany Cristina Silva Brito
Bruno Crescenti de Paiva
Márcio de Freitas Mozini
Victor da Silva Ferreira
Rian Gomes Corrêa
Samantha Almeida Gomes
Fábio Vilela de Albuquerque
Sheila Maria Aguiar de Araújo
Carlos Alberto Jacome Menezes
Maria Cristina Leite
Muller Luiz Borges
Alexandre Rabelo Patury



André Lartigau Wainer
Ana Clara Formiga Ferreira do Carmo
Eduardo de Araújo Nepomuceno
Isabela Maiolino
Bárbara Verônica Dias Mágero Viana
Helena Melo Moura
Miguel Lodi Carvalho
Clayton Rodrigues da Silva
Flávio Soares da Silva
Rafael Rodrigues de Sousa
Rafael Mota Brito
Robinson Lemos
Tiago Nunes Batista
Ivan Fonseca Filho
Débora Ribeiro Lopes
Marcelo Stelmacki
Maximiliano Martins de Faria
Felipe Pires Almeida de Miranda

Colaboradores

Roberto Santos Mendes
Leonardo Bueno de Melo
Gustavo Henrique Moreira Alvares da Silva
Leonardo Garcia Greco
Luís Spricigo Júnior

Aprovadores

Comitê de Governança de Tecnologia da Informação e
Comunicação – CTIC
Comitê de Governança Estratégica – CGE

Reunião de aprovação no CGE: 26 de novembro de 2020

SUMÁRIO

1. APRESENTAÇÃO	7
2. METODOLOGIA	9
3. REFERÊNCIAS.....	11
4. ORGANIZAÇÃO DA ÁREA DE TIC.....	13
5. RESULTADO DO PDTIC ANTERIOR	16
6. REFERENCIAL ESTRATÉGICO	24
7. INVENTÁRIO DAS NECESSIDADES DE TIC	26
8. CRITÉRIOS DE PRIORIZAÇÃO.....	53
9. PLANO DE METAS E AÇÕES	55
10. PLANO DE GESTÃO DE PESSOAS.....	63
10.1 Efetivo Atual.....	63
10.2 Atribuições e Necessidades de Pessoal.....	63
10.3 Processos Críticos com Carência de Servidores	65
10.4 Estimativa da capacidade de execução disponível da TIC. ...	66
10.5 Ações de pessoal em andamento.....	67
10.5.1 Contratação de 35 servidores temporários	67
10.5.2 Mestrado profissionalizante	68
10.5.3 Contratação de serviços de apoio à gestão de dados	68
10.5.4 Plano de Transformação Digital	68
10.6 Necessidades do Arquivo Nacional	69
11. PLANO ORÇAMENTÁRIO	71
12. PLANO DE GESTÃO DE RISCOS	73
12.1 Identificação dos Riscos	73
12.2 Análise dos Riscos	73
12.3 Critérios de Aceitação dos Riscos	74
13. MONITORAMENTO E AVALIAÇÃO DO PLANO.....	78
14. CONCLUSÃO	79

LISTA DE FIGURAS

Figura 1 - Fases de elaboração do PDTIC.....	9
Figura 2 - Estrutura Organizacional do MJSP.....	14
Figura 3 - Estrutura Organizacional da Secretaria-Executiva.....	14
Figura 4 - Estrutura Organizacional da DTIC/SE.....	15
Figura 5 - Necessidades de TIC do PDTIC anterior por Unidade.....	17
Figura 6 - Necessidades de TIC do PDTIC anterior - Alta Prioridade.....	18
Figura 7 - Necessidades de TIC do PDTIC anterior - Média Prioridade.....	19
Figura 8 - Necessidades de TIC do PDTIC anterior concluídas por área	20
Figura 9 - Necessidades de TIC do PDTIC anterior canceladas por área.....	21
Figura 10 - Necessidades de TIC do PDTIC anterior aguardando atendimento.....	22
Figura 11 - Necessidades de TIC do PDTIC anterior sem definição por parte do demandante	23
Figura 12 - Elementos do referencial estratégico delineado.....	25

LISTA DE TABELAS

Tabela 1 - Inventário de Necessidades de TIC	52
Tabela 2 - Critérios de Prioridade	53
Tabela 3 - Critérios de Desempate	53
Tabela 4 - Ações para atendimento das necessidades de TIC	62
Tabela 5 - Quadro de servidores da DTIC	63
Tabela 6 - Quantitativo de servidores temporários a serem contratados	67
Tabela 7 - Perfis dos servidores para execução do Plano de Transformação Digital	69
Tabela 8 - Plano Orçamentário	71
Tabela 9 - Ações vinculadas às áreas de atuação	72
Tabela 10 - Matriz de Probabilidade x Impacto	74
Tabela 11 - Respostas aos Riscos	74
Tabela 12 - Plano de Gestão de Riscos	77

1. APRESENTAÇÃO

O Plano Diretor de Tecnologia da Informação e Comunicação – PDTIC do Ministério da Justiça e Segurança Pública – MJSP, na definição da Instrução Normativa SGD/ME nº 01, de 04 de abril de 2019, Art. 2º, Inciso XXV, é um instrumento de diagnóstico, planejamento e gestão dos recursos e processos de Tecnologia da Informação e Comunicação - TIC que visa atender às necessidades finalísticas e de informação de um órgão ou entidade para um determinado período.

O PDTIC deve se alinhar ao Plano Estratégico de Tecnologia da Informação e Comunicação – PETIC e estabelecer o referencial tático para a execução das ações e projetos de TIC, possibilitando, segundo o Guia de PDTIC do Sistema de Administração dos Recursos de Tecnologia da Informação (SISP), justificar os recursos aplicados em TIC, minimizar o desperdício, garantir o controle, aplicar recursos naquilo que é considerado mais relevante e, por fim, melhorar a qualidade do gasto público e dos serviços prestados à sociedade como um todo.

O PDTIC terá vigência de 01 de janeiro de 2021 a 31 de dezembro de 2023, e revisões serão realizadas ao menos uma vez por ano ou a qualquer momento, diante de mudanças nas referências estratégicas utilizadas (incluindo-se as alterações no Planejamento Estratégico Institucional – PEI).

Por ocasião de tais revisões, poderão ser submetidas ao CTIC eventuais propostas de inclusão de novas necessidades de TIC ou de outras alterações. Excepcionalmente, a critério da DTIC/SE, tais propostas poderão ser submetidas ao referido comitê em data distinta daquelas previstas para as revisões do PDTIC.

Por fim, apresentam-se as unidades do MJSP abrangidas por este PDTIC:

- Gabinete do Ministro – GM;
- Assessoria Especial de Controle Interno – AECI;
- Assessoria Especial de Assuntos Federativos e Parlamentares – AFEPAR;
- Assessoria Especial de Assuntos Legislativos – AEAL;
- Assessoria Especial Internacional – ASINT;
- Secretaria-Executiva – SE;
- Subsecretaria de Administração – SAA;
- Subsecretaria de Planejamento e Orçamento – SPO;

- Diretoria de Tecnologia da Informação e Comunicação – DTIC;
- Consultoria Jurídica – CONJUR;
- Departamento Penitenciário Nacional – DEPEN;
- Secretaria de Gestão e Ensino em Segurança Pública – SEGEN;
- Secretaria Nacional de Justiça – SENAJS;
- Secretaria Nacional de Políticas sobre Drogas – SENAD;
- Secretaria Nacional de Segurança Pública – SENASP;
- Secretaria Nacional do Consumidor – SENACON;
- Secretaria de Operações Integradas – SEOPI; e
- Arquivo Nacional – AN.

Destaque-se que a Polícia Federal, a Polícia Rodoviária Federal, o CADE e a FUNAI possuem unidades de TIC internas e elaboram PDTICs próprios.

Além do planejamento de todas as contratações e aquisições de TIC necessárias ao cumprimento dos objetivos institucionais do MJSP, este documento apresenta um diagnóstico da execução do PDTIC anterior, consolida o inventário de necessidades levantadas para o próximo triênio, prioriza-as e propõe um Plano de Metas e Ações a serem executadas para o seu atendimento.

2. METODOLOGIA

A elaboração do PDTIC 2021-2023 do MJSP baseou-se no modelo proposto pelo Guia de PDTIC do SISP versão 2.0, bem como nas orientações dos órgãos de quanto à observância e recomendações de boas práticas referentes a Gestão e Governança de TIC.

Seguindo as recomendações do Guia do SISP, o processo de elaboração do PDTIC foi dividido em três fases:

- preparação;
- diagnóstico; e
- planejamento.

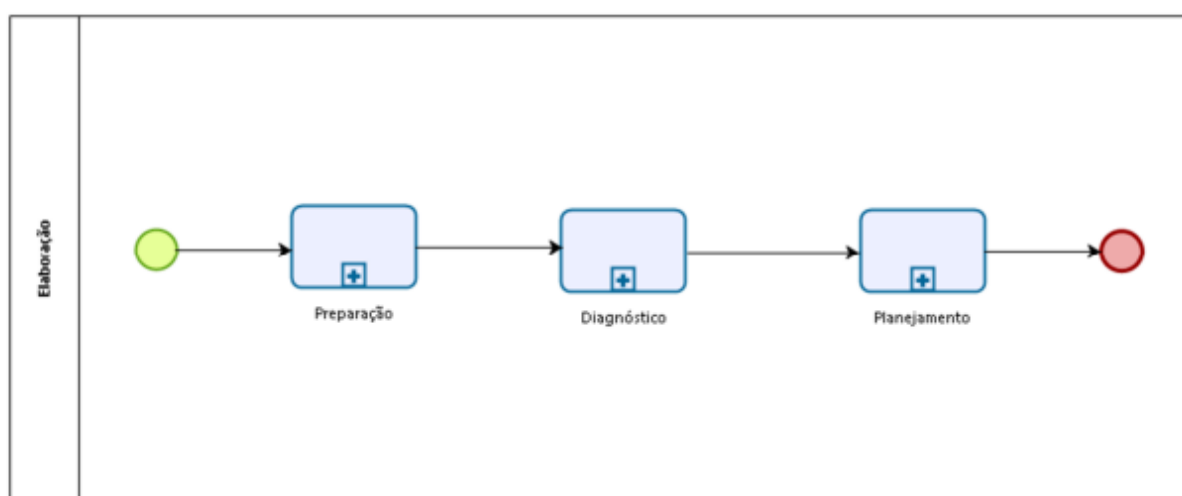


Figura 1 - Fases de elaboração do PDTIC

Na fase de preparação, foi institucionalizada no âmbito do MJSP uma Equipe de Elaboração do PDTIC, com a formação de um Grupo de Trabalho – GT por meio da Portaria SE nº 1.162, de 8 de setembro de 2020. Foram indicados um integrante titular e um substituto para cada unidade integrante do CTIC, que atuaram como pontos focais para o levantamento das necessidades de TIC nas áreas de negócio de suas respectivas unidades organizacionais.

Nessa fase, foram realizadas reuniões com os pontos focais para esclarecer sobre a necessidade de envolvimento de todos no processo de elaboração do PDTIC e orientar quanto à coleta das necessidades de TIC.

Também foram definidas a abrangência e o período do PDTIC, identificados os documentos de referência e estabelecidos os critérios de priorização, bem como os de desempate, devidamente aprovados no Grupo de Trabalho.



A fase de diagnóstico objetivou a compreensão da situação atual da TIC no Ministério por meio da análise das ações previstas no PDTIC anterior e da identificação das necessidades de TIC.

Após o levantamento de tais necessidades e sua consolidação conforme o tipo (contratação ou desenvolvimento interno), foi elaborado um Inventário de Necessidades de TIC priorizado com base nas informações fornecidas por cada Unidade.

Finalmente, na última fase (planejamento), foi possível, com base no diagnóstico realizado na fase anterior, definir as ações de atendimento das demandas alinhadas aos objetivos e indicadores estratégicos contemplados no Plano Estratégico de TIC – PETIC. Além da definição do Plano de Metas e Ações, foi realizado o planejamento das ações de pessoal, o planejamento orçamentário e o planejamento da gestão de riscos.

3. REFERÊNCIAS

- Decreto nº 7579/11, de 11 de outubro de 2011 - Dispõe sobre o Sistema de Administração dos Recursos de Tecnologia da Informação – SISP, do Poder Executivo Federal;
- Portaria nº 778, de 4 de abril de 2019 - Dispõe sobre a implantação da Governança de Tecnologia da Informação e Comunicação nos órgãos e entidades pertencentes ao SISP;
- Portaria SLTI/MP nº 92, de 24 de dezembro de 2014 - Institui a arquitetura ePING (Padrões de Interoperabilidade de Governo Eletrônico) para interoperabilidade de serviços de Governo Eletrônico;
- Resolução CGE nº 4, de 18 de julho de 2018 - Aprova o Manual de Gerenciamento de Riscos e Controles Internos no âmbito do Ministério da Justiça;
- Decreto nº 9.507, de 21 de setembro de 2018 - Dispõe sobre a execução indireta de serviços da administração pública federal;
- Decreto nº 9.637, de 26 de dezembro de 2018 - Institui a Política Nacional de Segurança da Informação e dispõe sobre a governança da segurança da informação;
- Instrução Normativa – IN nº 01, de 04 de abril de 2019 – SGD/ME - Dispõe sobre o processo de contratação de soluções de TIC pelos órgãos e entidades integrantes do SISP;
- Decreto nº 9.854, de 25 de junho de 2019 - Institui o Plano Nacional de Internet das Coisas;
- Portaria nº 895, de 19 de dezembro de 2019 - Aprova o Planejamento Estratégico do Ministério da Justiça e Segurança Pública 2020-2023;
- Resolução CGE nº 9, de 10 de março de 2020 – Altera o conteúdo do Planejamento Estratégico 2020-2023;
- Resolução CGE nº 10, de 25 de agosto de 2020 – Altera o conteúdo de indicadores, metas e projetos estratégicos do Planejamento Estratégico 2020-2023;

- Portaria nº 86, de 23 de março de 2020 - Institui o Sistema de Governança do Ministério da Justiça e Segurança Pública e da Fundação Nacional do Índio;
- Decreto nº 10.332, de 28 de abril de 2020 - Institui a Estratégia de Governo Digital para o período de 2020 a 2022, no âmbito dos órgãos e das entidades da administração pública federal;
- Plano de Transformação Digital do Ministério da Justiça e Segurança Pública (MJSP) - Plano pactuado entre o MJSP, SEME/SG-PR e SGD/ME, visando oferecer maior facilidade e simplificação para o acesso, a solicitação e o acompanhamento de serviços ao cidadão;
- Guia de PDTIC do SISP versão 2.0 - Dispõe sobre os padrões, orientações, diretrizes e modelos para elaboração do Plano Diretor de TIC;
- *Control Objectives for Information and Related Technology* (COBIT 2019) - Fornece um modelo abrangente que auxilia as organizações a atingirem seus objetivos de governança e gestão de TIC;
- *Project Management Body of Knowledge* (PMBOK) 6ª edição - Guia com modernas práticas de gerenciamento de projetos; e
- *Information Technology Infrastructure Library* (ITIL V3) - Conjunto de boas práticas a serem aplicadas na infraestrutura, operação e manutenção de serviços de tecnologia da informação.

4. ORGANIZAÇÃO DA ÁREA DE TIC

No âmbito do Ministério da Justiça e Segurança Pública e de suas entidades vinculadas, a Diretoria de Tecnologia da Informação e Comunicação da Secretaria-Executiva – DTIC/SE exerce o papel de órgão setorial do Sistema de Administração dos Recursos de Tecnologia da Informação – SISP¹. Suas competências estão definidas no Art. 11 do Anexo I do Decreto nº 9.662, de 1º de janeiro de 2019:

I - planejar, coordenar e supervisionar a execução das atividades relacionadas com o Sistema de Administração dos Recursos de Tecnologia da Informação no âmbito do Ministério;

II - promover a articulação com os órgãos centrais do sistema federal referido no inciso I e informar e orientar os órgãos integrantes da estrutura do Ministério e da entidade a ele vinculada quanto ao cumprimento das normas estabelecidas;

III - elaborar e consolidar os planos e os programas das atividades de sua área de competência e submetê-los à decisão superior; e

IV - acompanhar e promover a avaliação de projetos e atividades, no âmbito de sua competência.

Assim, cabe à DTIC/SE acompanhar, cumprir e assegurar a aplicação das normas emanadas do SISP, incluindo-se a elaboração do PDTIC para as unidades do MJSP elencadas no Capítulo 1 - APRESENTAÇÃO (a Polícia Federal, a Polícia Rodoviária Federal, o CADE e a FUNAI possuem unidades de TIC internas e elaboram PDTICS próprios).

Como área de TIC, é responsabilidade da DTIC/SE organizar, manter e fornecer os serviços e recursos de TIC, bem como desenvolver, implementar, documentar e manter sistemas de informação, visando atender às necessidades das demais áreas do MJSP.

Na Figura 2 a seguir, é possível identificar a posição da Secretaria-Executiva na estrutura organizacional do Ministério, à qual a DTIC/SE está diretamente subordinada.

¹ Portaria SE/MJSP nº 77, de 17 de janeiro de 2020, Art. 4º, Inciso VII



Figura 2 - Estrutura Organizacional do MJSP

O posicionamento da DTIC/SE na estrutura da Secretaria-Executiva, por sua vez, está representado na Figura 3 a seguir.

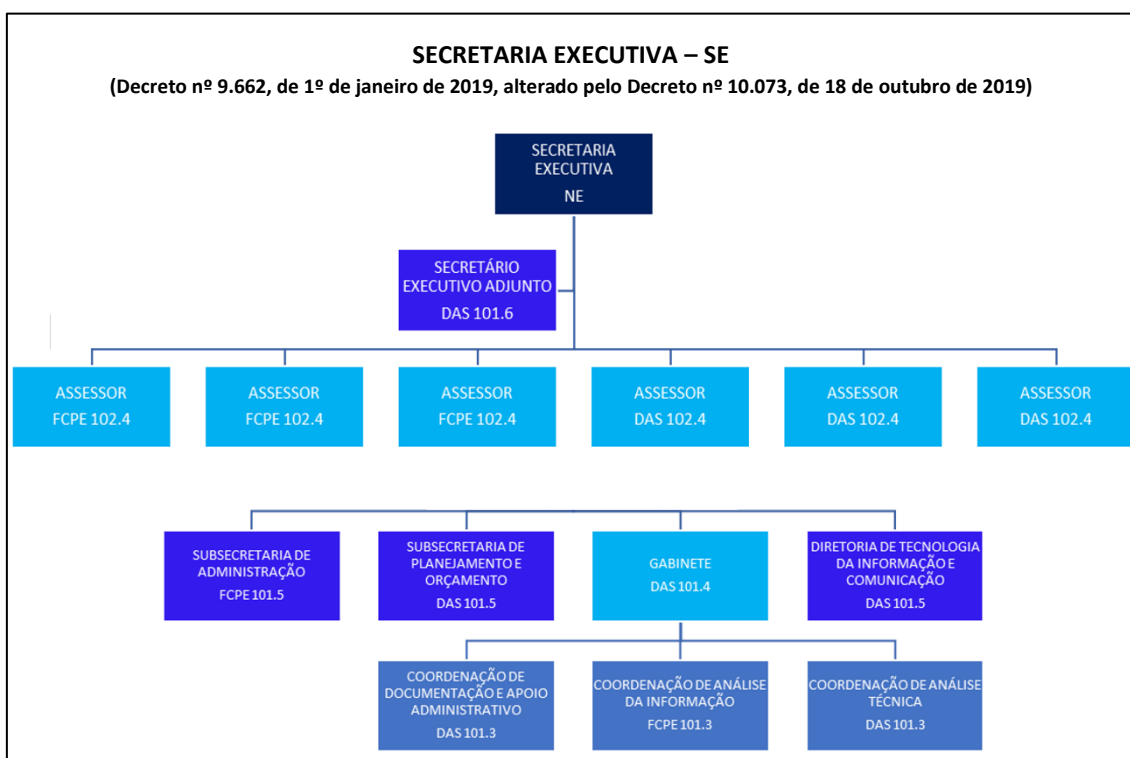


Figura 3 - Estrutura Organizacional da Secretaria-Executiva

E, por fim, a Figura 4 abaixo apresenta a estrutura organizacional interna da DTIC/SE.

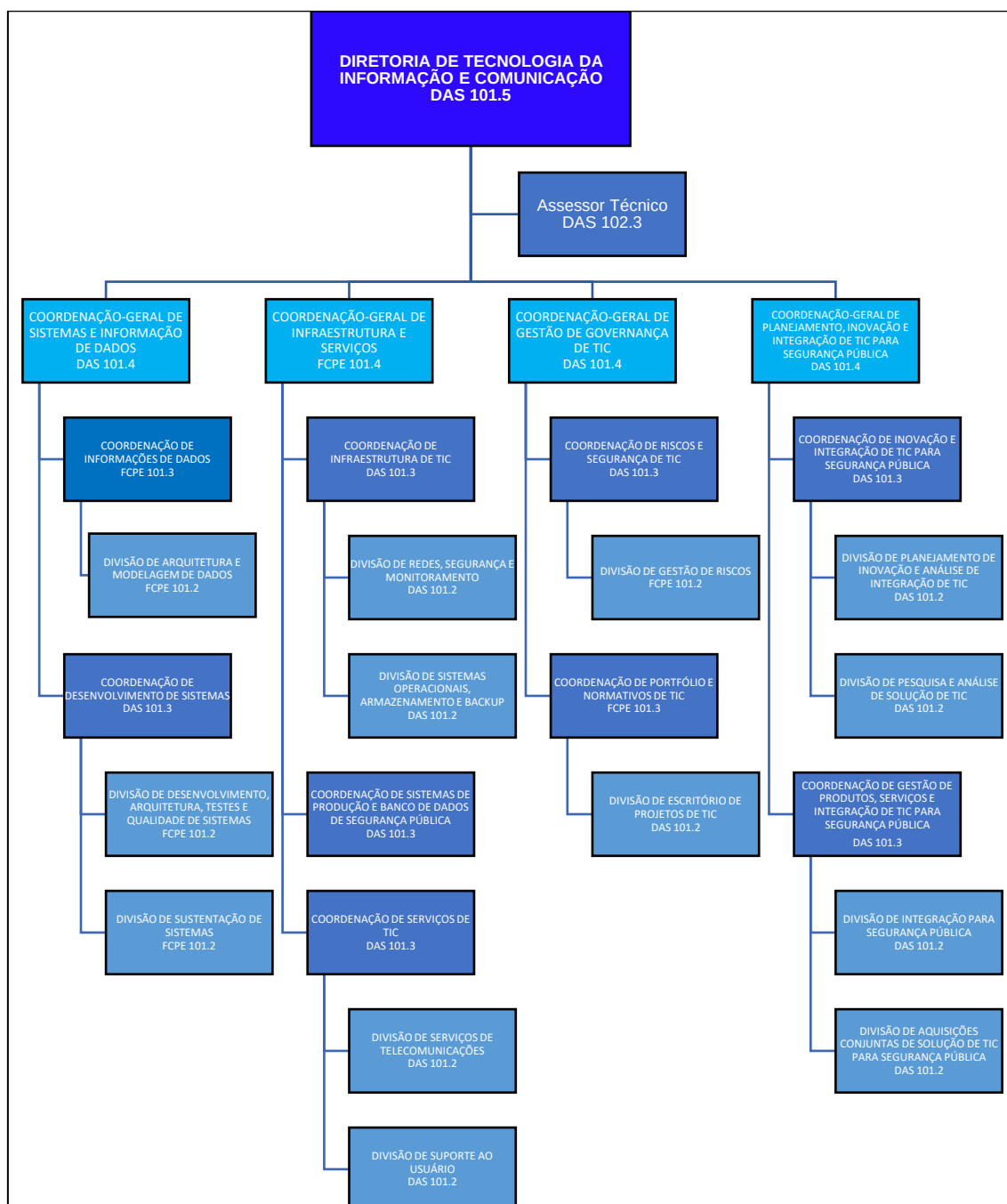


Figura 4 - Estrutura Organizacional da DTIC/SE

As atribuições da DTIC/SE e de suas unidades internas estão sendo definidas no processo de elaboração do novo Regimento Interno do MJSP.

5. RESULTADO DO PDTIC ANTERIOR

Na última revisão do PDTIC 2017-2020, foram levantadas 578 (quinhentos e setenta e oito) necessidades de TIC junto às Unidades do MJSP.

Os resultados do PDTIC anterior são demonstrados nos gráficos abaixo

Ressalta-se que, em vista da necessidade de aprovação deste PDTIC antes do término do período de vigência do plano anterior, as informações referem-se à execução ocorrida até o mês de outubro de 2020. Os resultados definitivos e completos envolvendo todo o exercício de 2020 serão contemplados na próxima revisão deste PDTIC.

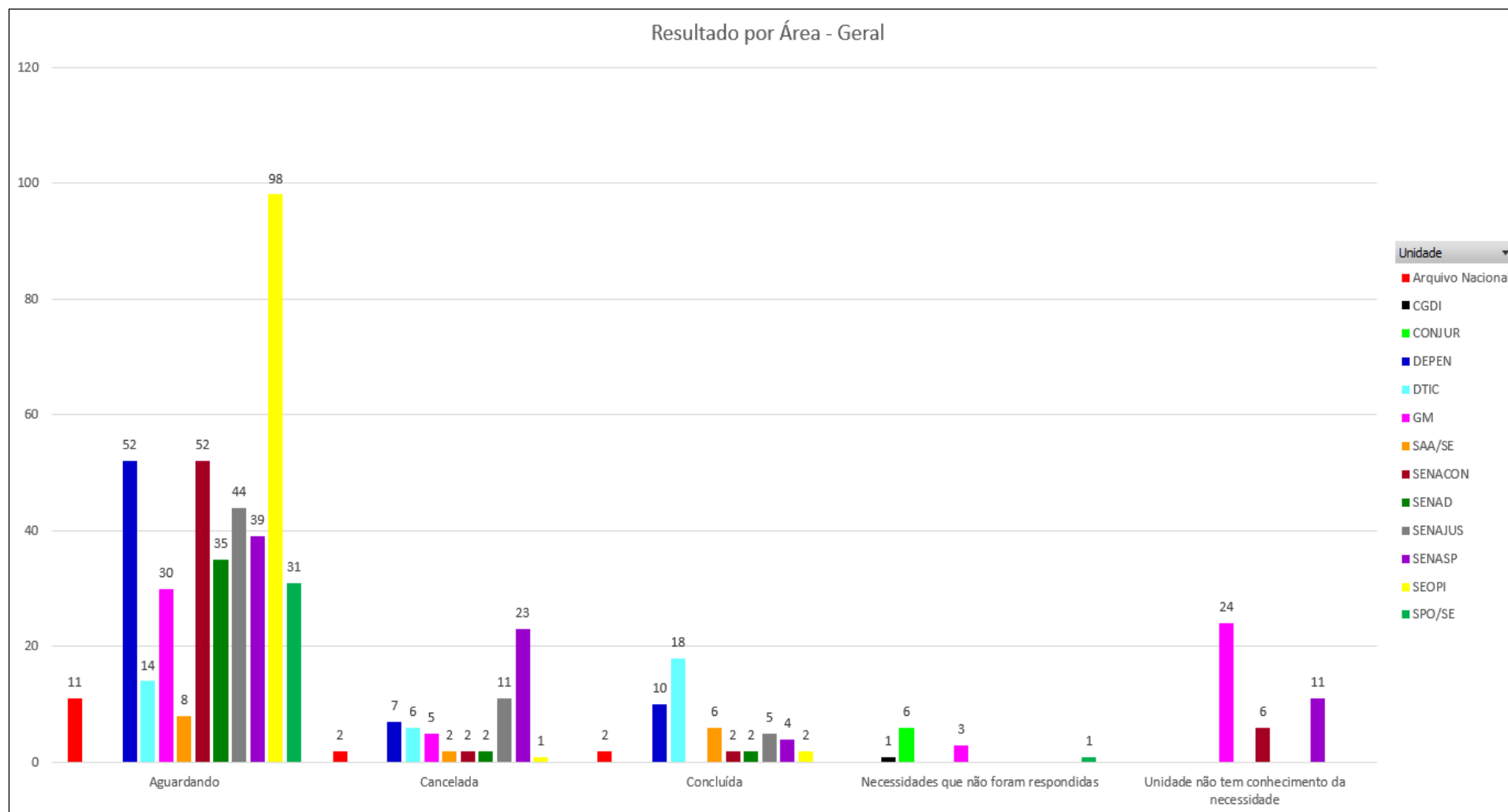


Figura 5 - Necessidades de TIC do PDTIC anterior por Unidade

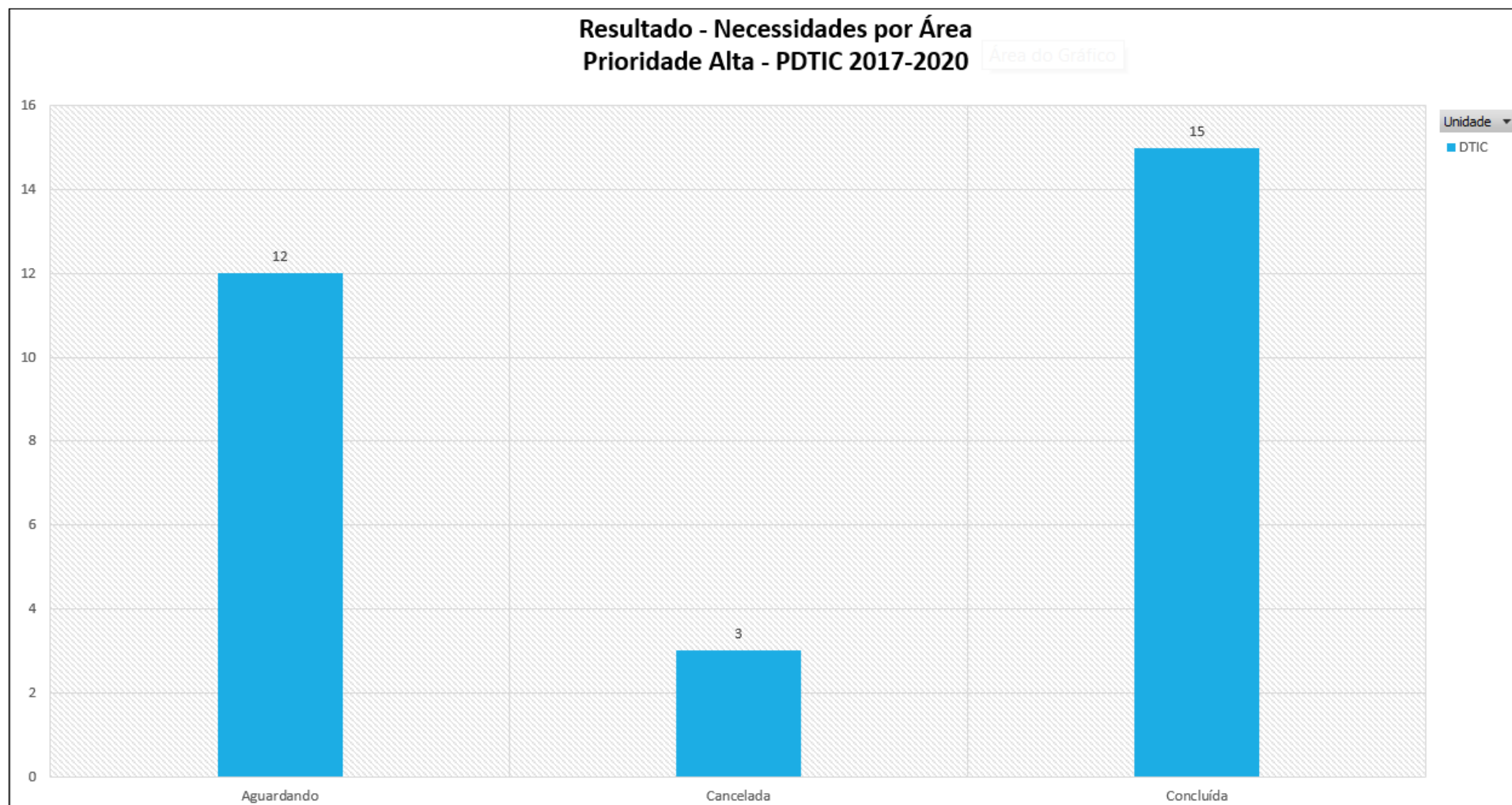


Figura 6 - Necessidades de TIC do PDTIC anterior - Alta Prioridade

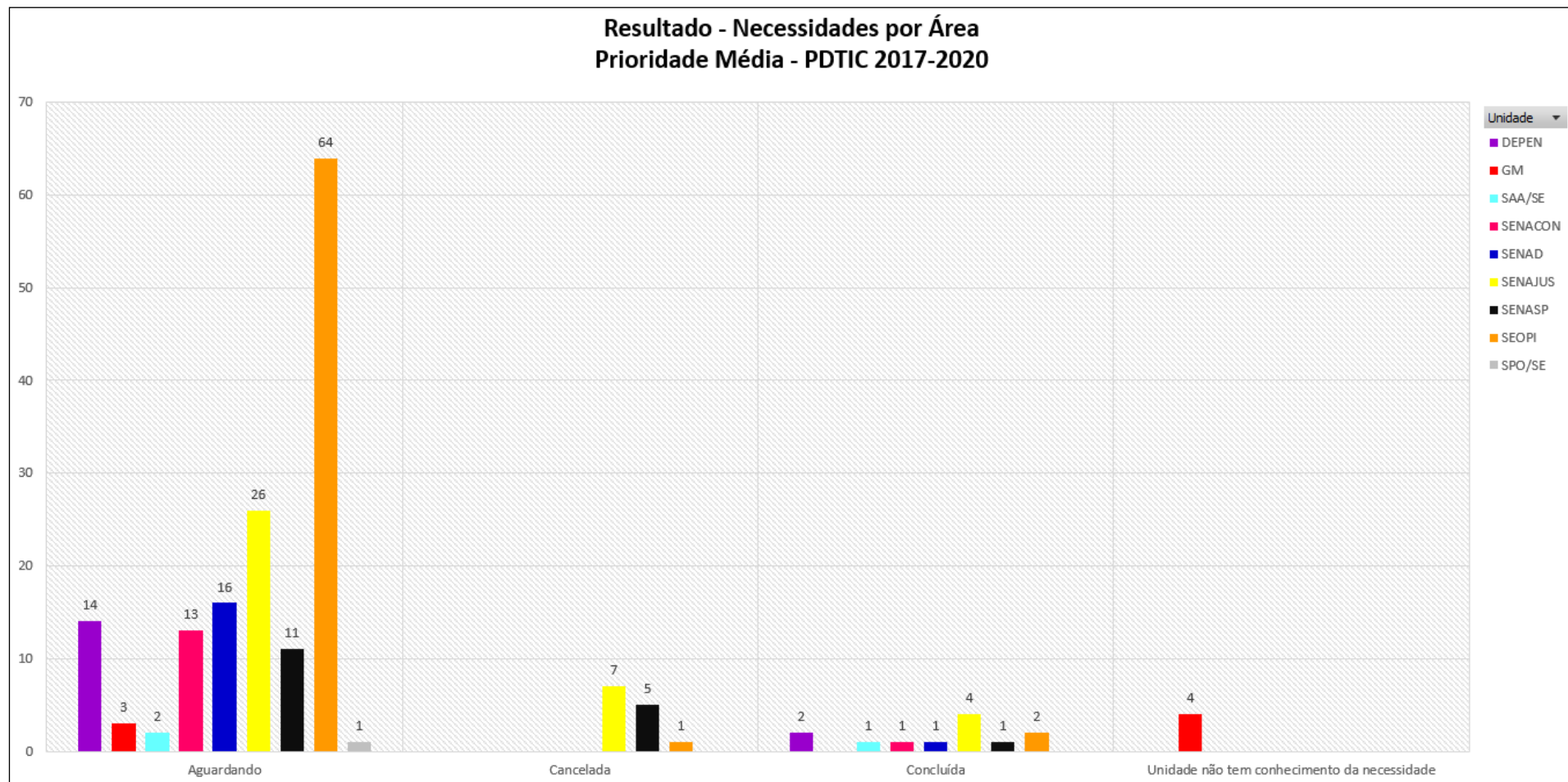


Figura 7 - Necessidades de TIC do PDTIC anterior - Média Prioridade

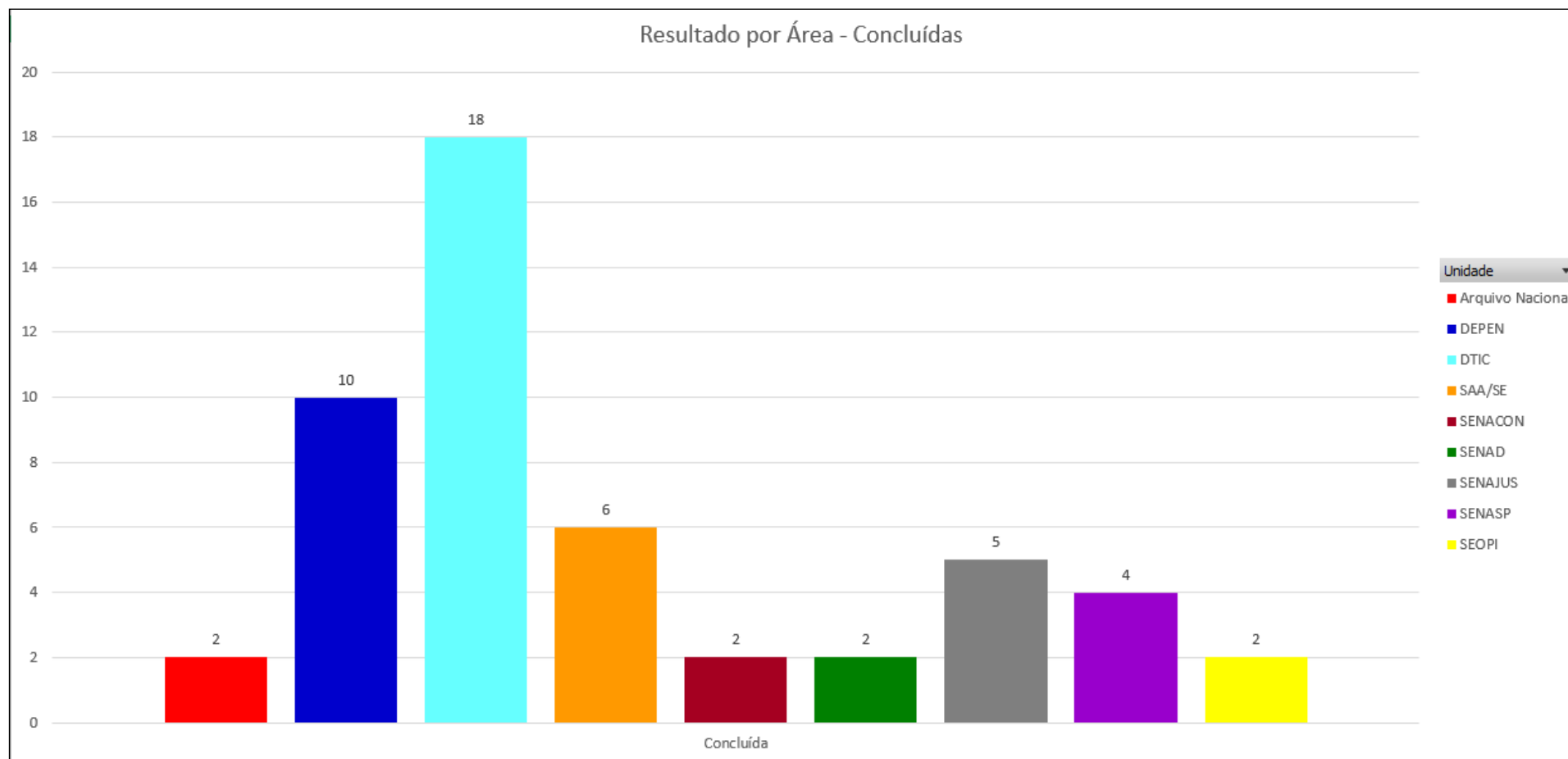


Figura 8 - Necessidades de TIC do PDTIC anterior concluídas por área

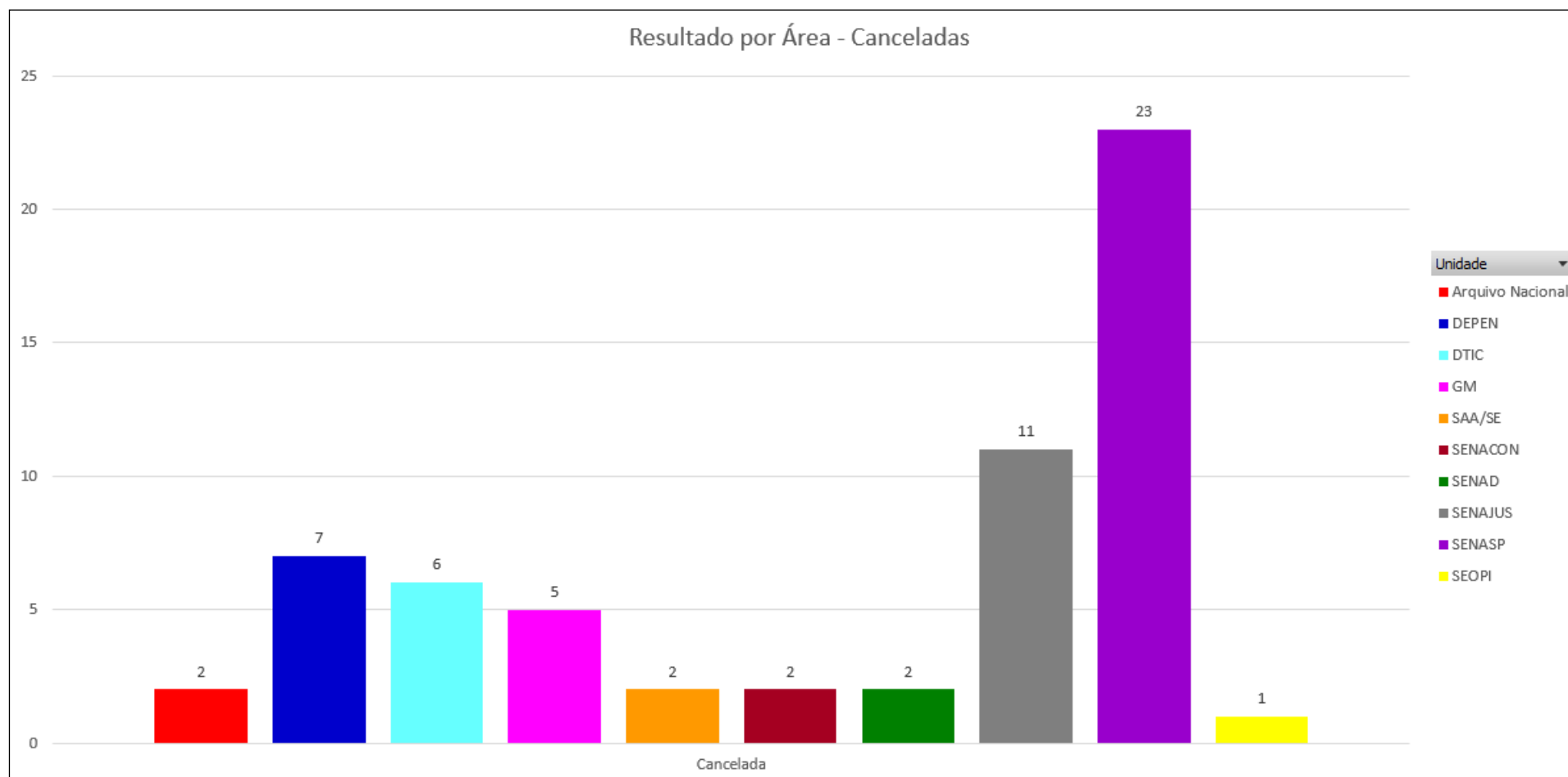


Figura 9 - Necessidades de TIC do PDTIC anterior canceladas por área

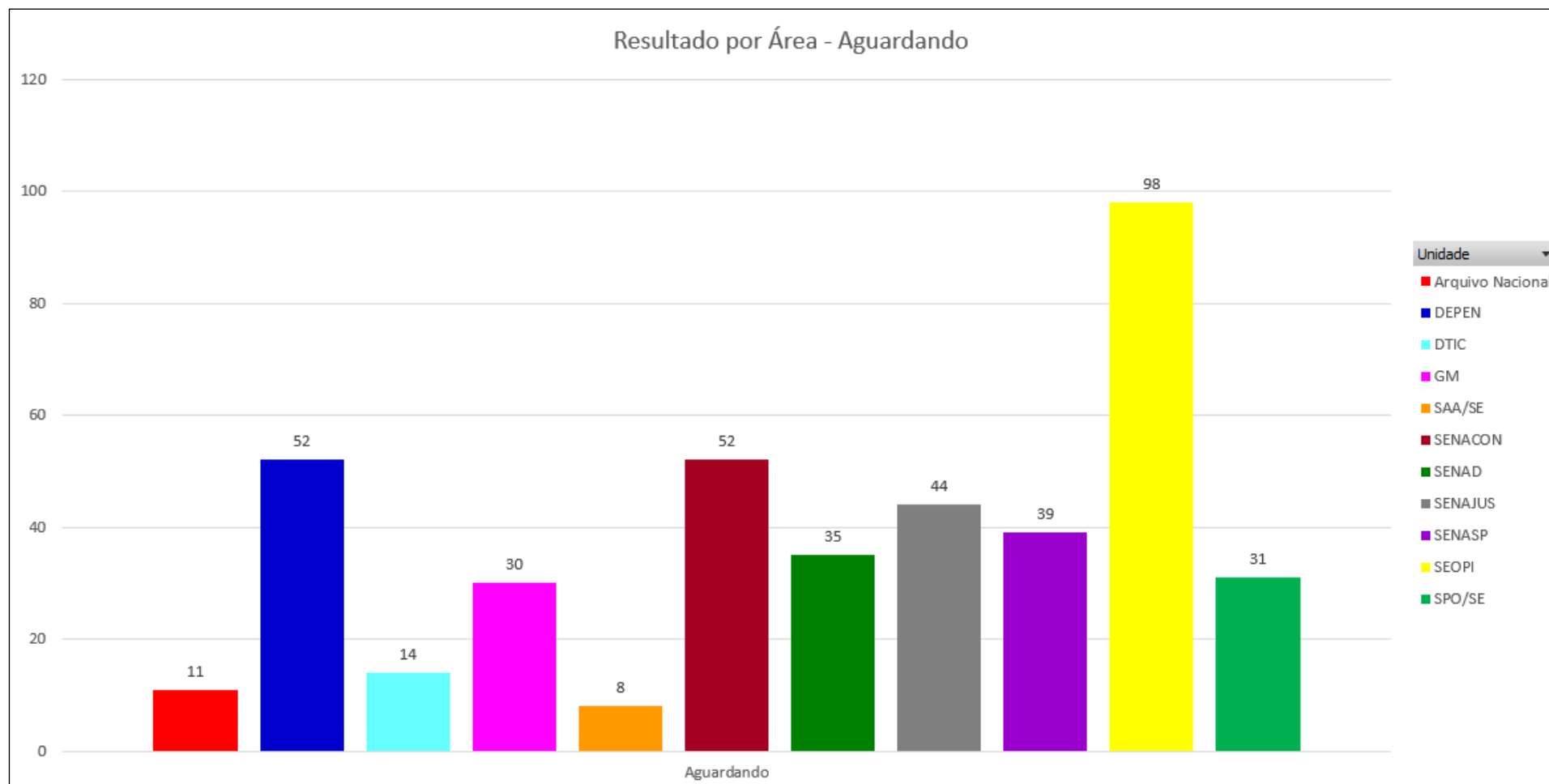


Figura 10 - Necessidades de TIC do PDTIC anterior aguardando atendimento

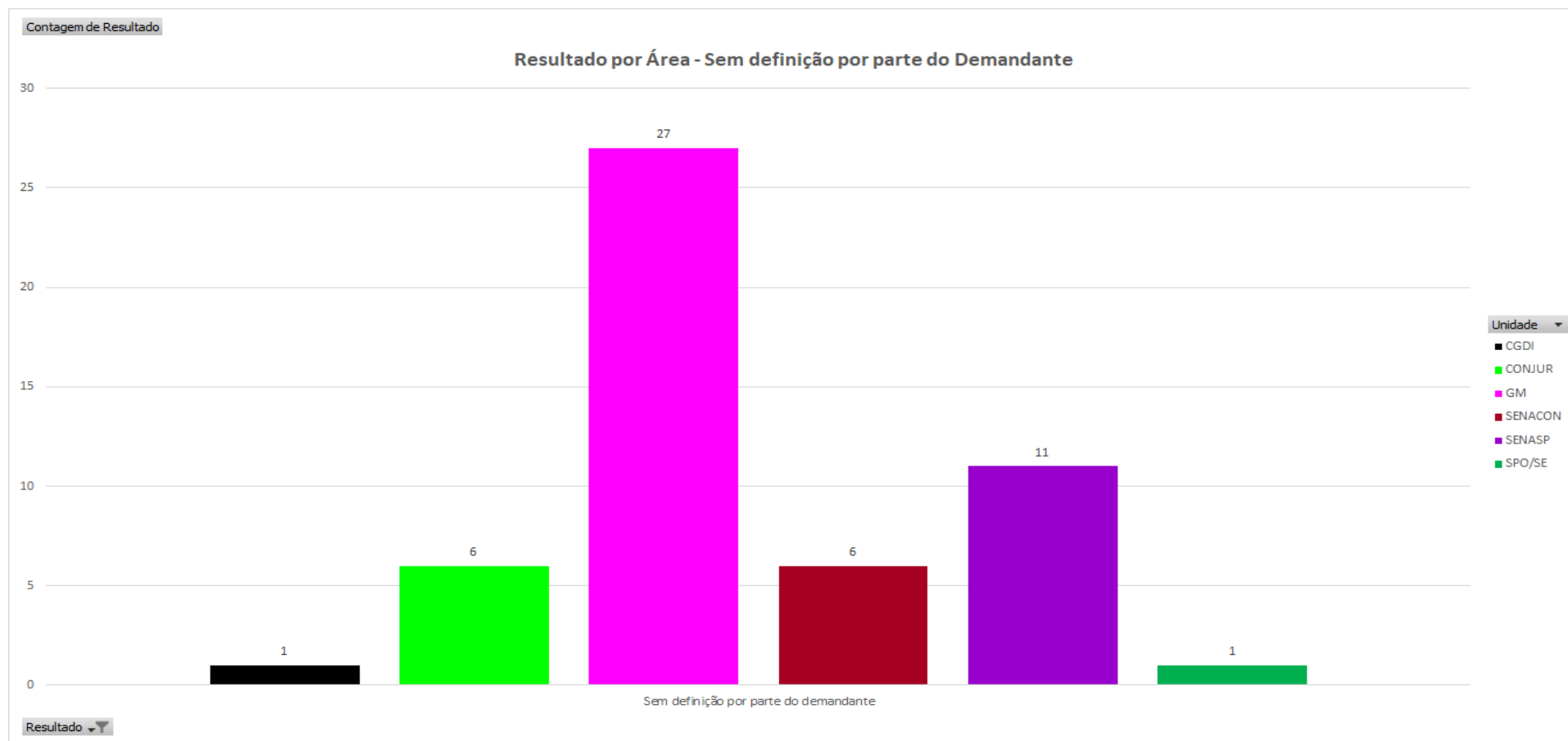


Figura 11 - Necessidades de TIC do PDTIC anterior sem definição por parte do demandante

6. REFERENCIAL ESTRATÉGICO

No âmbito do MJSP, o referencial estratégico da área de Tecnologia da Informação e Comunicação é construído no Plano Estratégico de Tecnologia da Informação e Comunicação – PETIC 2021-2023.

No PETIC, estão elencados os artefatos estratégicos de TIC (princípios e diretrizes, missão, visão, valores, análise SWOT, mapa estratégico, objetivos e indicadores estratégicos), bem como são descritas suas principais fontes direcionadoras, com destaque para o Plano Estratégico Institucional - PEI e a Estratégia de Governo Digital - EGD.

Aqui, portanto, cabe demonstrar o alinhamento do PDTIC ao PETIC, do qual decorrerão sua coerência, compatibilidade e alinhamento com a estratégia organizacional, o modelo de negócio e os objetivos de negócio.

Inicialmente, cabe destacar que, a partir da análise SWOT, foram incluídas no Inventário de Necessidades de TIC demandas específicas para aproveitar oportunidades de melhoria e a mitigação de ameaças.

Outro esforço de alinhamento está no estabelecimento dos critérios de priorização para o atendimento das necessidades de TIC (Capítulo 8), que atribuem maior peso àquelas vinculadas aos projetos estratégicos do MJSP. Os princípios, valores e diretrizes estratégicas também estão devidamente contemplados nos demais critérios que privilegiam a conformidade (atendimento de exigência legal e previsão no PAC), a eficiência (transversalidade da necessidade), eficácia (viabilidade assegurada pela previsão no PAC) e a transformação digital (vinculação ao Plano Digital).

Assim, neste PDTIC fazem-se presentes elementos do Plano Estratégico do Ministério – PEI, da Estratégia de Governança Digital - EGD, do Plano de Transformação Digital do MJSP, da Lei Geral de Proteção de Dados Pessoais – LGPD e de outras referências adotadas pelo PETIC. A Figura 12 a seguir representa os principais elementos do referencial estratégico delineado para o estabelecimento de um plano tático de TIC deste Ministério.

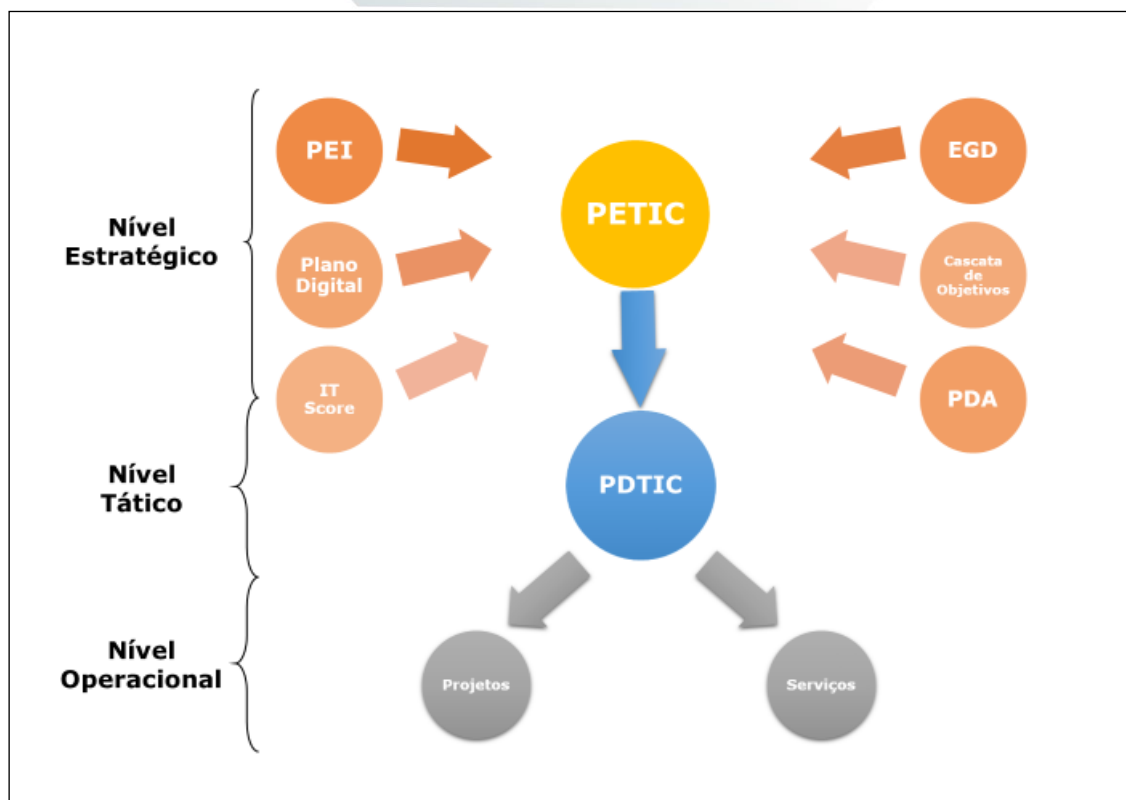


Figura 12 - Elementos do referencial estratégico delineado

7. INVENTÁRIO DAS NECESSIDADES DE TIC

Priorização	Código	Unidade	Área	Objetivo Estratégico	Projeto Estratégico	Tipo	Subtipo	Descrição	Qtd
1	N0572	SEGEN	DIGES	OE03	PE1U	Desenvolvimento Interno	Desenvolvimento de novo sistema de informação ou aplicativo móvel	Solução para gerenciar os processos licitatórios	1
2	N0275	SE/SAA	CGGP	OE09	N/D	Desenvolvimento Interno	Outros serviços de provimento de solução de TIC	Implantação de sistema informatizado para o Programa de Gestão	1
3	N0414	SEGEN	DIGES	OE10	N/D	Desenvolvimento Interno	Desenvolvimento de novo sistema de informação ou aplicativo móvel	Sistema de gestão das transferências Fundo a Fundo (FaF)	1
4	N0529	SEGEN	DIGES	OE10	N/D	Desenvolvimento Interno	Desenvolvimento de novo sistema de informação ou aplicativo móvel	Sistema de Gestão de Convênios e Contratos de Repasse	1
5	N0160	SENASP	DGI	OE03	PE97	Desenvolvimento Interno	Provimento de solução de análise técnica e gerencial de dados	SINESP Big Data - desenvolvimento	1
6	N0161	SENASP	DGI	OE03	PE97	Contratação	Sistema de Informação comercial	SINESP Infoseg - desenvolvimento	1
7	N0162	SENASP	DGI	OE03	PE97	Desenvolvimento Interno	Desenvolvimento de novo sistema de informação ou aplicativo móvel	SINESP OCR	1

Priorização	Código	Unidade	Área	Objetivo Estratégico	Projeto Estratégico	Tipo	Subtipo	Descrição	Qtd
8	N0163	SENASP	DGI	OE03	PE97	Contratação	Serviços de TIC	SINESP Big Data - nuvem privada	1
9	N0164	SENASP	DGI	OE03	PE97	Desenvolvimento Interno	Provimento de solução de análise técnica e gerencial de dados	Portal SINESP	1
10	N0165	SENASP	DGI	OE03	PE97	Desenvolvimento Interno	Provimento de solução de análise técnica e gerencial de dados	SINESP DW Análise	1
11	N0167	SENASP	DGI	OE03	PE97	Contratação	Serviços de TIC	SINESP Infoseg – Módulos Remotos e links MPLS	1
12	N0168	SENASP	DGI	OE03	PE97	Desenvolvimento Interno	Outros serviços de provimento de solução de TIC	SINESP - Replicação da base de dados	1
13	N0176	SENASP	DGI	OE03	PE97	Contratação	Sistema de Informação comercial	SINESP Segurança	1
14	N0177	SENASP	DGI	OE03	PE97	Desenvolvimento Interno	Desenvolvimento de novo sistema de informação ou aplicativo móvel	SINESP Auditoria	1
15	N0185	SENASP	DGI	OE03	PE97	Desenvolvimento Interno	Desenvolvimento de novo sistema de informação ou aplicativo móvel	SINESP Agente de Campo	1

Priorização	Código	Unidade	Área	Objetivo Estratégico	Projeto Estratégico	Tipo	Subtipo	Descrição	Qtd
16	N0193	SENASP	DGI	OE03	PE97	Contratação	Sistema de Informação comercial	SINESP CAD	1
17	N0247	SENASP	DGI	OE03	PE97	Contratação	Serviços de TIC	Central de atendimento 24/7 ao usuário dos sistemas do SINESP	1
18	N0263	SE/DTIC	CGGOV	OE11	N/D	Contratação	Licença e uso de software	Ferramentas de avaliação de vulnerabilidades em ativos	9000
19	N0264	SE/DTIC	CGGOV	OE11	N/D	Contratação	Serviços de TIC	Contratação de Serviço de Centro de Operações de Segurança	1
20	N0267	SE/DTIC	CGGOV	OE11	N/D	Contratação	Licença e uso de software	Contratação de ferramenta de auditoria e análise de logs de SIC	1
21	N0350	SE/SAA	CGGP	OE09	N/D	Contratação	Serviços de TIC	Serviço de suporte técnico ao sistema eletrônico de ponto REP	1
22	N0358	SENAJUS	DPIJUS	OE02	PE77	Contratação	Licença e uso de software	Licença para uso do Microsoft BI (Business Intelligence)	4
23	N0373	SENAJUS	DPIJUS	OE02	PE77	Contratação	Licença e uso de software	Licença para uso do Microsoft BI (Business Intelligence)	4
24	N0202	SE/DTIC	CGISP	OE11	N/D	Contratação	Serviços de TIC	Central de atendimento 24/7 ao usuário dos sistemas do MJSP	1
25	N0210	SE/DTIC	CGSID	OE11	N/D	Contratação	Serviços de TIC	Fábrica de Software para desenvolvimento e sustentação de sistemas	1
26	N0007	SE/DTIC	CGGOV	OE11	N/D	Contratação	Serviços de TIC	Modelo de Governança de TIC no MJSP	1
27	N0008	SE/DTIC	CGGOV	OE11	N/D	Contratação	Capacitação	Curso de Mestrado Profissional em Ciência de Dados e Segurança da Informação por meio de TED com a UnB	1

Priorização	Código	Unidade	Área	Objetivo Estratégico	Projeto Estratégico	Tipo	Subtipo	Descrição	Qtd
28	N0157	DEPEN	DIPEN	OE04	PE1D	Desenvolvimento Interno	Outros serviços de provimento de solução de TIC	Sistema de coleta de informações prisionais	1
29*	N0197	SENASP	DGI	OE03	PE97	Desenvolvimento Interno	Desenvolvimento de novo sistema de informação ou aplicativo móvel	Sistema de Identidades Funcionais Digital	1
30	N0290	SENAJUS	DEMIG	OE02	PE73	Contratação	Equipamentos de TIC	Aquisição de Webcams	20
31	N0409	DEPEN	DIREX	OE04	PE1B	Desenvolvimento Interno	Desenvolvimento de novo sistema de informação ou aplicativo móvel	Sistema de monitoramento das obras prisionais	1
32	N0248	SE/DTIC	CGGOV	OE11	N/D	Desenvolvimento Interno	Outros serviços de provimento de solução de TIC	Normativos de Segurança da Informação e Comunicação	15
33	N0249	SE/DTIC	CGGOV	OE11	N/D	Desenvolvimento Interno	Outros serviços de provimento de solução de TIC	Conscientização de Segurança da Informação e Comunicação	1
34	N0250	SE/DTIC	CGGOV	OE11	N/D	Desenvolvimento Interno	Outros serviços de provimento de solução de TIC	Gestão de Ativos de TIC	1
35	N0252	SE/DTIC	CGGOV	OE11	N/D	Desenvolvimento Interno	Outros serviços de provimento de solução de TIC	Serviços de Segurança da Informação e Comunicação	1
36	N0253	SE/DTIC	CGGOV	OE11	N/D	Desenvolvimento Interno	Outros serviços de provimento de solução de TIC	Análise de segurança de sistemas informatizados	1

Priorização	Código	Unidade	Área	Objetivo Estratégico	Projeto Estratégico	Tipo	Subtipo	Descrição	Qtd
37	N0254	SE/DTIC	CGGOV	OE11	N/D	Desenvolvimento Interno	Outros serviços de provimento de solução de TIC	Mitigação de vulnerabilidades dos sistemas do MJSP	1
38	N0256	SE/DTIC	CGGOV	OE11	N/D	Desenvolvimento Interno	Outros serviços de provimento de solução de TIC	Realização de testes de segurança nos sistemas do MJSP	1
39	N0270	SE/DTIC	CGGOV	OE11	N/D	Contratação	Licença e uso de software	Ferramenta para classificação e monitoramento de dados sensíveis, incidentes de segurança e alerta em tempo real	1
40	N0510	SE/SAA	CGDS	N/D	N/D	Desenvolvimento Interno	Outros serviços de provimento de solução de TIC	SEI - Atualizações do Módulo de Pesquisa Pública	1
41	N0530	SEGEN	DIGES	OE09	N/D	Desenvolvimento Interno	Desenvolvimento de novo sistema de informação ou aplicativo móvel	Sistema de Gestão e Controle de Efetivo	1
42	N0555	SEGEN	DIGES	OE10	N/D	Desenvolvimento Interno	Provimento de solução de análise técnica e gerencial de dados	Desenvolvimento de API para acesso a Base de Dados do Sistema Gestão Ágil do Banco do Brasil	1
43	N0564	SEGEN	DIGES	OE10	N/D	Desenvolvimento Interno	Provimento de solução de análise técnica e gerencial de dados	Painel BI de Transferências Voluntárias e Obrigatórias	1
44	N0013	SEGEN	DEP	OE01	N/D	Contratação	Sistema de Informação comercial	Desenvolvimento de recursos para e-learning interativo	1

Priorização	Código	Unidade	Área	Objetivo Estratégico	Projeto Estratégico	Tipo	Subtipo	Descrição	Qtd
45	N0513	SE/SAA	CGDS	N/D	N/D	Desenvolvimento Interno	Outros serviços de provimento de solução de TIC	SEI - Implantação do Módulo de Gestão Documental	1
46	N0178	SENASP	DGI	OE03	PE97	Contratação	Sistema de Informação comercial	SINESP Integração	1
47	N0180	SENASP	DGI	OE03	PE97	Contratação	Serviços de TIC	Rede SINESP	1
48	N0186	SENASP	DGI	OE03	PE97	Contratação	Sistema de Informação comercial	Sistema de gestão de frota veicular	1
49	N0188	SENASP	DGI	OE03	PE97	Desenvolvimento Interno	Desenvolvimento de novo sistema de informação ou aplicativo móvel	Solução de Gestão de logística de operações, suprimentos, transporte	1
50	N0280	SE/SAA	CGGP	OE09	PE64	Desenvolvimento Interno	Desenvolvimento de novo sistema de informação ou aplicativo móvel	Sistema Competências	1
51	N0384	SENAICON	CGPFF	OE06	PE87	Contratação	Capacitação	Capacitação	16
52	N0390	SE/GAB SE	CODAP	OE09	PE64	Contratação	Equipamentos de TIC	Notebook	1
53	N0398	SE/GAB SE	COAT	OE09	PE64	Contratação	Equipamentos de TIC	Notebook	3
54	N0401	SE/GAB SE	COAT	OE09	PE64	Contratação	Equipamentos de TIC	Equipamento de videoconferência	3

Priorização	Código	Unidade	Área	Objetivo Estratégico	Projeto Estratégico	Tipo	Subtipo	Descrição	Qtd
55	N0429	SE/DTIC	CGISE	OE01	PE95	Contratação	Equipamentos de TIC	Equipamentos de infraestrutura hiperconvergente	20
56	N0435	SE/DTIC	CGISE	OE03	PE97	Contratação	Serviços de TIC	Contratação de subscrição de softwares da empresa Red Hat	1000
57	N0436	SE/DTIC	CGISE	OE01	PE81	Contratação	Serviços de TIC	Contratação de suporte Microsoft Premier	250
58	N0448	SE/DTIC	CGISE	OE01	PE81	Contratação	Serviços de TIC	Renovação do licenciamento e suporte para a solução de backup corporativo da DTIC	8
59	N0451	SE/DTIC	CGISE	OE01	PE81	Contratação	Serviços de TIC	Contratação de certificado digital wildcard	1
60	N0173	SENASP	DGI	OE03	PE97	Desenvolvimento Interno	Outros serviços de provimento de solução de TIC	Internalização do SINESP	1
61	N0175	SENASP	DGI	OE03	PE97	Contratação	Sistema de Informação comercial	SINESP PPE - Sistema de Boletim Eletrônico	1
62	N0179	SENASP	DGI	OE03	PE97	Desenvolvimento Interno	Desenvolvimento de novo sistema de informação ou aplicativo móvel	SINESP Cidadão	1
63	N0181	SENASP	DGI	OE03	PE97	Desenvolvimento Interno	Desenvolvimento de novo sistema de informação ou aplicativo móvel	SINESP Perícia	1
64	N0182	SENASP	DGI	OE03	PE97	Contratação	Serviços de TIC	SINESP Delegacia Virtual	1

Priorização	Código	Unidade	Área	Objetivo Estratégico	Projeto Estratégico	Tipo	Subtipo	Descrição	Qtd
65	N0183	SENASP	DGI	OE03	PE97	Desenvolvimento Interno	Evolução/melhoria de sistema de informação ou aplicativo móvel já existente	SINESP SAIE	1
66	N0184	SENASP	DGI	OE03	PE97	Desenvolvimento Interno	Desenvolvimento de novo sistema de informação ou aplicativo móvel	SINESP VDE	1
67	N0192	SENASP	DGI	OE03	PE97	Contratação	Serviços de TIC	SINESP - sustentação	1
68	N0271	SENACON	DPDC	OE06	PE50	Desenvolvimento Interno	Outros serviços de provimento de solução de TIC	Sistema de recall	0
69	N0005	AN	COAD	OE08	PE43	Desenvolvimento Interno	Desenvolvimento de novo sistema de informação ou aplicativo móvel	Sistema de Gestão de Documentos de Arquivo da Administração Pública Federal - SIGA	1
70	N0006	AN	COAD	OE08	PE1	Desenvolvimento Interno	Desenvolvimento de novo sistema de informação ou aplicativo móvel	Aperfeiçoamento do Sistema Nacional de Informações do Arquivo Nacional - SIAN	1
71	N0158	SENACON	CNCP	OE06	N/D	Desenvolvimento Interno	Desenvolvimento de novo sistema de informação ou aplicativo móvel	Criação de um Canal de Denúncias do CNCP	1
72	N0208	SE/DTIC	CGSID	OE11	N/D	Contratação	Soluções de análise técnica e gerencial de dados (analytics)	Contratação de serviços especializados para dados, BI,	1

Priorização	Código	Unidade	Área	Objetivo Estratégico	Projeto Estratégico	Tipo	Subtipo	Descrição	Qtd
								ciência de dados, big data e governança de dados	
73	N0288	SENACON	CGARI	OE06	N/D	Contratação	Equipamentos de TIC	Contratação de computadores e impressoras	400
74	N0010	SEGEN	DEP	OE01	N/D	Contratação	Licença e uso de software	Licença de software de análise de similaridade textual	1
75	N0309	SENAJUS	DPJUS	OE02	PE70	Contratação	Sistema de Informação comercial	Plataforma Online Resoluto	467
76	N0351	SENAJUS	DRCI	OE01	PE75	Contratação	Serviços de TIC	Infraestrutura e serviços de nuvem para a Rede-Lab	1
77	N0361	SENAJUS	DRCI	OE01	PE75	Contratação	Licença e uso de software	Ferramentas colaborativas (reestruturação da Rede-Lab)	557
78	N0374	SENAJUS	DRCI	OE01	PE75	Contratação	Equipamentos de TIC	Computadores	6
79	N0479	SEOPI	DIOP	OE01	PE89	Contratação	Equipamentos de TIC	Computadores do tipo Servidores	6
80	N0480	SEOPI	DIOP	OE01	PE89	Contratação	Equipamentos de TIC	Sistema de VideoWall	9
81	N0486	SEOPI	DIOP	OE01	PE91	Contratação	Capacitação	Capacitação	3
82*	N0487	SEOPI	DIOP	OE01	PE91	Contratação	Licença e uso de software	Aquisição de software para a CGCCO	13
83*	N0492	SEOPI	DIOP	OE01	PE91	Contratação	Licença e uso de software	Software para Gerenciamento de Máquinas Virtuais VMWare vCenter Server Standard	1

Priorização	Código	Unidade	Área	Objetivo Estratégico	Projeto Estratégico	Tipo	Subtipo	Descrição	Qtd
84*	N0493	SEOPI	DIOP	OE01	PE91	Contratação	Equipamentos de TIC	Roteadores 3g/4g Wifi	2
85	N0495	SEOPI	DIOP	OE01	PE91	Contratação	Equipamentos de TIC	MiniPCs, Workstations e Notebooks	70
86	N0502	SEOPI	DINT	OE03	PE90	Contratação	Licença e uso de software	Software de extração de dados em dispositivos móveis com licença de uso perpétua	2
87	N0503	SEOPI	DINT	OE03	PE90	Contratação	Licença e uso de software	Software capaz de analisar inúmeras extrações ao mesmo tempo	5
88	N0504	SEOPI	DINT	OE03	PE90	Contratação	Licença e uso de software	Software de Inteligência para análise e extração de dados multiplataforma	1
89	N0505	SEOPI	DINT	OE03	PE90	Contratação	Capacitação	Capacitação na área de extração de dados de smartphones danificados	30
90	N0506	SEOPI	DINT	OE03	PE90	Desenvolvimento Interno	Evolução/melhoria de sistema de informação ou aplicativo móvel já existente	Desenvolvimento do Banco de Dados	1
91	N0507	SEOPI	DINT	OE03	PE90	Contratação	Licença e uso de software	Atualização de licenças para extração de dados de dispositivos móveis	3
92	N0519	SEOPI	DIOP	OE01	PE89	Contratação	Equipamentos de TIC	Mini Desktops	30
93	N0520	SEOPI	DIOP	OE01	PE89	Contratação	Equipamentos de TIC	Notebooks	30

Priorização	Código	Unidade	Área	Objetivo Estratégico	Projeto Estratégico	Tipo	Subtipo	Descrição	Qtd
94	N0521	SEOPI	DIOP	OE01	PE89	Contratação	Equipamentos de TIC	Desktops	18
95	N0522	SEOPI	DIOP	OE01	PE91	Contratação	Equipamentos de TIC	Notebooks	30
96	N0523	SEOPI	DIOP	OE01	PE91	Contratação	Equipamentos de TIC	Mini Desktops	30
97	N0524	SEOPI	DIOP	OE01	PE91	Contratação	Equipamentos de TIC	Desktops	10
98*	N0528	SEOPI	DIOP	OE01	PE91	Contratação	Equipamentos de TIC	Servidor de virtualização	1
99	N0211	SE/DTIC	CGSID	OE11	N/D	Contratação	Serviços de TIC	Serviços de contagem de métrica de Software	1
100	N0009	SE/DTIC	GAB/DTIC	OE11	N/D	Contratação	Serviços de TIC	Serviço de apoio especializado de TIC	1
101	N0289	SE/SPO	CGGE	OE10	N/D	Contratação	Licença e uso de software	Licença do Power BI	14
102	N0298	SE/SPO	CGGE	OE09	N/D	Contratação	Capacitação	Capacitação para elaboração de painéis de BI	14
103	N0154	DEPEN	DISPF	OE11	N/D	Contratação	Sistema de Informação comercial	Software para gerenciamento de biblioteca	1
104	N0227	SENAJUS	DEMIG	OE09	N/D	Contratação	Equipamentos de TIC	Notebooks	2
105	N0251	SE/DTIC	CGGOV	OE11	N/D	Desenvolvimento Interno	Outros serviços de provimento de solução de TIC	Relatórios de vulnerabilidades de ativos de TIC	1

Priorização	Código	Unidade	Área	Objetivo Estratégico	Projeto Estratégico	Tipo	Subtipo	Descrição	Qtd
106	N0259	SE/DTIC	CGGOV	OE11	N/D	Contratação	Capacitação	Capacitação de servidores que atuam na área de Segurança da Informação	1
107	N0260	SE/DTIC	CGGOV	OE11	N/D	Contratação	Capacitação	Capacitação com certificação oficial em conhecimentos de hacking ético	1
108	N0261	SE/DTIC	CGGOV	OE11	N/D	Desenvolvimento Interno	Outros serviços de provimento de solução de TIC	Indicadores e controles de monitoramento contínuo de Segurança da Informação e Comunicação	1
109	N0325	SE/DTIC	DPDC	OE06	N/D	Desenvolvimento Interno	Outros serviços de provimento de solução de TIC	Servidor para um sistema em PHP com banco de dados MySQL	1
110	N0327	SE/DTIC	DPDC	OE06	N/D	Desenvolvimento Interno	Outros serviços de provimento de solução de TIC	Migração do portal www.defesadoconsumidor.gov.br para o portal.gov.br	5
111	N0348	DEPEN	DIRPP	OE04	N/D	Contratação	Equipamentos de TIC	Impressora	38
112	N0444	GM	COGER	OE03	N/D	Desenvolvimento Interno	Outros serviços de provimento de solução de TIC	Software homologado para fragmentar arquivos de vídeo	10
113	N0509	SE/SAA	CGDS	N/D	N/D	Desenvolvimento Interno	Outros serviços de provimento de solução de TIC	SEI - Atualizações do Módulo de Protocolo Integrado	1
114	N0153	DEPEN	DISPF	OE04	PE1G	Contratação	Licença e uso de software	Solução de Interoperabilidade Polycom	1

Priorização	Código	Unidade	Área	Objetivo Estratégico	Projeto Estratégico	Tipo	Subtipo	Descrição	Qtd
115	N0166	SENASP	DGI	OE03	PE97	Contratação	Licença e uso de software	Solução de auxílio à gravação, degravação, reconhecimento de texto	1
116	N0170	SENASP	DGI	OE03	PE97	Contratação	Equipamentos de TIC	Desktop com 2 monitores	500
117	N0171	SENASP	DGI	OE03	PE97	Contratação	Serviços de TIC	Sistema de telemetria para viaturas	1
118	N0172	SENASP	DGI	OE03	PE97	Contratação	Equipamentos de TIC	Monitor	500
119*	N0187	SENASP	DGI	OE03	PE97	Contratação	Sistema de Informação comercial	SINESP Justiça Criminal	1
120	N0189	SENASP	DGI	OE03	PE97	Contratação	Equipamentos de TIC	Smartphone	2000
121	N0190	SENASP	DGI	OE03	PE97	Contratação	Equipamentos de TIC	Tablet	500
122	N0191	SENASP	DGI	OE03	PE97	Contratação	Equipamentos de TIC	Desktop com 1 Monitor	500
123*	N0194	SENASP	DGI	OE03	PE97	Contratação	Licença e uso de software	Licença de softwares de banco de dados	5
124	N0195	SENASP	DGI	OE03	PE97	Contratação	Licença e uso de software	Licença de softwares para solução de BI (PowerBI Pro)	15
125*	N0196	SENASP	DGI	OE03	PE97	Contratação	Equipamentos de TIC	Solução completa de videowall	3
126	N0229	SENASP	DPSP	OE03	PE96	Contratação	Equipamentos de TIC	Notebooks	6

Priorização	Código	Unidade	Área	Objetivo Estratégico	Projeto Estratégico	Tipo	Subtipo	Descrição	Qtd
127	N0230	SENASP	DPSP	OE03	PE96	Contratação	Equipamentos de TIC	Câmeras para videoconferência	6
128	N0232	SENASP	DPSP	OE03	PE96	Contratação	Equipamentos de TIC	Fones de ouvido com microfone para videoconferência	6
129	N0233	SENASP	DPSP	OE03	PE96	Contratação	Equipamentos de TIC	Desktop	3
130	N0235	SENASP	DPSP	OE01	PE92	Contratação	Sistema de Informação comercial	Sistema de Gerenciamento de Informações de Laboratório - LIMS	54
131	N0236	SENASP	DPSP	OE01	PE92	Contratação	Licença e uso de software	Software destinado à análise de perfis genéticos	54
132	N0237	SENASP	DPSP	OE01	PE92	Contratação	Equipamentos de TIC	Tablets	54
133	N0238	SENASP	DPSP	OE01	PE92	Contratação	Equipamentos de TIC	Servidores (Equipamento de TI)	54
134	N0244	SENASP	DGI	OE03	PE97	Contratação	Equipamentos de TIC	Mini Rastreador Veicular	1755
135	N0277	SENA CON	DPDC	OE06	PE17	Contratação	Serviços de TIC	Contratação/renovação de Nuvem Oracle	1
136	N0278	SENA CON	DPDC	OE06	PE17	Contratação	Licença e uso de software	Certificados digitais	1
137	N0340	SENAJUS	DPJUS	OE02	PE70	Contratação	Equipamentos de TIC	Notebooks	4
138	N0342	SENAJUS	DPJUS	OE02	PE70	Contratação	Equipamentos de TIC	Webcam	10
139	N0344	SENAJUS	DPJUS	OE02	PE70	Contratação	Equipamentos de TIC	Fones de ouvido	10

Priorização	Código	Unidade	Área	Objetivo Estratégico	Projeto Estratégico	Tipo	Subtipo	Descrição	Qtd
140	N0372	SENAJUS	DRCI	OE01	PE75	Contratação	Equipamentos de TIC	Webcams	5
141	N0423	SENAD	DGA	OE05	PE1P	Contratação	Equipamentos de TIC	Computadores, licenças de Power BI, painéis de BI e equipamentos de videoconferência	2
142	N0426	DEPEN	DIPEN	OE04	PE98	Contratação	Licença e uso de software	Extrator de dados em aparelhos de telefonia móvel	6
143	N0428	DEPEN	DIPEN	OE04	PE98	Contratação	Licença e uso de software	Ferramenta de vínculo de dados (tipo I-2)	6
144	N0430	DEPEN	DIPEN	OE04	PE98	Contratação	Licença e uso de software	Programa para gravação de áudio	1
145	N0434	DEPEN	DIPEN	OE04	PE98	Contratação	Equipamentos de TIC	Notebook	200
146	N0438	DEPEN	DIPEN	OE04	PE98	Contratação	Equipamentos de TIC	Servidor de rede	27
147	N0439	DEPEN	DIPEN	OE04	PE98	Contratação	Equipamentos de TIC	Servidor de rede	27
148	N0501	SEOPI	DIOP	OE01	PE91	Contratação	Serviços de TIC	Provimento de internet móvel	15
149	N0150	DEPEN	GABDEPEN	OE11	N/D	Contratação	Licença e uso de software	Licença Adobe Creative Cloud para equipes	14
150	N0258	SE/DTIC	CGGOV	OE11	N/D	Contratação	Licença e uso de software	Ferramenta de Gestão de Projetos	1
151	N0268	SE/DTIC	CGGOV	OE11	N/D	Contratação	Licença e uso de software	Ferramenta para gerenciamento e acompanhamento de metas e indicadores	1

Priorização	Código	Unidade	Área	Objetivo Estratégico	Projeto Estratégico	Tipo	Subtipo	Descrição	Qtd
152	N0272	GM	OUVG	OE10	N/D	Contratação	Equipamentos de TIC	Webcams	5
153	N0273	GM	OUVG	OE10	N/D	Contratação	Licença e uso de software	Common Data Service	1
154	N0389	GM	ASCOM	OE10	N/D	Contratação	Licença e uso de software	Licenças Adobe - pacote completo	10
155	N0437	SE/DTIC	CGISE	OE11	N/D	Contratação	Equipamentos de TIC	Aquisição de switches de acesso e de equipamentos de rede sem fio	100
156	N0497	SE/SAA	CGDS	N/D	N/D	Desenvolvimento Interno	Outros serviços de provimento de solução de TIC	SEI - Atualização para versão 315	1
157	N0498	SE/SAA	CGDS	N/D	N/D	Desenvolvimento Interno	Outros serviços de provimento de solução de TIC	SEI - Atualização para versão 40	1
158	N0500	SE/SAA	CGDS	N/D	N/D	Desenvolvimento Interno	Outros serviços de provimento de solução de TIC	Atualizações futuras do Sistema SEI	1
159	N0508	SE/SAA	CGDS	N/D	N/D	Desenvolvimento Interno	Outros serviços de provimento de solução de TIC	SEI - Atualizações do Módulo Peticionamento e Intimação Eletrônicos	1
160	N0512	SE/SAA	CGDS	N/D	N/D	Desenvolvimento Interno	Outros serviços de provimento de solução de TIC	SEI - Atualizações do Módulo Aplicativo para Celulares	1
161	N0514	SE/SAA	CGDS	N/D	N/D	Desenvolvimento Interno	Outros serviços de provimento de solução de TIC	SEI - Implantação do Módulo de Produtividade	1

Priorização	Código	Unidade	Área	Objetivo Estratégico	Projeto Estratégico	Tipo	Subtipo	Descrição	Qtd
162	N0516	SE/SAA	CGDS	N/D	N/D	Desenvolvimento Interno	Outros serviços de provimento de solução de TIC	DSpace - Adaptação em funcionalidade	1
163	N0536	SENAD	GAB_SENAD	OE05	N/D	Contratação	Equipamentos de TIC	Notebook	2
164	N0539	SENAD	GAB_SENAD	OE05	N/D	Contratação	Licença e uso de software	Contratação de banco de imagens	1
165	N0545	SENAD	DPPA	OE05	N/D	Contratação	Licença e uso de software	Licença Power BI	4
166	N0554	DEPEN	DISPF	OE11	N/D	Contratação	Equipamentos de TIC	Aquisição de desktops e notebooks	70
167	N0556	DEPEN	DISPF	OE11	N/D	Contratação	Equipamentos de TIC	Kit multimídia para videoconferência	20
168	N0574	DEPEN	DISPF	OE11	N/D	Contratação	Equipamentos de TIC	Monitor	30
169	N0014	SE/SAA	CGDS	N/D	N/D	Desenvolvimento Interno	Outros serviços de provimento de solução de TIC	SEI - Atualizações do Módulo de Barramento Interórgãos (ConectaGov)	1
170	N0015	SE/SAA	CGDS	N/D	N/D	Desenvolvimento Interno	Outros serviços de provimento de solução de TIC	SEI - Painel BI	1
171	N0293	SE/SPO	CGGE	OE10	N/D	Contratação	Licença e uso de software	Ferramentas para o monitoramento da estratégia	1
172	N0294	SE/SPO	CGGE	OE10	N/D	Desenvolvimento Interno	Outros serviços de provimento de solução de TIC	Solução de fluxo de informação para o PEI	1
173	N0326	SE/SPO	CGGE	OE10	N/D	Desenvolvimento Interno	Provimento de solução de análise	Painel de monitoramento do PE	1

Priorização	Código	Unidade	Área	Objetivo Estratégico	Projeto Estratégico	Tipo	Subtipo	Descrição	Qtd
							técnica e gerencial de dados		
174	N0386	SE/SPO	CGGE	OE10	N/D	Desenvolvimento Interno	Evolução/melhoria de sistema de informação ou aplicativo móvel já existente	Manutenção de solução de Gestão Estratégica	1
175	N0203	SE/DTIC	CGISP	OE09	N/D	Contratação	Capacitação	Contratação de cursos e capacitações em TIC para os servidores da DTIC	200
176	N0266	SE/DTIC	CGGOV	OE11	N/D	Contratação	Equipamentos de TIC	Aquisição de Notebooks de alta performance e monitores	200
177	N0525	SE/SPO	CGGE	OE10	N/D	Contratação	Equipamentos de TIC	Computadores	9
178	N0526	SE/SPO	CGGE	OE10	N/D	Contratação	Equipamentos de TIC	Notebook de alto desempenho	2
179	N0151	DEPEN	ESPEN	OE09	N/D	Contratação	Licença e uso de software	Licença Adobe Creative Cloud para equipes	2
180	N0152	DEPEN	DIREX	OE11	N/D	Contratação	Equipamentos de TIC	Dispositivo de multimídia utilizado para vídeo conferência	369
181	N0155	DEPEN	DISPF	OE04	N/D	Contratação	Sistema de Informação comercial	Sistema de gerenciamento de consultas e de estoque de medicamentos	5
182*	N0205	SENASP	DFNSP	OE01	N/D	Contratação	Equipamentos de TIC	Equipamento para a instalação em sites táticos ou transportáveis	20
183	N0207	SENASP	DFNSP	OE01	N/D	Contratação	Equipamentos de TIC	Notebook	104

Priorização	Código	Unidade	Área	Objetivo Estratégico	Projeto Estratégico	Tipo	Subtipo	Descrição	Qtd
184	N0212	SENASP	DFNSP	OE01	N/D	Contratação	Licença e uso de software	Licenças Office 365	150
185	N0213	SENASP	DFNSP	OE01	N/D	Contratação	Equipamentos de TIC	Tablets	5
186	N0214	SENASP	DFNSP	OE01	N/D	Contratação	Equipamentos de TIC	Tablets	1
187	N0215	SENASP	DFNSP	OE01	N/D	Contratação	Licença e uso de software	Licenças Windows 10 PRO	150
188	N0216	SENASP	DFNSP	OE01	N/D	Contratação	Licença e uso de software	Licença Adobe Photoshop	5
189	N0217	SENASP	DFNSP	OE01	N/D	Contratação	Licença e uso de software	Licença Sublime Text 30	5
190	N0218	SENASP	DFNSP	OE01	N/D	Contratação	Licença e uso de software	Licença Prezi	1
191	N0219	SENASP	DFNSP	OE01	N/D	Contratação	Licença e uso de software	Licença Microsoft Project	1
192	N0220	SENASP	DFNSP	OE01	N/D	Contratação	Licença e uso de software	Licença Microsoft Visual Studio	5
193	N0221	SENASP	DFNSP	OE01	N/D	Contratação	Licença e uso de software	Licença AutoCAD 2019	5
194	N0222	SENASP	DFNSP	OE01	N/D	Contratação	Licença e uso de software	Licença CorelDRAW 2020	5
195	N0224	SENAJUS	DEMIG	OE09	N/D	Contratação	Equipamentos de TIC	Fone de ouvido estéreo com sistema de redução de ruído	7
196	N0225	SENAJUS	DEMIG	OE09	N/D	Contratação	Equipamentos de TIC	Câmeras para videoconferência	7

Priorização	Código	Unidade	Área	Objetivo Estratégico	Projeto Estratégico	Tipo	Subtipo	Descrição	Qtd
197	N0226	SENASP	DPSP	OE01	N/D	Desenvolvimento Interno	Evolução/melhoria de sistema de informação ou aplicativo móvel já existente	Evolução do sistema DESARMA	1
198	N0239	SENASP	CGESP	OE10	N/D	Contratação	Licença e uso de software	Licença Microsoft Project	5
199	N0240	SE/SPO	CGCONTAB	N/D	N/D	Contratação	Equipamentos de TIC	Câmera de vídeo tipo Webcam com Headset	10
200	N0241	SE/SPO	CGCONTAB	N/D	N/D	Desenvolvimento Interno	Provimento de solução de análise técnica e gerencial de dados	BI - Painel da Contabilidade	1
201	N0242	SE/SAA	CGAE	N/D	N/D	Contratação	Licença e uso de software	Licenças do Software AutoCad	10
202	N0245	SENASP	DPSP	OE10	N/D	Contratação	Licença e uso de software	Licença Microsoft Project	15
203*	N0246	SENASP	DPSP	OE10	N/D	Contratação	Sistema de Informação comercial	Solução para a Governança do SUSP	1
204	N0265	SE/DTIC	CGGOV	OE11	N/D	Contratação	Capacitação	Capacitação em Gestão e Governança de projetos	20
205	N0269	SE/DTIC	CGGOV	OE11	N/D	Contratação	Capacitação	Curso para elaboração de metas e indicadores	20
206	N0274	SE/SPO	CGOF	N/D	N/D	Contratação	Equipamentos de TIC	Desktops e notebooks	23
207	N0279	GM	OUVG	OE10	N/D	Contratação	Equipamentos de TIC	Aquisição de novos computadores desktop	4

Priorização	Código	Unidade	Área	Objetivo Estratégico	Projeto Estratégico	Tipo	Subtipo	Descrição	Qtd
208	N0281	GM	OUVG	OE10	N/D	Contratação	Licença e uso de software	Aquisição de licenças Pro do Power BI	5
209	N0282	GM	OUVG	OE10	N/D	Contratação	Equipamentos de TIC	Aquisição de fones de ouvido Headset	12
210	N0283	GM	OUVG	OE10	N/D	Contratação	Equipamentos de TIC	Aquisição de notebook com grande capacidade de processamento	2
211	N0287	GM	OUVG	OE10	N/D	Contratação	Equipamentos de TIC	Aquisição de computadores	5
212	N0299	SENASP	DFNSP	OE01	N/D	Contratação	Equipamentos de TIC	Notebooks	20
213*	N0300	SENASP	DFNSP	OE01	N/D	Contratação	Equipamentos de TIC	Impressoras	10
214	N0302	SENASP	DFNSP	OE01	N/D	Contratação	Equipamentos de TIC	Notebooks	1
215	N0303	SENASP	DFNSP	OE01	N/D	Contratação	Equipamentos de TIC	Monitor	2
216	N0306	SENASP	DFNSP	OE01	N/D	Contratação	Equipamentos de TIC	Notebooks	3
217	N0312	SENASP	DFNSP	OE01	N/D	Contratação	Equipamentos de TIC	Localizador Comunicador Satelital Bidirecional	100
218	N0313	SENASP	DFNSP	OE01	N/D	Contratação	Equipamentos de TIC	Tablet	5
219	N0316	SENASP	DFNSP	OE01	N/D	Contratação	Licença e uso de software	Localizador Comunicador Satelital Bidirecional - taxa de ativação	100
220	N0317	SENASP	DPSP	OE10	N/D	Contratação	Equipamentos de TIC	Desktop	4,5

Priorização	Código	Unidade	Área	Objetivo Estratégico	Projeto Estratégico	Tipo	Subtipo	Descrição	Qtd
221*	N0318	SENASP	DPSP	OE10	N/D	Contratação	Licença e uso de software	Licenças de software	27
222	N0319	SENASP	DPSP	OE01	N/D	Contratação	Licença e uso de software	Licenças de software Amped Five professional e Amped Authenticate	48
223	N0320	SENASP	DPSP	OE01	N/D	Contratação	Equipamentos de TIC	Computadores Desktop	113
224	N0322	SENASP	DPSP	OE01	N/D	Contratação	Licença e uso de software	Sistema para extração de dados em dispositivo móveis (UFED)	56
225	N0324	SENASP	DPSP	OE01	N/D	Contratação	Licença e uso de software	Sistema para extração de dados em dispositivos móveis (XRY)	56
226	N0328	SENAJUS	DEMIG	OE09	N/D	Contratação	Equipamentos de TIC	Webcam	4
227	N0332	SENACON	DPDC	OE06	N/D	Contratação	Equipamentos de TIC	Notebooks	2
228	N0334	SENACON	DPDC	OE06	N/D	Contratação	Licença e uso de software	Licença do Pacote Adobe	2
229	N0336	SENAJUS	DEMIG	OE09	N/D	Contratação	Equipamentos de TIC	Webcam	3
230	N0343	SE/SAA	CGAE	N/D	N/D	Desenvolvimento Interno	Evolução/melhoria de sistema de informação ou aplicativo móvel já existente	Evolução do sistema SIMAP	1
231	N0345	SENAJUS	CGJUS	OE11	N/D	Desenvolvimento Interno	Desenvolvimento de novo sistema de informação ou aplicativo móvel	Sistema para cadastro de entidades sociais	1

Priorização	Código	Unidade	Área	Objetivo Estratégico	Projeto Estratégico	Tipo	Subtipo	Descrição	Qtd
232	N0355	DEPEN	DIRPP	OE04	N/D	Contratação	Equipamentos de TIC	Computadores Desktop	5
233	N0363	SE/SPO	CGOF	N/D	N/D	Contratação	Capacitação	Cursos de capacitação	3
234	N0364	GM	OUVG	OE10	N/D	Contratação	Equipamentos de TIC	Aquisição de computadores com grande capacidade de processamento	2
235	N0376	SE/DTIC	CGGOV	OE11	N/D	Contratação	Licença e uso de software	Ferramenta de mapeamento de processos	30
236	N0378	DEPEN	DIRPP	OE04	N/D	Contratação	Equipamentos de TIC	Computadores Desktop	5
237	N0379	SE/SPO	CGCONTAB	N/D	N/D	Contratação	Equipamentos de TIC	Notebook e Desktops	6
238	N0382	GM	COGER	OE03	N/D	Desenvolvimento Interno	Outros serviços de provimento de solução de TIC	Conjunto de ferramentas Microsoft configuradas para atender os fluxos de trabalho	1
239	N0385	GM	COGER	OE03	N/D	Desenvolvimento Interno	Outros serviços de provimento de solução de TIC	Sistema Eletrônico de Processos (PJe-Cor)	1
240	N0387	GM	COGER	OE03	N/D	Contratação	Equipamentos de TIC	Notebooks	4
241	N0388	SEGEN	DIGES	OE11	N/D	Contratação	Equipamentos de TIC	Notebooks	155
242	N0393	ASINT	CGINT-ASINT	N/D	N/D	Contratação	Equipamentos de TIC	Notebook	1
243	N0395	ASINT	CGINT-ASINT	N/D	N/D	Contratação	Equipamentos de TIC	Tablet	1

Priorização	Código	Unidade	Área	Objetivo Estratégico	Projeto Estratégico	Tipo	Subtipo	Descrição	Qtd
244	N0396	GM	ASCOM	OE10	N/D	Contratação	Equipamentos de TIC	Aquisição de desktops e notebooks	4
245	N0397	ASINT	CGINT-ASINT	N/D	N/D	Contratação	Equipamentos de TIC	Webcam	1
246	N0404	GM	ASCOM	OE10	N/D	Contratação	Equipamentos de TIC	Impressora de fotos	1
247	N0408	SENAD	DPPA	OE01	N/D	Desenvolvimento Interno	Desenvolvimento de novo sistema de informação ou aplicativo móvel	Sistema para recebimento e gerenciamento das propostas de parcerias	1
248	N0410	SEGEN	DIGES	OE11	N/D	Contratação	Equipamentos de TIC	Notebooks	98
249	N0411	DEPEN	DISPF	OE04	N/D	Contratação	Equipamentos de TIC	Equipamento de videoconferência	10
250	N0413	DEPEN	DISPF	OE11	N/D	Contratação	Equipamentos de TIC	Manutenção preventiva, corretiva e adaptativa da rede de infraestrutura lógica GPON	1
251	N0415	SEGEN	DIGES	OE11	N/D	Contratação	Equipamentos de TIC	Monitor	98
252	N0417	DEPEN	DISPF	OE04	N/D	Contratação	Sistema de Informação comercial	Aquisição ou desenvolvimento de Software para gerenciamento de materiais	1
253	N0418	DEPEN	DIPEN	OE11	N/D	Contratação	Equipamentos de TIC	Central Telefônica de aparelhos	1
254	N0424	DEPEN	DIPEN	OE11	N/D	Contratação	Equipamentos de TIC	Computador - Estação de Trabalho	5
255	N0425	DEPEN	DIPEN	OE11	N/D	Contratação	Equipamentos de TIC	Monitor	15

Priorização	Código	Unidade	Área	Objetivo Estratégico	Projeto Estratégico	Tipo	Subtipo	Descrição	Qtd
256	N0470	GM	COGER	OE03	N/D	Contratação	Equipamentos de TIC	Webcams	7
257	N0474	DEPEN	DISPF	OE04	N/D	Contratação	Equipamentos de TIC	Fone de ouvido	35
258	N0475	SEGEN	DIGES	OE11	N/D	Contratação	Equipamentos de TIC	Aquisição de desktops	15
259	N0476	SEGEN	DIGES	OE11	N/D	Contratação	Equipamentos de TIC	Notebooks	15
260	N0490	SENAJUS	DEMIG	OE09	N/D	Contratação	Equipamentos de TIC	Fone de ouvido estéreo com sistema de redução de ruído	3
261	N0511	SE/SAA	CGDS	N/D	N/D	Desenvolvimento Interno	Outros serviços de provimento de solução de TIC	SEI - Atualizações do Módulo de Estatísticas	1
262	N0515	SE/SAA	CGDS	N/D	N/D	Desenvolvimento Interno	Outros serviços de provimento de solução de TIC	DSPACE – Implantações de Versões	1
263	N0517	SE/SAA	CGDS	N/D	N/D	Contratação	Equipamentos de TIC	Webcams	50
264	N0518	SE/SAA	CGDS	N/D	N/D	Contratação	Equipamentos de TIC	Notebooks	50
265	N0540	SENAD	GAB_SENAD	OE05	N/D	Contratação	Licença e uso de software	Licença do Corel Draw	1
266	N0541	SENAD	GAB_SENAD	OE05	N/D	Contratação	Licença e uso de software	Licença Photoshop	2
267	N0542	SENAD	GAB_SENAD	OE05	N/D	Contratação	Licença e uso de software	Licença do Bizagi Pro	3

Priorização	Código	Unidade	Área	Objetivo Estratégico	Projeto Estratégico	Tipo	Subtipo	Descrição	Qtd
268	N0543	SENAD	GAB_SENAD	OE05	N/D	Contratação	Equipamentos de TIC	Computadores	2
269	N0001	AN	COAD	OE11	N/D	Contratação	Licença e uso de software	Solução para prevenção a perda de dados	1
270	N0002	AN	COAD	OE11	N/D	Contratação	Licença e uso de software	Solução de auditoria avançada para gerenciamento de acesso à rede	1
271	N0003	AN	COAD	OE11	N/D	Contratação	Licença e uso de software	Solução para monitoramento e gerenciamento das aplicações	1
272	N0004	AN	COAD	OE11	N/D	Contratação	Licença e uso de software	Solução de antivírus e antispam	1
273	N0559	DEPEN	DISPF	OE11	N/D	Contratação	Equipamentos de TIC	Sistema de Monitoramento por áudio	1
274	N0561	DEPEN	DISPF	OE11	N/D	Contratação	Serviços de TIC	Celular via satélite, rural ou sistema similar	1
275	N0563	DEPEN	DISPF	OE11	N/D	Contratação	Serviços de TIC	Manutenção preventiva e corretiva das Centrais VoIP e seus terminais	1
276	N0565	DEPEN	DISPF	OE11	N/D	Contratação	Equipamentos de TIC	Injetores POE para alimentação elétrica de todos os VoIPs	500
277	N0566	DEPEN	DISPF	OE11	N/D	Contratação	Serviços de TIC	Sistemas de segurança eletrônica e monitoramento	1
278*	N0570	SENASP	DFNSP	OE01	N/D	Contratação	Serviços de TIC	Licenças de Telefone VoIP	15
279	N0577	DEPEN	DISPF	OE11	N/D	Contratação	Equipamentos de TIC	Desktops	210

Priorização	Código	Unidade	Área	Objetivo Estratégico	Projeto Estratégico	Tipo	Subtipo	Descrição	Qtd
280	N0579	DEPEN	DISPF	OE11	N/D	Contratação	Equipamentos de TIC	Sistema de circuito fechado de TV	5
281	N0580	SENAD	DPPA	OE05	N/D	Contratação	Equipamentos de TIC	Desktops	4
282	N0011	SEGEN	DEP	OE01	N/D	Contratação	Licença e uso de software	Licença Pacote Adobe	2
283	N0012	SEGEN	DEP	OE01	N/D	Contratação	Equipamentos de TIC	Webcam	10

Tabela 1 - Inventário de Necessidades de TIC

Em cerca de 5% das necessidades de TIC incluídas (indicadas com um *), não foi possível obter um entendimento completo da demanda por parte da DTIC/SE durante a fase de levantamento, o que inviabilizou a definição de ações para seu atendimento. Tais necessidades serão submetidas a um processo mais detalhado de análise junto aos demandantes e serão complementadas na próxima revisão do PDTIC.

8. CRITÉRIOS DE PRIORIZAÇÃO

Durante a identificação das necessidades de TIC, cada unidade do Ministério envolvida no processo elencou e descreveu suas necessidades de acordo com os critérios abaixo:

Critérios	Pontuação
Necessidade vinculada a Projeto Estratégico	10
Necessidade requerida por Exigência Legal	10
Necessidade Transversal (atende a 2 Secretarias ou mais)	8
Necessidade vinculada ao Plano de Transformação Digital	8
Necessidade contemplada no PAC	5

Tabela 2 - Critérios de Prioridade

A ideia central, durante o levantamento, não era meramente estabelecer uma pontuação para cada necessidade de TIC, e sim obter uma avaliação de cada uma delas quanto ao alinhamento à legislação, ao PEI, às diretrizes institucionais do Ministério, ao Plano de Transformação Digital e ao PAC.

Tais critérios foram aprovados pelo GT-PDTIC em uma das reuniões realizadas pelo grupo sob coordenação da integrante titular designada pela DTIC, sendo que cada um deles contribui para a priorização quanto à ordem de execução das necessidades de TIC. Quanto maior for a pontuação, maior será sua prioridade de atendimento.

Para os casos em que ocorreram empates na pontuação, serão usados os seguintes critérios de desempate:

Ordem	Critério
1ª	Necessidade requerida por Exigência Legal
2ª	Necessidade vinculada a Projeto Estratégico
3ª	Necessidade Transversal (atende a 2 Secretarias ou mais)
4ª	Necessidade vinculada ao Plano de Transformação Digital
5ª	Necessidade contemplada no PAC
6ª	Antiguidade (prioridade para a unidade que cadastrou primeiro)

Tabela 3 - Critérios de Desempate

Os critérios de desempate também foram aprovados pelo GT-PDTIC.

Além da priorização com base nos critérios supracitados, foram aprovados outros dois parâmetros que serão usados como referência para o atendimento das necessidades de TIC do PDTIC, de modo a viabilizar a execução do plano e otimizar os recursos disponíveis.

Assim, de acordo com a sistemática estabelecida, a DTIC empenhará esforços para atender às necessidades de TIC seguindo a ordem de prioridade, respeitando-se a capacidade das suas diferentes áreas internas, mas também poderá atender:

1. às necessidades de TIC cujo atendimento, em análise individualizada, não dependa de recursos necessários ao atendimento das de maior prioridade; e
2. às necessidades de TIC que forem necessárias à viabilização da própria execução do PDTIC.

Reiteram-se aqui as considerações do PETIC sobre a necessidade de revisão estratégica, que trará implicações no PDTIC, tais como:

- estruturação de um modelo de Governança de TIC por meio da conclusão de seu diagnóstico, viabilizado por meio da execução de um Termo de Execução Descentralizada – TED com a UnB, que abrangerá a definição de uma cascata de objetivos baseada no COBIT 2019 e poderá impactar na priorização das necessidades de TIC;
- realização de diagnóstico do *IT Score* pelo *Gartner Group*, com a consequente criação de um plano de ação; e
- trabalho de revisão e validação das necessidades do PDTIC pela DTIC junto aos dirigentes do MJSP em reuniões trimestrais (a ser proposto ao CGE), com implicações na exclusão/inclusão/alteração das necessidades.

9. PLANO DE METAS E AÇÕES

Após análise e consolidação das necessidades de TIC, foram definidas ações a serem executadas pela DTIC ou pelas próprias unidades demandantes para o seu atendimento.

Necessidades semelhantes que pudessem ser contempladas por uma mesma ação foram agrupadas na Tabela 4 abaixo, possibilitando assim otimizar os recursos disponíveis e maximizar o alcance da atuação da DTIC/SE.

Código Ação	Descrição Ação	Necessidades Atendidas
A0001	Aquisição de certificado digital	N0278
		N0451
A0002	Aquisição de computadores e monitores para o MJSP	N0207
		N0227
		N0229
		N0233
		N0266
		N0274
		N0279
		N0283
		N0287
		N0299
		N0303
		N0306
		N0332
		N0340
		N0355
		N0363
		N0364
		N0374
		N0378
		N0379
		N0387
		N0388
		N0390
		N0393
		N0396
		N0398
		N0410
		N0415
		N0423
		N0424
		N0425
		N0475
		N0476
		N0495
		N0518

Código Ação	Descrição Ação	Necessidades Atendidas
		N0522
		N0523
		N0524
		N0525
		N0526
		N0536
		N0543
		N0554
		N0574
		N0577
		N0580
A0003	Aquisição de computadores e periféricos para doação - DEPEN	N0434
A0004	Aquisição de computadores e periféricos para doação - SENACON	N0288
A0005	Aquisição de computadores e periféricos para doação - SENASP	N0170
		N0172
		N0191
		N0317
A0006	Aquisição de computadores e periféricos para doação - SEOPI	N0320
		N0519
		N0520
		N0521
A0007	Aquisição de computadores para o MJSP (Macbook)	N0302
A0009	Aquisição de equipamentos de TIC para videoconferência	N0152
		N0224
		N0225
		N0230
		N0232
		N0240
		N0272
		N0282
		N0290
		N0328
		N0336
		N0342
		N0344
		N0363
		N0372
		N0397
		N0401
		N0411
		N0423
		N0470
		N0474
		N0490
		N0517
		N0556

Código Ação	Descrição Ação	Necessidades Atendidas
A0009	Aquisição de equipamentos de TIC para videoconferência	N0012
A0010	Aquisição de impressora de fotos	N0404
A0011	Aquisição de impressoras para doação	N0348
A0013	Aquisição de licenças de software CAD	N0221
		N0242
A0014	Aquisição de licenças de software Common Data Service	N0273
A0015	Aquisição de licenças de software de edição gráfica	N0222
		N0540
A0016	Aquisição de licenças de software de modelagem e automação de processos	N0384
		N0542
A0017	Aquisição de licenças de software de videoconferência	N0153
A0018	Aquisição de licenças de software editor de código fonte	N0217
A0020	Aquisição de licenças de software para análise de vínculo de dados	N0428
		N0504
A0021	Aquisição de licenças de software para análises forenses em vídeos e imagens	N0319
A0022	Aquisição de licenças de software para apresentações não lineares	N0218
A0023	Aquisição de licenças de software para doação - RIBPG	N0236
A0025	Aquisição de licenças de software para extração e análise de dados de dispositivos móveis	N0322
		N0324
		N0426
		N0502
		N0503
A0026	Aquisição de licenças e suporte Microsoft	N0507
		N0195
		N0212
		N0215
		N0219
		N0220
		N0239
		N0245
		N0281
		N0289
		N0358
		N0361
		N0373
		N0384
A0027	Aquisição de rastreadores veiculares para doação	N0423
		N0436
A0030	Aquisição de servidores para doação - RIBPG	N0545
		N0244
A0031	Aquisição de servidores para doação - DEPEN	N0238
		N0438
A0032	Aquisição de servidores para doação	N0439
		N0479
A0033	Aquisição de sistema de gerenciamento de estoque	N0417

Código Ação	Descrição Ação	Necessidades Atendidas
A0034	Aquisição de smartphone para doação	N0189
A0036	Aquisição de software para degravação de áudio	N0166
		N0430
A0039	Aquisição de solução de videowall para doação	N0480
A0040	Aquisição de switches de acesso e de equipamentos de rede sem fio.	N0437
A0041	Aquisição de tablets para doação	N0190
		N0237
A0042	Aquisição de tablets para o MJSP	N0213
		N0214
		N0313
		N0395
A0043	Aquisição e ativação de equipamento localizador comunicador satelital bidirecional	N0312
		N0316
A0044	Aquisição/renovação de licenças de software Adobe	N0150
		N0151
		N0216
		N0334
		N0389
		N0541
		N0011
A0045	Atualização do DSPACE	N0515
A0046	Atualização do SEI	N0497
		N0498
		N0500
A0047	Atualizações do Módulo Aplicativo para Celulares do SEI	N0512
A0048	Atualizações do Módulo de Estatísticas do SEI	N0511
A0049	Atualizações do Módulo de Pesquisa Pública do SEI	N0510
A0050	Atualizações do Módulo de Protocolo Integrado do SEI	N0509
A0051	Atualizações do Módulo Petição e Intimação Eletrônicos do SEI	N0508
A0052	Capacitação dos servidores que atuam na área de SIC	N0259
A0053	Central Telefônica VOIP e aparelhos para a nova sede do DEPEN	N0418
A0054	Conscientização dos usuários de TIC do MJSP em Segurança da Informação e Comunicação	N0249
A0055	Contratação de banco de imagens	N0539
A0056	Contratação de capacitação para extração de dados de smartphones danificados	N0505
A0057	Contratação de capacitação para os servidores da DTIC	N0203
A0058	Contratação de capacitação para os servidores do MJSP em ferramentas de TIC	N0298
		N0363
		N0384
A0059	Contratação de curso de gerenciamento de projetos	N0265
		N0269
A0060	Contratação de curso de hacking ético	N0260
		N0486
A0061	Contratação de cursos de analytics e segurança da informação	N0486

Código Ação	Descrição Ação	Necessidades Atendidas
A0062	Contratação de equipamentos para expansão da capacidade da infraestrutura do Datacenter	N0429
A0063	Contratação de fábrica de software	N0210
A0064	Contratação de Ferramenta de análise de vulnerabilidades	N0263
A0065	Contratação de ferramenta de auditoria e análise de logs de SIC	N0267
A0066	Contratação de Ferramenta de Gestão de Projetos	N0258
A0067	Contratação de ferramenta de mapeamento de processos	N0376
A0068	Contratação de ferramenta para classificação e monitoramento de dados sensíveis, incidentes de segurança e alerta em tempo real	N0270
A0070	Contratação de links de telecomunicação para o SINESP	N0167
A0071	Contratação de manutenção do SINESP	N0180
		N0192
A0072	Contratação de manutenção preventiva e corretiva das Centrais VoIP do DEPEN e seus terminais	N0563
A0073	Contratação de nuvem privada para o SINESP Big Data	N0163
A0074	Contratação de pessoal de apoio de TIC	N0009
		N0010
		N0011
A0075	Contratação de serviço de dados de Internet móvel	N0501
A0076	Contratação de serviço de métrica de software	N0211
A0077	Contratação de serviço de SOC	N0264
A0078	Contratação de serviços de analytics	N0208
A0079	Contratação de serviços de nuvem Oracle	N0277
A0080	Contratação de sistema alternativo de comunicação	N0561
A0081	Contratação de sistema de gerenciamento de biblioteca	N0154
A0082	Contratação de sistema de gerenciamento de consultas e de estoque de medicamentos	N0155
A0083	Contratação de sistema de Gerenciamento de Informações de Laboratório	N0235
A0084	Contratação de sistema de Gestão de Frota	N0186
A0086	Contratação de sistema SINESP CAD	N0193
A0087	Contratação de sistema SINESP Delegacia Virtual	N0182
A0088	Contratação de sistema SINESP Infoseg	N0161
A0089	Contratação de sistema SINESP Integração	N0178
A0091	Contratação de sistema SINESP PPE	N0175
A0092	Contratação de sistema SINESP Segurança	N0176
A0093	Contratação de solução de telemetria veicular	N0171
A0094	Contratação de suporte para software open source de infraestrutura de TIC	N0435
A0095	Contratação de suporte para usuários de sistemas críticos	N0202
		N0247
A0096	Contratação de suporte técnico para a solução Netbackup	N0448
A0097	Desenvolvimento de API para acesso a Base de Dados do Sistema Gestão Ágil	N0555
A0098	Desenvolvimento de formulário eletrônico para coleta de informações prisionais	N0157
A0099	Desenvolvimento de Front End para o CNCP	N0158

Código Ação	Descrição Ação	Necessidades Atendidas
A0100	Desenvolvimento de Painel de BI de Transferências Voluntárias e Obrigatórias de recursos para segurança pública.	N0564
A0101	Desenvolvimento de painel de BI para a Contabilidade	N0241
A0102	Desenvolvimento de painel de BI para a SENAD	N0423
A0103	Desenvolvimento de painel de BI para o PEI	N0326
A0104	Desenvolvimento de painel de BI para o Portal SINESP	N0164
A0105	Desenvolvimento de sistema de gerenciamento de processos licitatórios	N0572
A0106	Desenvolvimento de sistema de gestão das transferências Fundo a Fundo	N0414
A0107	Desenvolvimento de sistema de gestão de competências a partir do SGC	N0280
A0108	Desenvolvimento de Sistema de Gestão de Convênios e Contratos de Repasse	N0529
A0109	Desenvolvimento de sistema de Gestão de Logística para o SINESP (Intranet)	N0188
A0110	Desenvolvimento de sistema de Gestão e Controle de Efetivo	N0530
A0112	Desenvolvimento de sistema de monitoramento das obras prisionais	N0409
A0113	Desenvolvimento de sistema de OSCIPs e OEs	N0345
A0114	Desenvolvimento de sistema para recebimento e gerenciamento das propostas de parcerias da SENAD	N0408
A0115	Desenvolvimento de sistema SIAN (AN)	N0006
A0116	Desenvolvimento de sistema SIGA (AN)	N0005
A0117	Desenvolvimento de sistema SINESP Agente de Campo	N0185
A0118	Desenvolvimento de sistema SINESP Auditoria	N0177
A0119	Desenvolvimento de sistema SINESP Cidadão	N0179
A0120	Desenvolvimento de sistema SINESP Perícia	N0181
A0121	Desenvolvimento de sistema SINESP VDE	N0184
A0122	Desenvolvimento de solução analytics - SINESP Big Data	N0160
A0123	Desenvolvimento de solução analytics - SINESP DW Análise	N0165
A0124	Desenvolvimento de solução de fluxo de informação para Corregedoria Digital	N0382
A0125	Desenvolvimento de solução de fluxo de informação para o PEI	N0294
A0126	Desenvolvimento do sistema Córtex	N0162
A0127	Disponibilização de ambiente Moodle	N0325
A0128	Disponibilização de infraestrutura e serviços de nuvem para a Rede-Lab	N0351
A0129	Disponibilização de solução para gerenciamento e acompanhamento de metas e indicadores	N0268
A0130	Elaboração de normativos de SIC	N0293
A0131	Especificação e aquisição de sistema de monitoramento para os presídios federais	N0248
A0132	Evolução do sistema Desarma	N0413
A0133	Evolução do sistema estratégia.mj/CIVIS	N0559
		N0565
		N0566
		N0579
		N0226
		N0386

Código Ação	Descrição Ação	Necessidades Atendidas
A0134	Evolução do sistema ORCRIM	N0506
A0135	Evolução do sistema SIMAP	N0343
A0136	Evolução do sistema SINESP SAIE	N0183
A0137	Execução de serviços e controles de Segurança da Informação e Comunicação no MJSP	N0252
A0138	Homologação de solução para fragmentação de vídeos	N0444
A0139	Identificação de vulnerabilidades de SIC nos ativos de TIC do MJSP	N0251
A0140	Implantação da plataforma Resoluto	N0309
A0141	Implantação de indicadores e controles específicos de monitoramento contínuo e da performance de SIC	N0261
A0142	Implantação de sistema de ponto eletrônico	N0350
A0143	Implantação de solução de antivírus e antispam no Arquivo Nacional	N0004
A0144	Implantação de solução de auditoria avançada para gerenciamento de acesso à rede no Arquivo Nacional	N0002
A0145	Implantação de solução para monitoramento e gerenciamento das aplicações no Arquivo Nacional	N0003
A0146	Implantação de solução para prevenção a perda de dados no Arquivo Nacional	N0001
A0147	Implantação do Módulo de Gestão Documental do SEI	N0513
A0148	Implantação do Módulo de Produtividade do SEI	N0514
A0149	Implantação no MJSP de sistema para o Programa de Gestão	N0275
A0150	Implementação de gestão de ativos de TIC	N0250
A0151	Internalização de Sistema Eletrônico de Processos (PJe-Cor)	N0385
A0152	Internalização de sistema Recall	N0271
A0153	Internalização do sistema Consumidor.gov.br	N0277
A0154	Migração do portal www.defesadoconsumidor.gov.br para o portal.gov.br	N327
A0155	Mitigação de vulnerabilidades de Segurança da Informação e Comunicação no MJSP	N0254
A0156	Planejamento da internalização do SINESP	N0173
A0157	Realização de análises de segurança nos sistemas do MJSP	N0253
A0158	Realização de TED com a UnB para definição, validação e implantação inicial de um modelo de Governança de TIC no MJSP	N0007
A0159	Realização de TED com a UnB para realização de curso de mestrado profissional em ciência, engenharia e segurança de dados	N0008
A0160	Realização de testes de segurança nos sistemas do MJSP	N0256
A0161	Reconfiguração do layout do relatório de descoberta da comunidade de legislação do Dspace	N0516
A0162	Replicação de base de dados do SINESP	N0168
A0163	Aquisição de licenças de software para verificação de similaridade dos trabalhos científicos e demais produções acadêmicas dos integrantes do SUSP	N0010
A0165	Atualizações do Módulo de Barramento Interórgãos (ConectaGov)	N0014

Código Ação	Descrição Ação	Necessidades Atendidas
A0166	Painel BI	N0015

Tabela 4 - Ações para atendimento das necessidades de TIC

As metas adotadas neste PDTIC são as estabelecidas no PETIC, com os respectivos indicadores vinculados aos objetivos estratégicos de TIC.

Na próxima revisão do PDTIC, quando serão incorporados os novos elementos resultantes da revisão estratégica (conclusão do diagnóstico situacional de Governança de TIC do MJSP e estabelecimento de uma cascata de objetivos) e houver a ampliação da força de trabalho da DTIC/SE com a chegada de 35 servidores temporários, serão estabelecidos também indicadores e metas para o acompanhamento da execução das ações listadas na Tabela 4, complementando assim no nível tático o monitoramento estratégico da área de TIC do MJSP.

10. PLANO DE GESTÃO DE PESSOAS

10.1 Efetivo Atual

A DTIC/SE/MJSP conta atualmente com um total de 48 (quarenta e oito) colaboradores, assim distribuídos:

Quadro de servidores da DTIC	Atual
Analista em Tecnologia da Informação - ATI	18
Analista Técnico Administrativo - ATA	6
Agente Administrativo	1
Assistente Administrativo	1
Cedidos	15
Temporários	4
Comissionados s/ vínculo	3
Total	48

Tabela 5 - Quadro de servidores da DTIC

10.2 Atribuições e Necessidades de Pessoal

O Decreto nº 9.662, de 01 de janeiro de 2019, que constituiu a DTIC na reestruturação do MJSP, estabeleceu um significativo aumento da estrutura de TIC no Ministério, passando de 07 (sete) cargos em comissão para 28 (vinte e oito). Entretanto, a criação desses cargos em comissão, embora necessária, não é suficiente para concretização das demandas existentes. Há necessidade de reforço do atual quadro de servidores efetivos da DTIC em razão desse acréscimo recente de sua estrutura organizacional.

Além do acréscimo de estrutura organizacional, à DTIC foram atribuídas novas competências de natureza estratégica para o MJSP, como é o caso do desenvolvimento e manutenção de um ambiente de compartilhamento de dados (*Big Data*) no âmbito do MJSP.

A instituição do Sistema Único de Segurança Pública – SUSP e a criação da Política Nacional de Segurança Pública e Defesa Social – PNSPDS, pela Lei nº 13.675/2018, teve por objetivo a preservação da ordem pública e da incolumidade das pessoas e do patrimônio.

Para isso, a referida lei prevê a atuação conjunta, coordenada, sistêmica e integrada dos órgãos de segurança pública e defesa social

da União, dos Estados, do Distrito Federal e dos Municípios, em articulação com a sociedade.

Nesse cenário, o MJSP é o órgão central dessa estrutura e ator fundamental na condução da PNSPDS, ao coordenar a atuação de todos os integrantes operacionais do SUSP (Polícia Federal, Polícia Rodoviária Federal, polícias civis, polícias militares, corpos de bombeiros militares, guardas municipais, agentes penitenciários, institutos oficiais de criminalística, medicina legal e identificação, entre outros).

De acordo com a referida Lei, são algumas das diretrizes da PNSPDS (Art. 5º):

"V - coordenação, cooperação e colaboração dos órgãos e instituições de segurança pública nas fases de planejamento, execução, monitoramento e avaliação das ações, respeitando-se as respectivas atribuições legais e promovendo-se a racionalização de meios com base nas melhores práticas;

VII - fortalecimento das instituições de segurança pública por meio de investimentos e do desenvolvimento de projetos estruturantes e de inovação tecnológica;

VIII - sistematização e compartilhamento das informações de segurança pública, prisionais e sobre drogas, em âmbito nacional;

XI - padronização de estruturas, de capacitação, de tecnologia e de equipamentos de interesse da segurança pública;

XXIII - uso de sistema integrado de informações e dados eletrônicos;"

A coordenação e integração entre órgãos e instituições de segurança pública exige a intercomunicação entre dezenas de sistemas e centenas de bancos de dados já existentes, bem como o desenvolvimento de diversas aplicações ou funcionalidades de novos sistemas.

Além disso, para que o SUSP possa ser realmente efetivo, será necessário criar e manter **um ambiente de compartilhamento de dados** para coletar, manipular, analisar e exibir dados, construindo valor agregado com as análises geradas, por meio da implantação de um *Big Data* no âmbito do MJSP.

Nesse contexto, é imperioso que a Diretoria de Tecnologia da Informação e Comunicação seja estruturada de forma a suportar as demandas de projetos voltados à utilização de tecnologias de *Big Data Analytics*, no âmbito do MJSP. Isso porque projetos dessa natureza demandam, além de infraestrutura robusta, especialistas altamente capacitados em diversas áreas da ciência da computação, a exemplo de cibersegurança, arquitetura de sistemas distribuídos, arquitetura de dados escaláveis, otimização de SGBD, processamento de fluxos contínuos de dados, dentre outras habilidades, todas voltadas à manutenção de ambiente capaz de coletar e processar grandes volumes de dados, estruturados ou não estruturados.

10.3 Processos Críticos com Carência de Servidores

Para fins de avaliação do dimensionamento da força de trabalho, foram identificados quatro processos mais críticos da DTIC, assim considerados aqueles prioritários em virtude de demandarem um elevado volume de trabalho (processos 1 e 2) e/ou pela sua criticidade quanto ao impacto nos resultados alcançados pela DTIC (processos 3 e 4):

- (1) planejamento de contratações e fiscalização de contratos de infraestrutura de TIC e de suporte aos usuários de sistemas;
- (2) planejamento de contratações e fiscalização de contratos de desenvolvimento de sistemas;
- (3) gestão dos processos de TIC; e
- (4) compartilhamento de dados e sustentação da Plataforma *Big Data*.

Do total de 24 (vinte e quatro) servidores ATAs e ATIs lotados na DTIC, 19 (dezenove) servidores (80%) estão dedicados aos dois primeiros processos críticos supracitados, quais sejam: planejamento e fiscalização de contratações de infraestrutura de TIC e de suporte aos usuários de sistemas e de desenvolvimento de sistemas.

A Coordenação-Geral de Infraestrutura e Serviços - CGISE da DTIC é responsável pela fiscalização de contratos de infraestrutura de TIC (segurança e monitoramento de redes, sistemas operacionais, armazenamento, sistemas de produção, bancos de dados, serviços de telecomunicações) e atendimento aos usuários dos sistemas de TIC. Nessa área, atualmente, a DTIC/MJSP conta com 13 (treze) servidores técnicos efetivos envolvidos com a fiscalização (fiscal requisitante e fiscal técnico) de 25 (vinte e cinco) contratos de TIC, que totalizam um montante de cerca de R\$ 30 (trinta) milhões por ano. Além do

montante em recursos financeiros, a complexidade dos contratos de TIC envolvem a complexidade da tecnologia, da gestão de especialistas, além de lidar com sistemas críticos, que exigem operação ininterrupta (24/7), muitas vezes em regime de urgência/emergência. Os sistemas desenvolvidos e/ou suportados pela DTIC/MJSP atendem aos vários órgãos que integram o MJSP, tais como SENACON, SENAD, SENASP, SENAJUS, além de mais de 250 (duzentos e cinquenta) mil profissionais de segurança pública da União, estados e municípios, como policiais federais, civis e militares, guardas municipais, bombeiros, agentes penitenciários e peritos criminais.

A recorrência de eventos e incidentes de segurança indica a necessidade de se reforçar os padrões e processos de segurança da informação a fim de proteger o MJSP contra comportamentos hostis. Nesse sentido, há a necessidade de reforço e qualificação do pessoal, próprio e terceirizado, com perfil especializado em segurança da informação.

A instituição do Comitê de Governança de Dados e Sistemas de Informação, no âmbito do MJSP, em funcionamento desde o mês de março/20, tem facilitado o compartilhamento de dados entre órgãos do MJSP e outros órgãos da APF em níveis que superam todos os alcançados anteriormente. Esse novo patamar de compartilhamento de dados demandará da área de TIC do MJSP uma estrutura de pessoal adequada para processar e atender às solicitações de compartilhamento, em apoio ao Comitê de Governança de Dados e Sistemas. Tal ação insere-se num contexto mais amplo de adequação da área de TIC do MJSP a fim de se possibilitar às áreas de negócio a tomada de decisões orientada a dados (*data driven*), aumentando a efetividade das políticas públicas do Ministério. Essa nova orientação da gestão demandará profissionais com competência para tratamento e análise de dados, além de profissionais para a gestão dos processos de compartilhamento de dados.

10.4 Estimativa da capacidade de execução disponível da TIC.

Embora não haja limitações para a quantidade de contratos ou sistemas em desenvolvimento que um fiscal/gestor de TIC consiga acompanhar simultaneamente, é preciso evitar que o profissional fique sobrecarregado, de forma a prejudicar a fiscalização/gestão da prestação do serviço pela empresa contratada (fábrica de *software*). Sobre essa questão, manifestou-se o TCU no seguinte sentido:

"a qualidade dos serviços prestados pelas contratadas e, por conseguinte, dos sistemas desenvolvidos, reflete de maneira direta no desempenho das organizações, já que os sistemas objeto de desenvolvimento/manutenção dão suporte aos seus processos de trabalho. Nesse sentido, a carência de pessoal capacitado para conduzir o processo de gestão contratual, além da falta de estrutura da organização contratante, prejudica sobremaneira a realização de avaliação de qualidade de forma sistemática." (Auditorias na gestão de contratos de TI / Tribunal de Contas da União, Secretaria de Fiscalização de Tecnologia da Informação; Relatoria Augusto, Sherman Cavalcanti, Ministro-substituto. – Brasília: TCU, 2015).

A experiência de gestão/fiscalização de contratos na DTIC/MJ recomenda que a cada gestor/fiscal de TIC seja designado o acompanhamento simultâneo do desenvolvimento de, no máximo, 03 (três) sistemas (ou contratos), a depender da complexidade.

10.5 Ações de pessoal em andamento

10.5.1 Contratação de 35 servidores temporários

Contratação de 35 (trinta e cinco) profissionais de tecnologia da informação e comunicação – TIC, conforme quadro a seguir, para a implantação de um ambiente de *Big Data* capaz de atender às crescentes necessidades dos órgãos que compõem o Ministério e dos órgãos de segurança pública de Estados e Municípios:

Função	Quantidade
Engenheiro de Dados (Big Data)	10
Analista de Governança de Dados (Big Data)	13
Cientista de dados (Big Data)	12

Tabela 6 - Quantitativo de servidores temporários a serem contratados

A finalização do processo seletivo e o início das atividades dos servidores estão previstos para ocorrer até o final do mês de novembro/2020.

10.5.2 Mestrado profissionalizante

Termo de Execução Descentralizada entre o MJSP e Universidade de Brasília para a capacitação (mestrado profissionalizante) do corpo de servidores da DTIC na área de ciência, engenharia e segurança de dados, de forma que haja um corpo de especialistas apto a manter o projeto de Big Data após sua implantação.

10.5.3 Contratação de serviços de apoio à gestão de dados

Encontra-se em andamento o planejamento da contratação de empresa para prestação de serviços de apoio à gestão do compartilhamento de dados no âmbito do MJSP. O serviço tem objetivo de apoiar a DTIC na formalização, renovação e monitoramento de Acordos de Cooperação Técnica e Termos de Acesso celebrados entre o MJSP e outros órgãos públicos para o compartilhamento de dados.

10.5.4 Plano de Transformação Digital

O plano de transformação digital pactuado entre a SE/MJSP, SEME/SG-PR e SGD/ME em outubro de 2019 e repactuado em agosto de 2020 prevê a alocação de 24 (vinte e quatro) servidores com os seguintes perfis:

Perfil	Qtd	Descrição	Motivação
Governança	3	Profissional capacitado e orientado a entender as necessidades de negócio e buscar as melhores soluções.	É necessário a ampliação dessa capacidade para o atendimento do quantitativo dos serviços previstos para o gerenciamento da integração dos serviços da TI.
Infraestrutura	5	Profissional com alta experiência em otimização de infraestrutura e implantação de processos ITIL.	Com a ampliação dos serviços digitais ofertados, assim como a otimização dos já existentes, é necessário que haja um reforço técnico na área de infraestrutura, de forma a otimizar os ambientes que hospedarão os serviços.
Segurança	3	Profissional com experiência em segurança da informação, e com conhecimentos diversos a	A adaptação de todos os serviços que interagem com o público externo necessitará de uma atenção especial em relação ao atendimento das normas de

Perfil	Qtd	Descrição	Motivação
		respeito dos normativos sobre o tema.	segurança da informação, em especial à Lei de Proteção de Dados.
Gestor de Projeto	13	Profissional com capacidade para apoiar na gestão e no monitoramento do órgão referente ao portfólio de serviços estabelecido no Plano Digital.	Tendo em vista a dimensão das metas estabelecidas no Plano Digital, será necessário montar uma estratégia de acompanhamento e monitoramento, identificando as necessidades e potencialidades de atuação conjunta com órgãos/entidades, definindo estratégia de abordagem, atores, para implementação da Estratégia de Governo Digital.

Tabela 7 - Perfis dos servidores para execução do Plano de Transformação Digital

Em 2020, foram disponibilizadas pela SGD/ME 5 (cinco) Gratificações Temporárias do Sistema de Administração dos Recursos de Tecnologia da Informação – GSISPs para serem concedidas, por meio de processo seletivo simplificado, a servidores que fossem atuar de forma dedicada ao Projeto de Transformação Digital do MJSP. Entretanto, houve baixa no quadro de pessoal de 02 (dois) servidores, que foram para o INSS através de processo seletivo similar.

Por fim, há expectativa de que o processo seletivo para contratação de 350 (trezentos e cinquenta) servidores temporários pela SGD/ME para atuação na transformação digital resulte no envio de servidores à DTIC/SE em quantidade correspondente à que falta para completar o efetivo previsto.

10.6 Necessidades do Arquivo Nacional

O Arquivo Nacional (AN) reportou a necessidade de reforçar seu efetivo na Coordenação Regional do Arquivo Nacional no Distrito Federal (Coreg) com dois profissionais, sendo um analista de sistemas (e/ou TIC) e um desenvolvedor de sistemas (não necessariamente servidores públicos).

O Arquivo Nacional desenvolve mais de onze projetos com sistemas novos, legados e customizações de softwares livres, sendo que dois desses sistemas são estratégicos e fazem parte do PEI da Instituição. Outros sete fazem parte do programa de Transformação Digital do Governo ou são customizações de software para atender os serviços prestados pelo AN.

A equipe de TIC do AN conta com cinco técnicos (para análise e desenvolvimento), todos alocados na sede, no Rio de Janeiro, e, diante



do crescimento das atividades de análise, desenvolvimento e descentralização das tarefas, surgiu a necessidade de complementá-la com profissionais da área lotados em Brasília. Esses profissionais seriam escalados para atuar nos projetos do AN na capital e apoiar as atividades de TIC dos servidores de lá.

11. PLANO ORÇAMENTÁRIO

Apresenta-se na Tabela 8 abaixo o planejamento de recursos necessários para o cumprimento das atribuições da DTIC/SE, de acordo com cada área de atuação.

Área de Atuação	Previsão 2021	Previsão 2022	Previsão 2023
Aquisição de computadores e acessórios	R\$15.163.802,68	R\$10.000.000,00	R\$10.000.000,00
Capacitação	R\$ 927.428,33	R\$ 927.428,33	R\$ 927.428,33
Contratação de pessoal	R\$1.688.960,00	R\$1.688.960,00	R\$1.688.960,00
Desenvolvimento de sistemas	R\$19.854.771,60	R\$19.854.771,60	R\$19.854.771,60
Gestão de dados	R\$19.240.800,00	R\$19.240.800,00	R\$19.240.800,00
Licenciamento de software	R\$19.714.235,39	R\$18.549.575,39	R\$18.549.575,39
Manutenção e melhorias da infraestrutura e serviços de TIC	R\$47.219.483,71	R\$34.219.483,71	R\$ 34.219.483,71
Melhoria da Governança e Gestão de TIC	R\$1.705.651,67	R\$1.540.098,33	R\$ 712.331,67
Segurança da Informação e Comunicação	R\$8.096.387,20	R\$9.823.282,35	R\$9.823.282,35
Total	R\$133.611.520,58	R\$115.844.399,71	R\$115.016.633,05

Tabela 8 - Plano Orçamentário

A seguir, são relacionadas as ações vinculadas a cada área de atuação, incluindo-se aquelas que, a princípio, serão executadas com recursos externos aos da DTIC/SE.

Aquisição de computadores e acessórios									
A0002	A0009	A0010	A0042						
Capacitação									
A0052	A0057	A0059	A0061	A0159					
Contratação de pessoal									
A0074									
Desenvolvimento de sistemas									
A0063	A0076	A0098	A0099	A0105	A0106	A0107	A0108	A0109	A0110
A0112	A0113	A0114	A0115	A0116	A0117	A0118	A0119	A0120	A0121
A0124	A0125	A0132	A0133	A0134	A0135	A0136	A0140	A0142	A0149
A0151	A0152	A0153	A0156						
Gestão de dados									
A0078	A0097	A0100	A0101	A0102	A0103	A0104	A0122	A0123	A0126
A0154	A0162								
Licenciamento de software									
A0014	A0017	A0026	A0044	A0163					
Manutenção e melhorias da infraestrutura e serviços de TIC									
A0001	A0040	A0045	A0046	A0047	A0048	A0049	A0050	A0051	A0062
A0070	A0073	A0075	A0079	A0094	A0095	A0096	A0127	A0128	A0138

A0147	A0148	A0161	A0165	A0166					
Melhoria da Governança e Gestão de TIC									
A0066	A0067	A0129	A0141	A0158					
Segurança da Informação e Comunicação									
A0054	A0060	A0064	A0065	A0068	A0077	A0130	A0137	A0139	A0150
A0155	A0157	A0160							
Orçamento externo à DTIC									
A0003	A0004	A0005	A0006	A0007	A0011	A0013	A0015	A0016	A0018
A0020	A0021	A0022	A0023	A0025	A0027	A0030	A0031	A0032	A0033
A0034	A0036	A0039	A0041	A0043	A0053	A0055	A0056	A0058	A0071
A0072	A0080	A0081	A0082	A0083	A0084	A0086	A0087	A0088	A0089
A0091	A0092	A0093	A0131	A0143	A0144	A0145	A0146		

Tabela 9 - Ações vinculadas às áreas de atuação

12. PLANO DE GESTÃO DE RISCOS

Um risco é um evento ou condição incerta que, se ocorrer, provocará um impacto positivo ou negativo junto à execução do PDTIC.

Com o objetivo de gerenciar os riscos de maneira simples e objetiva, foi elaborado o Plano de Gestão de Riscos abaixo, inspirado nos processos de gerenciamento de riscos previstos no Guia *PMBOK® - Project Management Body of Knowledge*.

Segundo este Guia, o Gerenciamento dos riscos inclui identificar, analisar, planejar respostas e controlar os riscos. Sendo assim, a ideia é aumentar a probabilidade e o impacto dos eventos positivos e reduzir a probabilidade e o impacto dos eventos negativos sobre a execução deste Plano.

12.1 Identificação dos Riscos

A primeira etapa para elaboração do Plano de Gestão de Riscos foi identificá-los.

12.2 Análise dos Riscos

A segunda etapa para a elaboração do Plano de Gestão de Riscos foi estimar os Riscos utilizando o método qualitativo.

Esta abordagem consiste em definir a criticidade dos Riscos por meio da avaliação combinada da Probabilidade do Risco ocorrer e da classificação do Impacto que o Risco poderá causar sobre a execução do PDTIC.

Neste método, os componentes dos Riscos são estimados como Alto, Médio e Baixo.

Para tanto, foi desenvolvida uma Matriz de Probabilidade x Impacto utilizada para definir a criticidade dos Riscos identificados:

Probabilidade	Impacto	Criticidade
Alta	Alto	Alta
Alta	Médio	Alta
Alta	Baixo	Média
Média	Alto	Alta

Probabilidade	Impacto	Criticidade
Média	Médio	Média
Média	Baixo	Baixa
Baixa	Alto	Média
Baixa	Médio	Baixa
Baixa	Baixo	Baixa

Tabela 10 - Matriz de Probabilidade x Impacto

12.3 Critérios de Aceitação dos Riscos

Após identificar e priorizar os Riscos, foi definida uma estratégia de tratamento e resposta aos Riscos negativos, visando trazer os níveis de risco para patamares aceitáveis. Foram consideradas as seguintes medidas para o tratamento dos Riscos negativos identificados:

Tipo de Tratamento do Risco	Resposta ao Risco
Aceitar	Nenhuma medida será tomada. O custo de proteção é maior que o custo do ativo ou o Risco já se encontra dentro de patamares aceitáveis.
Eliminar	Eliminação total do Risco. Como qualquer execução de atividade tem sempre um Risco associado à adoção dessa resposta. Normalmente, resulta na eliminação da atividade.
Mitigar	A medida irá diminuir a Probabilidade e o Impacto do Risco.
Transferir	Transferir a responsabilidade do Risco para um terceiro. Normalmente, resulta na contratação de um seguro ou na terceirização de serviços.

Tabela 11 - Respostas aos Riscos

E, enfim, tem-se o Plano de Gestão de Riscos

Identificação		Matriz				Estratégia	
Id	Descrição do Risco	Probabilidade	Impacto	Criticidade	Tratamento	Resposta	Responsável
1	Quantitativo inadequado de recursos humanos para a execução e acompanhamento do PDTIC	Alta	Alto	Alta	Mitigar	Realização de concursos temporário para a área de TIC, solicitação de ATIs ao ME e requisição de servidores / empregados públicos	Alta Gestão do MJSP e DTIC
2	Atraso na realização de novo processo seletivo de servidores temporários	Alta	Alto	Alta	Mitigar	Readequar o uso dos recursos humanos existentes e priorizar as demandas estratégicas	DTIC
3	Falta de patrocínio da Alta Gestão do Ministério para executar o PDTIC	Baixa	Baixo	Baixa	Aceitar	Adequar o uso da estrutura existente e priorizar as demandas estratégicas	DTIC
4	Ausência de recursos orçamentários ou financeiros	Baixa	Alto	Média	Aceitar	Executar as ações do PDTIC que forem possíveis	DTIC
5	Descumprimento da priorização estabelecida no PDTIC	Baixa	Alto	Média	Eliminar	Manter o Comitê de Governança de TIC operante, visando ao acompanhamento das ações do PDTIC, não executando qualquer ação que não esteja priorizada no PDTIC	Alta Gestão

Identificação				Matriz		Estratégia	
Id	Descrição do Risco	Probabilidade	Impacto	Criticidade	Tratamento	Resposta	Responsável
6	Falta de conhecimento técnico da equipe da DTIC para a execução do PDTIC	Média	Alto	Alta	Mitigar	Realizar ações de capacitação previstas no Plano de Gestão de Desenvolvimento	DTIC
7	Morosidade na execução do processo licitatório	Alta	Alto	Alta	Mitigar	Priorização do processo de contratação junto às áreas competentes	Alta Gestão
8	Atraso ou Suspensão do processo licitatório em face de impugnações	Média	Alto	Alta	Mitigar	Estar aderente à legislação e às boas práticas de contratações, sempre alinhado à Área Jurídica do MJSP	DTIC
9	Mudanças no cenário Político ou na legislação vigente	Média	Alto	Alta	Aceitar	Adequar o PDTIC no que for necessário	DTIC
10	Incapacidade de execução contratual pelas empresas contratadas da DTIC	Média	Alto	Alta	Mitigar	Empreender ações, criação, acompanhamento ou não renovação de contratos	DTIC
11	Não atualização do parque computacional (Desktop e Notebooks)	Baixa	Alto	Média	Mitigar	Empreender ações prévias para que a atualização ocorra no tempo correto	DTIC
12	Baixa qualidade dos serviços prestados pelas terceirizadas sob a gestão da DTIC	Média	Alto	Alta	Mitigar	Acompanhar continuamente a qualidade dos serviços prestados e executar ajustes imediatos, aplicando sanções cabíveis	DTIC

Identificação		Matriz				Estratégia	
Id	Descrição do Risco	Probabilidade	Impacto	Criticidade	Tratamento	Resposta	Responsável
13	Desinteresse da prestadora de serviços em renovar o contrato.	Baixa	Alto	Média	Mitigar	Realizar um planejamento da contratação efetivo, definindo os ANS – Acordos de Nível de Serviço - e o salário dos prestadores de acordo com os padrões de mercado.	DTIC

Tabela 12 - Plano de Gestão de Riscos

Importante ressaltar que este Plano de Gestão de Riscos ainda não está alinhado ao Modelo de Gerenciamento de Riscos e Controles Internos do MJSP. Este está baseado na estrutura do COSO ERM, na Norma Internacional ISO 31000/2009 e nas boas práticas adotadas no setor público.

Sendo assim, será revisto e alinhado ao Modelo de Gerenciamento de Riscos e Controles Internos do MJSP na próxima revisão deste PDTIC.

13. MONITORAMENTO E AVALIAÇÃO DO PLANO

Segundo o Guia do PDTIC do SISP, o monitoramento, no âmbito do acompanhamento do PDTIC, pode ser considerado como uma atividade constante e sistemática de coleta de informações a respeito do desempenho da execução do PDTIC, de modo a identificar possíveis desvios das ações programadas e colaborar para o momento de avaliação e posterior tomada de decisões.

Cabe à Coordenação de Portfólio e Normativos de TIC – CPN/CGGOV/DTIC/SE a responsabilidade de monitorar a execução do PDTIC, acompanhando a implementação das ações, o uso dos recursos e a entrega dos serviços com o objetivo de atender às estratégias e aos objetivos do órgão.

Com foco no plano de metas e ações e nos riscos, tal monitoramento concorrerá com a realização de reuniões trimestrais entre a DTIC/SE e as unidades de negócio do MJSP, em que a área de TIC buscará um entendimento mais abrangente das necessidades de cada unidade para, em conjunto, avaliar se as ações desempenhadas estão produzindo valor e alinhar expectativas. Com tal aproximação, busca-se assegurar a adequada alocação de recursos, com a eventual readequação dos programas, projetos e até mesmo dos objetivos estratégicos de TIC

Assim, o monitoramento da execução pontual de ações previstas no PDTIC será importante subsídio para tais reuniões de acompanhamento, que por sua vez poderão fornecer feedback essencial para a realização da avaliação dessa execução.

De acordo com a sistemática estabelecida, as avaliações intermediárias do PDTIC serão realizadas conjuntamente com as revisões periódicas, e, conforme exposto no PETIC, deverão contar com o desenvolvimento de novos indicadores para representar os resultados obtidos na próxima revisão estratégica do plano.

Avalia-se que, dessa forma, seja maximizada a possibilidade de alcance das metas planejadas com maior eficiência.

14. CONCLUSÃO

De acordo com a Instrução Normativa SGD/ME nº 01, de 04 de abril de 2019, solução de TIC é um “conjunto de bens e/ou serviços que apoiam processos de negócio, mediante a conjugação de recursos, processos e técnicas utilizados para obter, processar, armazenar, disseminar e fazer uso de informações”. Depreende-se de tal definição que a definição de solução de TIC depende não só da natureza de um equipamento a ser adquirido, por exemplo, mas também da forma como ele será utilizado. Assim, um equipamento de TIC que será usado de forma isolada, sem articulação com outros dispositivos ou sistemas de gerenciamento, e para atender uma necessidade finalística específica, pode não constituir uma solução de TIC, ao passo que o mesmo equipamento poderá ser considerado como tal se for utilizado em situação diversa.

Decorre que não é possível obter um entendimento amplo e completo das necessidades de TIC durante o período de elaboração do PDTIC, seja porque a demanda ainda não está suficiente madura por parte do titular, seja porque depende de análises aprofundadas que comumente são feitas somente após sua aprovação e alocação de pessoal para seu atendimento.

Esse PDTIC, portanto, cumpre sua missão de levantar no plano tático as necessidades de TIC do MJSP de forma a possibilitar um planejamento dos recursos de TIC do Ministério, porém requer revisão constante dessas necessidades de forma que, à medida que o conhecimento sobre elas se aprofunda, possa representá-las de forma mais precisa.

Anexo VIII - SEI MJSP 13636809 - Portaria de Pessoal SAA 1.pdf



13636809



08006.000003/2021-38

Boletim de Serviço em 11/01/2021



Ministério da Justiça e Segurança Pública

PORTARIA DE PESSOAL SAA/SE/MJSP Nº 1, DE 08 DE JANEIRO DE 2021

O SUBSECRETÁRIO DE ADMINISTRAÇÃO DA SECRETARIA-EXECUTIVA DO MINISTÉRIO DA JUSTIÇA E SEGURANÇA PÚBLICA, no uso da competência atribuída pelo § 1º do art. 1º do Anexo da Portaria nº 1.222, de 21 de dezembro de 2017, que aprova o Regimento Interno da Secretaria-Executiva do Ministério da Justiça e Segurança Pública, do art. 2º do Capítulo II da Portaria nº 1.429, de 3 de novembro de 2020, alterada pela Portaria nº 1.596, de 14 de dezembro de 2020, da Secretaria-Executiva do Ministério da Justiça e Segurança Pública, e do disposto no § 2º do art. 10 da Instrução Normativa nº 1, de 4 de abril de 2019, da Secretaria de Governo Digital do Ministério da Economia, e

Considerando a necessidade de instituir a Equipe de Planejamento para Contratação de Serviço de Centro de Operações de Segurança - SCO (Security Operations Center - SOC) com fornecimento suporte 24h por dia e 7 dias por semana abrangendo: aplicativos, equipamentos, Blue Team, Red Team e treinamentos para a equipe de gestão de SIC do MJSP, resolve:

Art. 1º Designar para compor a referida equipe os seguintes membros:

I - **Integrante Requisitante**: representante da Área Requisitante da Solução:

Ivanildo de Oliveira da Silva JR, CPF 031.033.324-59;

II - **Integrante Requisitante Substituto**: representante da Área Requisitante da Solução:

Joédes Cardoso da Silva, CPF 523.656.891-91;

III - **Integrante Técnico**: representante da Área de Tecnologia da Informação e Comunicação:

João Marcelo Rodrigues Sant' Ana, CPF nº 706.056.701-10;

IV - **Integrante Técnico Substituto**: representante da Área de Tecnologia da Informação e Comunicação:

Cintia Mye Yonekawa Yamaguti, CPF nº 619.425.371-15, e

V - **Integrante Administrativo**: representante da Área Administrativa:

Gustavo Henrique Corrêa de Paula Maciel, CPF 916.497.571-15.

Art. 2º Esta Portaria entra em vigor na data de sua publicação.



Documento assinado eletronicamente por **ROGÉRIO XAVIER ROCHA**, Subsecretário(a) de **Administração**, em 11/01/2021, às 16:33, conforme o § 1º do art. 6º e art. 10 do Decreto nº 8.539/2015.

A autenticidade do documento pode ser conferida no site <http://sei.autentica.mj.gov.br> informando o código verificador **13636809** e o código CRC **284C26A1**

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 13636809

Anexo IX - SEI MJSP 14627967 - Portaria SAA 57.pdf



14627967



08006.000003/2021-38

Boletim de Serviço em 11/05/2021



Ministério da Justiça e Segurança Pública

PORTARIA SAA/SE/MJSP Nº 57, DE 11 DE MAIO DE 2021

O SUBSECRETÁRIO DE ADMINISTRAÇÃO DA SECRETARIA-EXECUTIVA DO MINISTÉRIO DA JUSTIÇA E SEGURANÇA PÚBLICA, no uso da competência atribuída pelo § 1º do art. 1º do Anexo da Portaria nº 1.222, de 21 de dezembro de 2017, que aprova o Regimento Interno da Secretaria-Executiva do Ministério da Justiça e Segurança Pública, do art. 2º do Capítulo II do art. 13 do Capítulo X da Portaria nº 1.429, de 3 de novembro de 2020, alterada pela Portaria nº 1.596, de 14 de dezembro de 2020, da Secretaria-Executiva do Ministério da Justiça e Segurança Pública, e do disposto no § 2º do art. 10 da Instrução Normativa nº 1, de 4 de abril de 2019, da Secretaria de Governo Digital do Ministério da Economia, resolve:

Art. 1º Alterar o art. 1º da Portaria de Pessoal nº 1, de 8 de janeiro de 2021, da Subsecretaria de Administração da Secretaria-Executiva do Ministério da Justiça e Segurança Pública, que institui Equipe de Planejamento instituir a Equipe de Planejamento para Contratação de Serviço de Centro de Operações de Segurança - SCO (Security Operations Center - SOC) com fornecimento suporte 24h por dia e 7 dias por semana abrangendo: aplicativos, equipamentos, Blue Team, Red Team e treinamentos para a equipe de gestão de SIC do MJSP, que passa a vigorar com a seguinte redação:

"Art. 1º

I -

II -

III - **Integrante Técnico:** representante da Área de Tecnologia da Informação e Comunicação:

Cintia Mye Yonekawa Yamaguti, CPF nº 619.425.371-15;

IV - **Integrante Técnico Substituto:** representante da Área de Tecnologia da Informação e Comunicação:

Ivanildo de Oliveira da Silva JR, CPF nº 031.033.324-59. "(NR)

V -

Art. 2º Esta Portaria entra em vigor na data de sua publicação.

Documento assinado eletronicamente por **ROGÉRIO XAVIER ROCHA**, Subsecretário(a) de **Administração**, em 11/05/2021, às 18:54, conforme o § 1º do art. 6º e art. 10 do Decreto nº



8.539/2015.



A autenticidade do documento pode ser conferida no site <http://sei.autentica.mj.gov.br> informando o código verificador **14627967** e o código CRC **96BBB55D**

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 14627967

DIÁRIO OFICIAL DA UNIÃO

Publicado em: 16/09/2020 | Edição: 178 | Seção: 1 | Página: 269

Órgão: Ministério da Justiça e Segurança Pública/Gabinete do Ministro

PORTARIA Nº 513, DE 15 DE SETEMBRO DE 2020

Dispõe sobre a implantação de Programa de Integridade em empresas contratadas pelo Ministério da Justiça e Segurança Pública.

O MINISTRO DE ESTADO DA JUSTIÇA E SEGURANÇA PÚBLICA-SUBSTITUTO, no uso das atribuições que lhe confere o inciso II do parágrafo único do art. 87 da CRFB, c/c o inciso III do art. 1º do Decreto nº 8.851, de 20 de setembro de 2016, e tendo em vista o disposto no inciso VIII do art. 7º da Lei nº 12.846, de 1º de agosto de 2013, nos arts. 41 e 42 do Decreto nº 8.420, de 18 de março de 2015, no parágrafo único do art. 7º da Portaria CGU nº 57, de 4 de janeiro de 2019, e no Anexo IX da Portaria MJSP nº 86, de 23 de março de 2020, e o consta no processo administrativo nº 08001.004150/2019-11, resolve:

Art. 1º Dispor sobre a implantação de Programa de Integridade em empresas contratadas pelo Ministério da Justiça e Segurança Pública.

Parágrafo único. Esta Portaria se aplica:

I - no caso de contratações cujos valores sejam iguais ou superiores a R\$ 10.000.000,00 (dez milhões de reais); e

II - nos casos de contratações em que sejam celebrados termos aditivos para prorrogação da prestação de serviços continuados ou para efetivar acréscimos legais ao preço, ao ser atingida a alçada prevista no inciso I, pelo somatório dos valores.

Art. 2º São objetivos desta Portaria:

I - inserir as empresas contratadas na política e nas ações de integridade da administração pública;

II - contribuir para a redução dos riscos de práticas ilegais ou irregulares que possam gerar atos lesivos ou potencialmente lesivos aos princípios da administração pública, ao erário e à imagem do Ministério da Justiça e Segurança Pública;

III - prevenir a ocorrência de irregularidades relacionadas a desvios de conduta administrativa ou ética;

IV - orientar o relacionamento entre os agentes públicos e as empresas contratadas e seus dirigentes e funcionários; e

V - propiciar a prestação do serviço público com transparência e previsibilidade.

Art. 3º Deverá haver previsão expressa nos editais de licitação e em documentação prévia às contratações de que as empresas contratadas deverão se comprometer a implantar Programa de Integridade ou adequar seu Programa de Integridade já existente ao previsto nesta Portaria.

Art. 4º Os termos de referência e projetos básicos das contratações deverão conter cláusulas específicas com as obrigações deste Ministério e da empresa contratada relativamente às exigências de integridade, nos seguintes moldes:

I - das obrigações dos órgãos do Ministério da Justiça e Segurança Pública e seus agentes públicos:

a) não praticar atos para ingerência na administração da empresa contratada, especialmente quanto a direcionamento de escolha de possíveis trabalhadores;

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

c) notificar a empresa contratada, por escrito, sobre desvios de conduta, irregularidades, fraudes ou atos ilícitos, praticados na execução do contrato; e

II - das obrigações da empresa contratada:

a) estabelecer normas gerais de integridade:

1. em até 6 (seis) meses para contratos de até 12 (doze) meses; e

2. em até 9 (nove) meses para contratos de mais de 12 (doze) meses;

b) orientar seus empregados alocados para a execução do contrato sobre as normas de integridade e a indispensabilidade de seu cumprimento;

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

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

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

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

g) apresentar à equipe de fiscalização do contrato, juntamente com o rol de documentos obrigatórios do empregado alocado para a execução do contrato, Termo de Ciência e Concordância, devidamente assinado pelo empregado, conforme modelo constante no anexo a esta Portaria; e

h) encaminhar à equipe de fiscalização do contrato, observados os prazos estabelecidos na alínea "a", documentação que evidencie, em alinhamento com os parâmetros do Capítulo IV do Decreto nº 8.420, de 2015, a realização das seguintes ações e atividades:

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

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

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

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

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

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

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

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

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

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

Art. 5º A implantação ou a adequação do Programa de Integridade poderá ser comprovada por qualquer documento hábil a ser encaminhado à equipe de fiscalização do contrato, preferencialmente, em meio digital.

Art. 6º Caberá à equipe de fiscalização do contrato acompanhar o cumprimento do prazo para apresentação dos documentos comprobatórios, que, após análise da conformidade das informações, deverá dar ciência à unidade do Ministério da Justiça e Segurança Pública responsável pelo Programa de Integridade e à empresa contratada.

§ 1º Após a implementação ou adequação do Programa de Integridade pela contratada, a equipe de fiscalização deverá realizar acompanhamento da execução do programa, por meio do relatório encaminhado pela empresa contratada, semestralmente.

§ 2º Em caso de descumprimento do envio do relatório semestral, o responsável pelo acompanhamento deverá notificar a empresa contratada e proceder com o registro do ocorrido.

§ 3º Em caso de descumprimento da obrigação de apresentar o Programa de Integridade dentro dos prazos estabelecidos, a equipe de fiscalização deverá tomar as providências cabíveis para a aplicação de penalidade à empresa contratada.

Art. 7º O descumprimento das obrigações previstas nesta Portaria ensejará aplicação das penalidades previstas e acordadas no contrato ou de penalidades de natureza administrativa, no caso dos agentes públicos.

Art. 8º Esta Portaria deverá constar como anexo dos editais referentes às licitações e contratações, inclusive em potencial, de que tratam os incisos do parágrafo único do art. 1º.

Art. 9º Esta Portaria entrará em vigor no dia 30 de novembro de 2020.

TERCIO ISSAMI TOKANO

Este conteúdo não substitui o publicado na versão certificada.



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 FAZEI 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 LICITAÇÃO E CONTRATOS, E A EMPRESA XXXXXXXXXXXXXXXXXXXX.

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 nº 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 nº 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 nº 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 **XXXXXXXXXXXXXXXXXX**, inscrita no CNPJ nº XXXXXXXXXX e inscrição estadual nº XXXXXXXX, estabelecida XXXXXXXXXX - CEP XXXXXXXX, neste ato representada pelo Senhor **XXXXXXX**, CPF nº xxxxxxxx, RG nº 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**, 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. Ptes:
- 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
Tecnologia da Informação e Comunicação
Ministério da Justiça e Segurança Pública
Justiça e Segurança Pública

RODRIGO LANGE

Diretor de
Ministério da

XXXXXXXXXXXXXXXXXXXXXXX

Representante da Contratada

TESTEMUNHAS:

1. NOME:

CPF:

2. NOME:

CPF:



Documento assinado eletronicamente por **Gustavo Henrique Correa de Paula Maciel**,



Coordenador(a) de Contratos, em 15/02/2022, às 17:11, 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 **17243768** e o código CRC **CF1CA3A6**

O trâmite deste documento pode ser acompanhado pelo site

<http://www.justica.gov.br/aceso-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 17243768



17309079



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 III DO EDITAL

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 XXXXXXXX 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 **EDUARDO DE OLIVEIRA DA ROSA, Pregoeiro(a)**, em 22/02/2022, às 14:14, 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 **17309079** e o código CRC **55039053**

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 17309079