



Poder Judiciário

Conselho Nacional de Justiça

PREGÃO ELETRÔNICO N. 90012/2026

Objeto	Contratação de Serviços Gerenciados de Segurança da Informação.		
Valor estimado	R\$ 17.117.372,20 (dezessete milhões, cento e dezessete mil, trezentos e setenta e dois reais e vinte centavos)		
Data de abertura: 19/06/2026	Horário: 14h (horário de Brasília)		
Endereço eletrônico: https://www.gov.br/compras/pt-br	UASG: 40003		
Exclusiva ME/EPP? NÃO	Reserva de quota para ME/EPP? NÃO		
Decreto n. 7.174/2010? NÃO	Vistoria? SIM		
Amostra/Demonstração? NÃO	Modo de disputa: ABERTO E FECHADO		
Forma de julgamento: MENOR PREÇO	Forma de adjudicação: ITEM E GRUPO		
Instrumento contratual: TERMO DE CONTRATO	Impugnação e pedido de esclarecimento: até 18hs do dia 16/06/2026		



Poder Judiciário

Conselho Nacional de Justiça

Pregoeiro e equipe de apoio	<p>COMISSÃO PERMANENTE DE CONTRATAÇÃO (CPC)</p> <p>Edifício Sede do CNJ, SAF Sul, Quadra 2, CEP: 70070-600, Brasília/DF.</p> <p>Telefone: (61) 2326-5159 / (61) 2326-5016. E-mail: cpc@cnj.jus.br</p>
Mensagem aos licitantes	<p>O edital, anexos e demais informações estão disponíveis para <i>download</i> no Portal Nacional de Contratações Públicas (PNCP) (https://www.gov.br/pncp/pt-br) e Portal do CNJ (https://www.cnj.jus.br/transparencia-cnj/gestao-administrativa/licitacoes-e-contratos/).</p> <p>Os licitantes sujeitam-se às sanções e penalidades estabelecidas neste edital e em seus anexos.</p> <p>Antes de apresentarem propostas, os licitantes deverão analisar cuidadosamente o inteiro teor deste edital e dos anexos, compreender todos os termos, certificar-se de que dispõem dos recursos materiais e humanos necessários para participar da sessão pública e obter a certeza de que toda a documentação exigida está atualizada de acordo com exigências editalícias e pronta para ser exibida quando requisitada pelo pregoeiro.</p>



Poder Judiciário

Conselho Nacional de Justiça

PREGÃO ELETRÔNICO N. 90012/2026

PREÂMBULO

O Conselho Nacional de Justiça (CNJ) torna público o Pregão Eletrônico n. 90012/2026, com critério de julgamento por menor preço. A sessão pública será realizada em **19/06/2026**, às **14h** (horário de Brasília), no CNJ, por meio do sítio <https://www.gov.br/compras/pt-br>. Esta licitação foi autorizada no Processo SEI n. 04520/2025, nos termos da Lei n. 14.133/2021, e demais legislação aplicável, de acordo com as condições estabelecidas neste edital.

SEÇÃO I – DO OBJETO DA LICITAÇÃO

1.1. Contratação de Serviços Gerenciados de Segurança da Informação, observadas as condições e especificações estabelecidas nos Anexos I, II e III deste edital.

SEÇÃO II – DAS CONDIÇÕES DE PARTICIPAÇÃO

2.1. A sessão deste pregão será pública e realizada conforme este edital, em data, horário e endereço eletrônico indicados no preâmbulo.

2.2. Poderão participar deste pregão eletrônico pessoas físicas e jurídicas que:

- a) atendam às condições deste edital e seus anexos, inclusive quanto à documentação, e estejam devidamente cadastradas no sítio <https://www.gov.br/compras/pt-br>, na forma do regulamento;
- b) possuam registro cadastral atualizado no Sistema de Cadastramento Unificado de Fornecedores (SICAF), o qual também será requisito para fins de habilitação;
- c) explorem ramo de atividade compatível com o objeto da licitação;



Poder Judiciário

Conselho Nacional de Justiça

- d) estejam constituídas na forma de cooperativas, desde que atendidos os requisitos do art. 16 da Lei n. 14.133/2021, mediante declaração em campo próprio do sistema;
- e) constituam consórcios de empresas, desde que atendidos os requisitos do art. 15 da Lei n. 14.133/2021.

2.3. 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.

2.4. É de responsabilidade do cadastrado conferir a exatidão dos seus dados cadastrais nos sistemas e mantê-los atualizados junto aos órgãos responsáveis pela informação, devendo proceder à imediata correção ou à alteração dos registros tão logo identifique incorreção ou aqueles se tornem desatualizados.

2.5. A não observância do disposto no item anterior poderá ensejar desclassificação no momento da habilitação.

2.6. A obtenção do benefício dos arts. de 42 a 49 da Lei Complementar n. 123/2006 limita-se às microempresas e às empresas de pequeno porte que, no ano-calendário de realização da licitação, ainda não tenham firmado contratos com a Administração Pública cujos valores somados extrapolem a receita bruta máxima admitida para enquadramento como empresa de pequeno porte.

2.6.1. A microempresa ou empresa de pequeno porte, caso contratada, será responsável por solicitar seu desenquadramento de tal condição quando houver ultrapassado o limite de faturamento estabelecido no art. 3º, da Lei Complementar n. 123/2006, em razão desta contratação.



Poder Judiciário

Conselho Nacional de Justiça

2.7 A declaração falsa relativa à proposta de preços e ao cumprimento dos requisitos de habilitação e do art. 3 da Lei Complementar n. 123/2006 sujeitará o licitante às sanções previstas na legislação.

2.8. Não poderá participar desta licitação pessoa física ou jurídica que:

- a) não explore atividade compatível com o objeto desta licitação;
- b) seja, de forma direta ou indireta, agentes públicos do CNJ;
- c) constitua empresa, isoladamente ou em consórcio, responsável por elaborar o projeto básico ou executivo, ou empresa da qual o autor do projeto seja dirigente, gerente, controlador, acionista ou detentor de mais de 5% (cinco por cento) do capital com direito a voto, responsável técnico ou subcontratado, quando a licitação versar sobre obra, serviços ou fornecimento de bens a ela necessários;
- d) se encontre, ao tempo da licitação, impossibilitada de participar em decorrência de sanção que lhe foi imposta;
- e) mantenha vínculo de natureza técnica, comercial, econômica, financeira, trabalhista ou civil com dirigente do órgão ou entidade contratante ou com agente público que exerça função na licitação, atue na fiscalização ou na gestão do contrato, ou que deles seja cônjuge, companheiro ou parente em linha reta, colateral ou por afinidade, até o terceiro grau;
- f) seja empresa controladora, controlada ou coligada, nos termos da Lei n. 6.404/1976, concorrendo entre si;
- g) tenha sido, nos 5 (cinco) anos anteriores à divulgação do edital, condenada judicialmente, com trânsito em julgado, por explorar trabalho infantil, por submeter trabalhadores a condições análogas à escravidão ou por contratar adolescentes nos casos vedados pela legislação trabalhista;
- h) configure Organização da Sociedade Civil de Interesse Público (OSCIP) atuando nessa condição;



Poder Judiciário

Conselho Nacional de Justiça

i) seja autor do anteprojeto, do projeto básico ou do projeto executivo, quando a licitação versar sobre obra, serviços ou fornecimento de bens a ele relacionados; e

j) seja empresa que, por conta de vínculo com o CNJ, tenha prestado auxílio técnico na elaboração dos documentos da fase interna do procedimento licitatório, tais como o Documento de Oficialização de Demanda, os Estudos Preliminares ou o Termo de Referência (TR).

2.9. Não poderá participar, direta ou indiretamente, da licitação ou da execução do contrato agente público do órgão ou entidade contratante, devendo ser observadas as situações que possam configurar conflito de interesses no exercício ou após o exercício do cargo ou emprego, nos termos da legislação que disciplina a matéria, conforme § 1º do art. 9º da Lei n. 14.133/2021.

2.10. O impedimento que trata da impossibilidade de participar de licitação será também aplicado ao licitante que atue em substituição de outra pessoa, física ou jurídica, com o intuito de burlar a efetividade da sanção a ela aplicada, inclusive sua controladora, controlada ou coligada, desde que devidamente comprovado o ilícito ou a utilização fraudulenta da personalidade jurídica do licitante.

2.11. A declaração falsa relativa ao cumprimento dos requisitos de habilitação e da proposta de preços sujeitará o licitante às sanções legais.

2.12. Os documentos apresentados nesta licitação deverão conter os números de CNPJ dos estabelecimentos que, a critério de uma mesma pessoa jurídica licitante, serão responsáveis pela execução do objeto e que poderão emitir, em decorrência, ao longo da vigência do contrato, as notas fiscais que serão apresentadas a pagamento.

2.13. Quando permitida a participação de consórcio de empresas, a habilitação técnica, quando exigida, será feita por meio do somatório dos



Poder Judiciário

Conselho Nacional de Justiça

quantitativos de cada consorciado e, para efeito de habilitação econômico-financeira, quando exigida, será observado o somatório dos valores de cada consorciado.

2.13.1. Se o consórcio não for formado integralmente por microempresas ou empresas de pequeno porte (MEs/EPPs) e o TR exigir requisitos de habilitação econômico-financeira, haverá acréscimo de 10% (dez por cento) do valor exigido do licitante individual para a habilitação econômico-financeira, salvo se houver justificativa nos autos para suprimir tal acréscimo para o consórcio em relação ao valor exigido para os licitantes individuais.

SEÇÃO III – DA APRESENTAÇÃO DA PROPOSTA DE PREÇOS

3.1. Nesta licitação, a fase de habilitação sucederá as fases de apresentação de propostas e lances e de julgamento.

3.2. Após a divulgação do edital no endereço eletrônico, os licitantes encaminharão, exclusivamente por meio do sistema, mediante digitação de senha privativa, a proposta com a descrição do objeto ofertado e o preço, **formulada de acordo com os Anexos I e II do edital**, até a data e o horário estabelecidos para abertura da sessão pública, quando, então, encerrar-se-á, automaticamente, a fase de recebimento de propostas.

3.3. Ao encaminhar a proposta de preços, o licitante deverá incluir o **detalhamento do objeto** ofertado no campo “Descrição Detalhada do Objeto”. Caso o número de caracteres seja insuficiente, deverá incluir descrição resumida com as informações essenciais.

3.4. No cadastro da proposta inicial, em campo próprio do sistema, o licitante deverá responder se:

a) cumpre os requisitos estabelecidos no art. 3º da Lei Complementar n. 123/2006, estando apto a usufruir do tratamento estabelecido nos arts. 42 a 49, bem como se os limites dos valores dos contratos celebrados com a Administração



Poder Judiciário

Conselho Nacional de Justiça

Pública não extrapolaram a receita bruta máxima admitida para o ano calendário a para enquadramento como empresa de pequeno porte;

a.1) nos itens exclusivos para participação de MEs e EPPs, a assinalação do campo “não” impedirá o prosseguimento no certame;

a.2) nos itens em que a participação não for exclusiva para MEs e EPPs, assinalar o campo “não” exclui o licitante do tratamento favorecido previsto na Lei Complementar n. 123/2006, mesmo que se configure como tal;

b) está ciente e concorda com as condições contidas no edital e seus anexos, bem como cumpre os requisitos de habilitação neles definidos;

c) a proposta apresentada está conformidade as exigências editalícias;

d) inexistem fatos supervenientes e impeditivos à habilitação no certame, ciente da obrigatoriedade de declarar ocorrências posteriores;

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

f) 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;

g) os serviços são prestados por empresas que comprovem cumprir reserva de cargos para pessoa com deficiência, para reabilitado da Previdência Social ou para aprendiz, bem como reservas fixadas em outras normas específicas.

h) a proposta econômica compreende os custos integrais para atender os direitos trabalhistas assegurados na Constituição, nas leis trabalhistas, nas normas infralegais, nas convenções coletivas de trabalho e nos termos de ajustamento de conduta vigentes à data de entrega da proposta.



Poder Judiciário

Conselho Nacional de Justiça

h.1) o não cumprimento da exigência acima acarretará desclassificação do certame, nos termos do art. 63, §1º da Lei n. 14.133/2021.

3.5. Até a abertura da sessão pública, o licitante poderá retirar ou substituir a proposta e os documentos de habilitação (quando houver previsão de anteceder a fase) inseridos no sistema.

3.6. O licitante deverá consignar em campo próprio do sistema **o valor unitário de cada item e, se for o caso, de cada item que compõe o grupo**, já considerados e inclusos os tributos, fretes, tarifas e demais despesas decorrentes da execução do objeto.

3.7. Não será aceita oferta de objeto com especificações distintas das indicadas nos anexos deste edital.

3.8. Em caso de divergência entre as especificações técnicas descritas no Sistema Comprasnet e as deste edital, prevalecerão estas.

3.9. Os valores deverão ser calculados com duas casas decimais.

3.10. Na etapa de apresentação da proposta, não haverá ordem de classificação. A proposta do licitante mais bem classificado será disponibilizada para avaliação do pregoeiro e para acesso público apenas após o fim do envio de lances.

3.11. A proposta deverá ser redigida em língua portuguesa, sem alternativas, opções, emendas, ressalvas, borrões, rasuras ou entrelinhas, e dela deverá constar:

a) identificação social, número do CNPJ dos estabelecimentos que, a critério de uma mesma pessoa jurídica licitante, serão responsáveis pela execução do objeto, assinatura do representante legal da proponente, referência a esta licitação, endereço, dados bancários, número de telefone e e-mail;

b) indicação do responsável pela assinatura do contrato, com número da carteira de identidade, CPF e, caso não seja sócio da empresa, procuração com poderes para assinar o instrumento em nome da proponente passada em



Poder Judiciário

Conselho Nacional de Justiça

instrumento público particular, acompanhada de documento oficial de identificação do outorgante para comparação das assinaturas e verificação de autenticidade;

c) prazo de validade da proposta de 60 (sessenta) dias a contar da data de abertura da sessão pública estabelecida no preâmbulo deste edital;

d) indicação única de preço (em R\$), com exibição dos valores unitário, em algarismos, e total, em algarismos e por extenso, conforme o lance final respectivo; e

e) descrição clara do objeto cotado, em conformidade com as especificações técnicas constantes no Anexo I do edital (Termo de Referência), com indicação de quantidade, prazo de entrega e demais características, quando houver.

f) Especificação clara, completa e minuciosa da solução ou produto ofertado para os serviços dos itens 2, 4 e 5 do Grupo 1, informando o nome, a descrição e o fabricante, bem como indicação precisa da comprovação de cada característica constante nas especificações técnicas deste Termo de Referência conforme modelo de planilha constante no ANEXO J – PLANILHA DE ATENDIMENTO AOS REQUISITOS TÉCNICOS:

f.1) Entende-se por documento (s) a documentação técnica oficial do fabricante da solução ou produto ofertado, seja em meio eletrônico ou materializada em papel;

f.2) Não serão aceitas declarações ou cartas de conformidade ou adequação ao solicitado e especificado no termo de referência em substituição ou complementação da documentação técnica oficial e original.

3.12. 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 do licitante.

3.13. A apresentação das propostas obriga ao cumprimento das disposições nelas contidas, de acordo com o disposto no TR. O proponente se compromete a



Poder Judiciário

Conselho Nacional de Justiça

executar o objeto licitado em tais termos, bem como a fornecer materiais, equipamentos, ferramentas e utensílios necessários, em quantias e qualidades adequadas à perfeita execução contratual, substituindo-os quando requerido.

3.14. Se disponível a opção no sistema, o licitante poderá parametrizar o valor final mínimo ao cadastrar a proposta e obedecerá às regras a seguir:

I - O intervalo mínimo de diferença de valores 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 0,10% (um décimo por cento) do valor total da contratação estimado no Anexo II deste edital;

II - os lances serão de envio automático pelo sistema, respeitado o valor final mínimo estabelecido e o intervalo de que trata o inciso I.

3.15. O valor final mínimo poderá ser alterado pelo fornecedor durante a fase de disputa, sendo vedado o valor superior a lance já registrado pelo fornecedor no sistema, quando adotado o critério de julgamento por menor preço.

3.16. O valor final mínimo parametrizado será sigiloso para os demais fornecedores e para o CNJ, podendo ser disponibilizado estrita e permanentemente aos órgãos de controle externo e interno.

SEÇÃO IV – DA ABERTURA DA SESSÃO PÚBLICA E DA FASE DE ENVIOS DE LANCES

4.1. A sessão pública será aberta automaticamente pelo sistema no dia e hora indicados no preâmbulo deste edital.

4.2. A comunicação entre pregoeiro e licitantes ocorrerá mediante troca de mensagens em campo próprio do sistema, vedada outra forma de comunicação.

4.3. O licitante deverá acompanhar as operações no sistema durante a sessão pública, ficando responsável pelo ônus devido à perda de negócios pela inobservância de qualquer mensagem emitida pelo sistema ou de sua desconexão.



Poder Judiciário

Conselho Nacional de Justiça

4.4. Aberta a fase competitiva, os licitantes classificados poderão enviar lances exclusivamente por meio do sistema, sendo imediatamente informados do recebimento do lance e do valor consignado no registro.

4.5. O licitante somente poderá oferecer valor inferior ao último lance por ele ofertado e registrado pelo sistema, observado o intervalo mínimo de diferença de valores ou de percentuais entre os lances, que incidirá tanto em relação aos lances intermediários quanto em relação ao lance que cobrir a melhor oferta.

4.6. O licitante poderá, uma única vez, excluir seu último lance ofertado, no intervalo de quinze segundos após o registro no sistema, na hipótese de lance inconsistente ou inexequível.

4.7. O pregoeiro poderá, durante a disputa, como medida excepcional, excluir a proposta ou lance que possa comprometer, restringir ou frustrar o caráter competitivo do processo licitatório, mediante comunicação automática via sistema.

4.7.1. Eventual exclusão de proposta do licitante implica retirada do certame, sem prejuízo do direito de defesa.

4.8. Durante a sessão pública, os licitantes serão informados, em tempo real, do valor do melhor lance registrado, vedada a identificação do licitante.

4.9. Na formulação de lances, deverão ser observados os seguintes aspectos:

a) os licitantes poderão oferecer lances sucessivos, observados o horário fixado para abertura da sessão e as regras estabelecidas neste edital;

b) não serão aceitos dois ou mais lances iguais, prevalecendo aquele que for recebido e registrado primeiro;

c) embora a classificação final seja pelo valor total do grupo, a disputa será por item. A cada lance, o sistema atualizará automaticamente o valor total.



Poder Judiciário

Conselho Nacional de Justiça

4.10. Os lances apresentados e levados em consideração para efeito de julgamento serão de exclusiva e total responsabilidade do licitante, não lhe cabendo o direito de pleitear qualquer alteração.

4.11. Será adotado para o envio de lances o modo de disputa “aberto e fechado”, em que os licitantes apresentarão lances públicos e sucessivos, com lance final fechado, conforme o critério de julgamento adotado neste edital.

4.12. No modo de disputa aberto e fechado, a etapa de envio de lances da sessão pública terá duração de **15 minutos**.

4.13. Ao fim do prazo de 15 minutos, o sistema avisará o fechamento iminente dos lances e, após período de **até 10 minutos** aleatoriamente determinado, a recepção de lances se encerra automaticamente, dando fim à etapa aberta.

4.14. Encerrada a etapa de lances, o sistema permitirá que o autor da oferta de valor mais baixo ou de maior percentual de desconto e os autores das ofertas com valores até 10% superiores ou inferiores, conforme o critério adotado, ofertem um lance final e fechado em **até 5 minutos**, que será sigiloso até o fim do prazo.

4.15. O licitante poderá manter o último lance da etapa aberta ou ofertar melhor lance.

4.16. Na ausência de, no mínimo, três ofertas na etapa fechada na margem dos 10%, o sistema permitirá aos autores dos melhores lances subsequentes na ordem de classificação, até o máximo de três, ofertar um lance final e fechado em **até 5 minutos**, que será sigiloso até o encerramento do prazo.

4.17. Encerrados os prazos, o sistema ordenará os lances em ordem crescente quando adotado o critério de julgamento por menor preço, ou decrescente quando adotado o por maior desconto.

4.18. Caso o sistema desconecte para o pregoeiro durante a fase competitiva e siga acessível aos licitantes, os lances continuarão a ser recebidos, sem prejuízo dos atos realizados.



Poder Judiciário

Conselho Nacional de Justiça

4.19. Se a desconexão persistir por mais de **10 minutos**, a sessão pública será suspensa e somente reiniciada **24 horas** após a comunicação do fato aos participantes no sítio eletrônico utilizado para divulgação.

4.20. Caso não envie lance, o licitante concorrerá com o valor da proposta.

SEÇÃO V – DOS CRITÉRIOS DE DESEMPATE

5.1. Em itens não exclusivos para MEs e EPPs, ao fim da etapa de lances, o porte da entidade empresarial será verificado automaticamente junto à Receita Federal. O sistema identificará em coluna própria as MEs e EPPs, comparando com os valores da primeira colocada, se esta for empresa de maior porte, assim como das demais classificadas, para fins de aplicação dos arts. 44 e 45 da Lei Complementar n. 123/2006, regulamentada pelo Decreto n. 8.538/2015.

5.2. Nessas condições, consideram-se empatadas com a primeira colocada as propostas de MEs e EPPs com valor até 5% acima do melhor lance ou proposta.

5.3. A mais bem classificada nos termos do subitem anterior terá direito de enviar uma oferta final para desempate, obrigatoriamente em valor inferior ao da primeira colocada, no prazo de 5 (cinco) minutos controlados pelo sistema, contados após comunicação automática para tanto.

5.4. Caso a ME ou EPP mais bem classificada desista ou não se manifeste no prazo, serão convocadas as demais licitantes ME e EPP que estejam naquele intervalo de 5% (cinco por cento), na ordem de classificação, para exercer o mesmo direito, no prazo do subitem anterior.

5.6. 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.

5.7. Em caso de empate entre duas ou mais propostas, serão utilizados os critérios de desempate previstos no art. 60 da Lei n. 14.133/2021, nesta ordem:



Poder Judiciário

Conselho Nacional de Justiça

I - disputa final, hipótese em que os licitantes empatados poderão apresentar nova proposta em ato contínuo à classificação;

II - avaliação do desempenho contratual prévio das licitantes, para a qual deverão preferencialmente ser utilizados registros cadastrais para efeito de atesto de cumprimento de obrigações previstas;

III - desenvolvimento pelo licitante de ações de equidade entre homens e mulheres no ambiente de trabalho, conforme regulamento;

IV - desenvolvimento pelo licitante de programa de integridade, conforme orientações dos órgãos de controle.

5.8. Persistindo o empate, será assegurada preferência, sucessivamente, aos bens e serviços produzidos ou prestados por empresas:

- a) estabelecidas no território do estado ou do Distrito Federal do órgão ou entidade da Administração Pública estadual ou distrital licitante ou, no caso de licitação realizada por órgão ou entidade de município, no território do estado em que este se localize;
- b) brasileiras;
- c) que invistam em pesquisa e no desenvolvimento de tecnologia no país;
- d) que comprovem a prática de mitigação, nos termos da Lei n. 12.187/2009.

SEÇÃO VI – DA CONFORMIDADE, DA ORDENAÇÃO E DA CLASSIFICAÇÃO DAS PROPOSTAS

6.1. Encerrada a etapa de envio de lances da sessão pública, o pregoeiro verificará a conformidade da proposta classificada em primeiro lugar quanto à adequação ao objeto estipulado e à compatibilidade do preço ou maior desconto final em relação ao estimado para a contratação, como definido no edital.

6.2. O licitante terá prazo de **3 (três) horas**, contado da solicitação do pregoeiro e prorrogável por igual período, para enviar proposta adequada ao último



Poder Judiciário

Conselho Nacional de Justiça

lance ofertado e, se for o caso, documentos complementares necessários à confirmação daqueles exigidos no edital.

6.3. A prorrogação poderá ocorrer nas seguintes situações:

I - por solicitação do licitante, mediante justificativa aceita pelo pregoeiro, ou

II - de ofício, a critério do pregoeiro, quando constatado que o prazo estabelecido não é suficiente para envio dos documentos exigidos no edital para a verificação de conformidade de que trata essa seção.

6.4. O pregoeiro, durante as fases de julgamento das propostas e/ou habilitação, poderá, em diligência, solicitar, mediante decisão fundamentada, registrada em ata e acessível aos licitantes, a juntada de documentos que apenas venham a atestar condição pré-existente à abertura da sessão pública.

SEÇÃO VII – DA NEGOCIAÇÃO E DO JULGAMENTO DA PROPOSTA

7.1. Caso a proposta do primeiro colocado permaneça acima do preço máximo ou inferior ao desconto definido para a contratação, o pregoeiro poderá negociar condições mais vantajosas, após definido o resultado do julgamento.

7.2. A negociação será realizada por meio do sistema e poderá ser acompanhada pelos demais licitantes.

7.3. Quando o primeiro colocado, mesmo após a negociação, for desclassificado em razão de sua proposta permanecer acima do preço máximo ou inferior ao desconto definido para a contratação, a negociação poderá ser feita com os demais licitantes classificados, exclusivamente por meio do sistema, respeitada a ordem de classificação, ou, em caso de propostas intermediárias empatadas, serão utilizados os critérios de desempate definidos neste edital.



Poder Judiciário

Conselho Nacional de Justiça

7.4. Concluída a negociação, se houver, o resultado será registrado na ata da sessão pública, devendo esta ser anexada aos autos do processo de contratação.

7.5. Encerrada a etapa de negociação, o pregoeiro verificará se o licitante provisoriamente classificado em primeiro lugar atende às condições de participação no certame, conforme previsto no art. 14 da Lei n. 14.133/2021, legislação correlata e neste edital, especialmente quanto à existência de sanção que impeça participação no certame ou futura contratação, mediante a consulta aos seguintes cadastros:

- a) Sistema de Cadastramento Unificado de Fornecedores (SICAF);
- b) Cadastro Nacional de Empresas Inidôneas e Suspensas (CEIS):
<https://www.portalttransparencia.gov.br/sancoes/ceis>; e
- c) Cadastro Nacional de Empresas Punidas (CNEP):
<https://www.portalttransparencia.gov.br/sancoes/cnep>.

7.6. A consulta aos cadastros será realizada em nome do licitante e do sócio majoritário, por força da vedação de que trata o art. 12 da Lei n. 8.429/1992.

7.7. Caso conste na Consulta de Situação do licitante a existência de ocorrências impeditivas indiretas, o pregoeiro diligenciará para verificar se houve fraude por parte das empresas apontadas no Relatório de Ocorrências Impeditivas Indiretas.

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

7.7.2. O licitante será convocado para manifestação previamente a uma eventual desclassificação.

7.7.3. Constatada a existência de sanção, o licitante será reputado inabilitado, por falta de condição de participação.

7.8. Atendidas as condições de participação, inicia-se o procedimento de habilitação.



Poder Judiciário

Conselho Nacional de Justiça

7.9. Observado o prazo de que trata o item 6.2, o pregoeiro deverá solicitar, no sistema, o envio da proposta adequada ao último lance ofertado após a negociação e, se necessário, dos documentos complementares.

7.10. Será desclassificada a proposta vencedora que:

- a) conter vícios insanáveis;
- b) desobedecer às especificações técnicas contidas no TR;
- c) apresentar preços inexequíveis ou acima máximo definido para a contratação;
- d) não tiver exequibilidade demonstrada, quando exigido pela Administração;
- e) apresentar desconformidade com quaisquer outras exigências deste edital ou seus anexos, desde que insanável.

7.11. Será considerado indício de inexequibilidade das propostas valores inferiores a 50% (cinquenta por cento) do valor orçado pela Administração para bens e serviços em geral. Nessa hipótese, só será considerada inexequível após diligência do pregoeiro, que comprove que:

- a) o custo do licitante ultrapassa o valor da proposta; e
- b) inexistem custos de oportunidade aptos a justificar o vulto da oferta.

7.12. Se houver indícios de inexequibilidade da proposta ou se necessários esclarecimentos adicionais, poderão ser efetuadas diligências para que a empresa comprove a exequibilidade.

7.13. Erros no preenchimento da planilha não constituem razão para desclassificar a proposta. O fornecedor poderá ajustar a planilha no prazo indicado pelo sistema, desde que não eleve o preço.

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



Poder Judiciário

Conselho Nacional de Justiça

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

7.14. Caso exija-se amostra, o licitante classificado em primeiro lugar deverá apresentá-la como disposto no TR, sob pena de rejeição da proposta.

7.15. Se a proposta classificada em primeiro lugar não for aceitável ou se o licitante não atender às exigências habilitatórias, o pregoeiro examinará a subsequente e, assim, sucessivamente, na ordem de classificação, até a apuração de proposta que atenda aos requisitos.

7.16. Será declarado vencedor o licitante que, atendidas as demais exigências fixadas neste edital, apresentar o **menor valor para o item/grupo, observado o valor unitário máximo constante da Estimativa de Preços do Anexo II deste edital.**

SEÇÃO VIII – DA FASE DE HABILITAÇÃO

8.1. Os documentos para habilitação, relativos a estabelecimento matriz e filiais que a critério da mesma pessoa jurídica licitante serão responsáveis pela execução do objeto, serão os seguintes:

Habilitação jurídica

- a) registro comercial, no caso de empresário individual;
- b) 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 dos administradores e alterações ou da consolidação respectiva;

Regularidade fiscal e trabalhista

- c) comprovante de inscrição no Cadastro Nacional da Pessoa Jurídica (CNPJ);



Poder Judiciário

Conselho Nacional de Justiça

d) comprovante de inscrição no cadastro de contribuintes estadual ou municipal, se houver, relativo ao domicílio ou à sede do licitante, pertinente ao ramo de atividade e compatível com o objeto deste edital;

e) prova de regularidade perante a Fazenda federal, estadual ou municipal do domicílio ou sede do licitante, ou outra equivalente, na forma da lei;

f) prova de regularidade relativa à Seguridade Social;

g) Certificado de Regularidade do FGTS (CRF), emitido pela Caixa Econômica Federal que ateste cumprimento dos encargos sociais instituídos por lei;

h) Certidão Negativa de Débitos Trabalhistas (CNDT), emitida pela Justiça do Trabalho;

Qualificação econômico-financeira

i) Certidão negativa de feitos sobre falência expedida pelo distribuidor da sede do licitante;

j) Certidão negativa de insolvência civil, no caso de pessoa física;

k) Balanço patrimonial, demonstração de resultado de exercício e demais demonstrações contábeis dos 2 (dois) últimos exercícios sociais;

k.1) Os documentos referidos acima limitar-se-ão ao último exercício no caso de a pessoa jurídica ter sido constituída há menos de 2 (dois) anos;

l) Patrimônio líquido no valor mínimo de R\$ 1.711.737,22 (um milhão, setecentos e onze mil, setecentos e trinta e sete reais e vinte e dois centavos), correspondentes a 10% (dez por cento) do valor total estimado para a contratação;

m) caso o balanço patrimonial apresente alguma irregularidade ou, mesmo regular, apresente índices de LG, SG e LC menores que 1 (um), poderá ser exigida declaração, assinada por profissional habilitado da área contábil, que ateste o atendimento pelo licitante dos índices econômicos previstos neste edital.



Poder Judiciário

Conselho Nacional de Justiça

Qualificação técnica

n) Atestado(s) de Capacidade Técnica Operacional, fornecido por pessoa jurídica de direito público ou privado, que comprove que o licitante tenha executado serviços de características técnicas semelhantes ao objeto desta contratação nos termos da Lei, comprovando:

n.1) Grupo 1 – Item 1:

n.1.1) Experiência na prestação de serviços de proteção de tráfego de borda, incluindo a administração de solução de Firewall, UTM ou NGFW, em ambiente com, no mínimo, 1000 ativos;

n.1.2) Experiência na prestação de serviços de administração de solução de proteção de endpoints (antivírus, EDR ou equivalente), em ambiente com, no mínimo, 1000 endpoints;

n.1.3) Experiência na prestação de serviços de administração de solução de segurança para gateway de e-mail, contemplando proteção antimalware e anti-spam em ambiente computacional com, no mínimo, 1000 caixas postais;

n.1.4) Experiência na prestação de serviços de administração de solução de WAF (Web Application Firewall), destinada à proteção de aplicações web, contemplando controle e mitigação de ataques a aplicações, em ambiente computacional compatível com aplicações críticas ou de missão institucional;

n.1.5) Experiência na prestação de serviços de administração de segurança nas soluções de segurança hospedadas em nuvem ou para a nuvem (tais como AWS, Azure, GCP ou equivalentes).

n.2) Grupo 1 – Item 2:

n.2.1) Experiência na prestação de serviços de gestão de vulnerabilidades, incluindo identificação, análise, priorização e tratamento das



Poder Judiciário

Conselho Nacional de Justiça

vulnerabilidades encontradas em ambientes com, no mínimo, 750 (setecentos e cinquenta) ativos;

n.2.2) Experiência na prestação de serviços de gerenciamento de patches, contemplando identificação, priorização, aplicação e validação de correções em ambientes com, no mínimo, 750 (setecentos e cinquenta) ativos

n.3) Grupo 1 – Item 3: Experiência na prestação de serviços de monitoramento proativo e resposta a incidentes de segurança da informação em ambientes com, no mínimo, 1000 (mil) ativos.

n.4) Grupo 1 – Item 4:

n.4.1) 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, 1000 (mil) ativos ou volume mínimo de 1500 eventos por segundo (EPS).

n.4.2) Experiência na prestação de serviços de detecção e resposta a ameaças em rede (NDR ou equivalentes), contemplando monitoramento de tráfego, identificação de comportamentos anômalos e apoio à resposta a incidentes de segurança da informação.

n.4.3) Experiência na prestação de serviços de monitoramento de superfície de ataque externa, incluindo ativos expostos na internet e coleta e análise de informações em surface web, deep web e dark web, com identificação de riscos e comunicação de achados relevantes.

n.5) Grupo 1 – Item 5: Experiência na prestação de serviços de conscientização em segurança da informação, contemplando o planejamento, a execução e a avaliação de ações de capacitação para, no mínimo, 500 (quinhentos) usuários, admitindo-se o uso de plataformas automatizadas, desde que a licitante comprove sua atuação na execução, gestão e acompanhamento das ações.



Poder Judiciário

Conselho Nacional de Justiça

n.6) Item 6: Experiência na prestação de serviços de testes de invasão (pentest) para exploração de vulnerabilidades de segurança da informação, em conformidade com boas práticas reconhecidas de mercado, tais como OWASP, NIST, PTES ou equivalentes.

n.7) Para fins de habilitação nos itens do Grupo 1 (Itens 1 a 5), a licitante deverá comprovar possuir, no mínimo, uma certificação vigente relacionada à gestão de serviços ou à segurança da informação, emitida por organismo de certificação acreditado, tais como:

n.7.1) ISO/IEC 27001;

n.7.2) ISO/IEC 20000;

n.7.3) ISO 9001.

n.8) Entende-se por similar, soluções ou produtos (equipamentos ou softwares) com funcionalidades equivalentes, escalabilidade compatível e porte corporativo aos listados no ANEXO B – PLATAFORMA DE SEGURANÇA.

n.9) 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.

n.10) Será permitido o somatório de atestados para comprovação da capacidade técnica, desde que os serviços sejam compatíveis com o objeto da contratação.

n.11) O CONTRATANTE poderá diligenciar a pessoa jurídica indicada no Atestado de Capacidade Técnica, visando validar ou esclarecer informações sobre o serviço prestado

8.2. Declarações extraídas do SICAF substituirão os documentos listados nas alíneas 'a', 'b', 'c', 'd', 'e', 'f', 'g', 'h' do item 8.1, para fins de habilitação do licitante cadastrado naquele sistema. Tais declarações serão válidas se:



Poder Judiciário

Conselho Nacional de Justiça

a) as informações relativas àqueles documentos estiverem disponíveis para consulta na data da sessão de recebimento da proposta e da documentação; e

b) estiverem dentro dos respectivos prazos de validade.

8.3. Caso conste documento com prazo de validade vencido, o licitante deverá encaminhar comprovante idêntico, com o prazo atualizado, no mesmo decurso estipulado no item 6.2 sob pena de inabilitação.

8.4. Quando a certidão for emitida com prazo de validade indeterminado ou o prazo de validade da certidão não estiver nela expresso, aquela expedida nos 60 (sessenta) dias anteriores à data da sessão deste certame será considerada válida, exceto se norma (lei, resolução, instrução normativa, portaria etc.) fixar prazo de validade inferior, hipótese na qual prevalecerá o prazo ali previsto. Os prazos aqui referidos serão contados a partir da data de emissão.

8.5. As MEs, EPPs e sociedades cooperativas (apenas as enquadradas no art. 34 da Lei n. 11.488/2007) deverão apresentar a documentação exigida para comprovação de regularidade fiscal mesmo que esta apresente alguma restrição.

8.6. Havendo alguma restrição na comprovação da regularidade fiscal das MEs e EPPs que atendam os requisitos do art. 4º da Lei n. 14.133/2021, ou sociedades cooperativas (apenas as enquadradas no art. 34 da Lei n. 11.488/2007), será assegurado prazo de 5 (cinco) dias úteis, prorrogável por igual período, a critério do pregoeiro, a contar do momento em que se declarar o vencedor do certame, para regularizar a documentação, pagar ou parcelar o débito, e emitir eventuais certidões negativas ou positivas com efeito de certidão negativa.

8.7. A não regularização da documentação, no prazo previsto no item acima, implica decadência do direito à contratação, sem prejuízo das sanções legais.

8.8. No caso de empresas estrangeiras participantes da licitação que não funcionem no Brasil, as exigências de habilitação serão atendidas mediante documentos equivalentes, conforme regulamento emitido pelo Executivo Federal.



Poder Judiciário

Conselho Nacional de Justiça

8.9. Após a entrega dos documentos para habilitação, não será permitido substituir ou apresentar novos documentos, salvo em sede de diligência para:

a) complementar informações acerca dos documentos já apresentados pelos licitantes, desde que necessárias para apurar fatos existentes à época da abertura do certame;

b) atualizar documentos cuja validade tenha expirado após a data de recebimento das propostas.

8.9.1. Não se consideram novos os documentos e informações que possam ser obtidos em consulta gratuita, aberta a qualquer interessado, a bases de dados de órgãos ou entes públicos, privados ou de caráter público, disponíveis na internet.

8.10. Na análise dos documentos de habilitação, a comissão de licitação poderá sanar erros ou falhas que não alterem a substância e a validade jurídica dos documentos, mediante despacho fundamentado registrado e acessível a todos, atribuindo-lhes eficácia para fins de habilitação e classificação.

8.11. Se necessário suspender a sessão pública para realizar diligências, com vistas ao saneamento tratado no item acima, a sessão somente poderá ser reiniciada mediante aviso prévio no sistema com antecedência mínima de **24 (vinte e quatro) horas**. A ocorrência será registrada em ata.

8.12. O pregoeiro ou autoridade superior poderão subsidiar-se em pareceres emitidos por técnicos ou especialistas no objeto desta licitação.

SEÇÃO IX – DOS RECURSOS

9.1. Declarado o vencedor, qualquer licitante poderá, durante o prazo concedido na sessão pública, não inferior a 10 (dez) minutos, de forma imediata após o fim do julgamento das propostas e do ato de habilitação ou inabilitação, em campo próprio do sistema, manifestar intenção de recorrer, sob pena de preclusão, ficando a autoridade superior autorizada a adjudicar o objeto ao licitante declarado vencedor.



Poder Judiciário

Conselho Nacional de Justiça

9.2. A falta de manifestação imediata do licitante implicará decadência do direito de recurso e o pregoeiro estará autorizado a adjudicar o objeto ao licitante declarado vencedor.

9.3. A recorrente deverá apresentar as razões do recurso no prazo de **3 (três) dias úteis** contados da data de intimação ou de lavratura da ata de habilitação ou inabilitação, ficando os demais licitantes, desde logo, intimados a apresentar contrarrazões em igual prazo, contado da data de intimação pessoal ou de divulgação da interposição do recurso, sendo-lhes assegurada vista imediata dos elementos indispensáveis à defesa dos seus interesses.

9.4. Recursos interpostos fora do prazo não serão conhecidos.

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

9.6. Os autos do processo seguirão com vista franqueada aos interessados.

SEÇÃO X – DA ADJUDICAÇÃO E DA HOMOLOGAÇÃO

10.1. Encerradas as fases de julgamento e habilitação, e exauridos os recursos administrativos, o processo licitatório será encaminhado à autoridade competente: o Diretor-Geral ou o Secretário de Administração, conforme o caso.

SEÇÃO XI – DAS OBRIGAÇÕES DA ADJUDICATÁRIA

11.1. A adjudicatária ficará obrigada a:

a) assinar o contrato no prazo de 5 (cinco) dias úteis contados da notificação, prorrogável uma única vez, por igual período, a critério da Administração;

b) executar o objeto, observadas as condições estipuladas neste edital, em seus anexos, na proposta e no contrato;

c) apresentar, caso seja optante do Simples Nacional, no ato da assinatura do contrato, declaração em conformidade com o Art. 6º da Instrução



Poder Judiciário

Conselho Nacional de Justiça

Normativa SRF n. 1.234/2012;

c.1) caso não seja apresentada a declaração prevista na alínea acima, serão retidos todos os tributos e contribuições no pagamento a ser efetuado;

d) apresentar, no prazo de 2 (dois) dias úteis contados da solicitação do CNJ, os originais necessários à aceitação da proposta e à habilitação da empresa.

e) prestar garantia conforme disposto neste edital.

11.2. Decorrido o prazo de validade das propostas, de **60 (sessenta) dias corridos**, sem convocação para assinatura do contrato, ficam os licitantes liberados dos compromissos assumidos.

11.3. A recusa injustificada da adjudicatária em assinar o contrato ou em aceitar ou retirar o instrumento equivalente no prazo estabelecido pela Administração caracterizará o descumprimento total da obrigação assumida e a sujeitará às penalidades legalmente estabelecidas e à imediata perda da garantia de proposta em favor do órgão ou entidade licitante.

11.4 O disposto no item acima não será aplicado aos licitantes remanescentes convocadas na forma do inciso I, § 4º, art. 90 da Lei n. 14.133/2021.

SEÇÃO XII – DAS SANÇÕES

12.1. Sujeitam-se às penalidades previstas na Lei n. 12.846/2013 aqueles que cometerem atos lesivos à administração pública no tocante a licitações e contratos, assim definidos:

a) frustrar ou fraudar, mediante ajuste, combinação ou qualquer outro expediente, o caráter competitivo de procedimento licitatório público;

b) impedir, perturbar ou fraudar a realização de qualquer ato de procedimento licitatório público;

c) afastar ou procurar afastar licitante, por meio de fraude ou oferecimento de vantagem de qualquer tipo;



Poder Judiciário

Conselho Nacional de Justiça

- d) fraudar licitação pública ou contrato dela decorrente;
- e) criar, de modo fraudulento ou irregular, pessoa jurídica para participar de licitação pública ou celebrar contrato administrativo;
- f) obter vantagem ou benefício indevido, de modo fraudulento, de modificações ou prorrogações de contratos celebrados com a administração pública, sem autorização em lei, no ato convocatório da licitação pública ou nos respectivos instrumentos contratuais;
- g) manipular ou fraudar o equilíbrio econômico-financeiro dos contratos celebrados com a administração pública.

12.2. Nos termos dos arts. 155, 156 e 162 da Lei n. 14.133/2021 e da Instrução Normativa CNJ n. 94/2023, após regular procedimento de apuração, a penalidade será aplicada conforme a dosimetria a seguir, sem prejuízo das multas previstas no TR e demais sanções legais, assegurada prévia e ampla defesa:

Ocorrência	Penalidade
a) Dar causa a inexecução parcial do objeto;	<i>Advertência, quando não se justificar a imposição de penalidade mais grave.</i>
b) Dar causa à inexecução parcial do objeto que cause grave dano à Administração, ao funcionamento dos serviços públicos ou ao interesse coletivo;	<i>Impedimento de licitar e contratar no âmbito da União pelo período de 6 (seis) meses a 2 (dois) anos, quando não se justificar a imposição de penalidade mais grave.</i>
c) Dar causa à inexecução total do objeto;	<i>Impedimento de licitar e contratar no âmbito da União pelo período de 1 um) ano a 3 (três) anos, quando não se</i>



Poder Judiciário

Conselho Nacional de Justiça

	<i>justificar a imposição de penalidade mais grave.</i>
d) Deixar de entregar documentação exigida para o certame;	<i>Impedimento de licitar e contratar no âmbito da União pelo período de 15 (quinze) dias a 6 (seis) meses, quando não se justificar a imposição de penalidade mais grave.</i>
e) Não manter a proposta, salvo em decorrência de fato superveniente devidamente justificado;	<i>Impedimento de licitar e contratar no âmbito da União pelo período de 15 (quinze) dias a 1 (um) ano, quando não se justificar a imposição de penalidade mais grave.</i>
f) Não celebrar a ata de registro de preços ou não entregar a documentação exigida para a contratação quando convocado dentro do prazo de validade de sua proposta;	<i>Impedimento de licitar e contratar no âmbito da União pelo período de 3 (três) meses a 2 (dois) anos, quando não se justificar a imposição de penalidade mais grave.</i>
g) Ensejar o retardamento da execução do objeto ou da entrega do objeto da licitação sem motivo justificado;	<i>Impedimento de licitar e contratar no âmbito da União pelo período de 3 (três) meses a 1 (um) ano e 6 (seis) meses, quando não se justificar a imposição de penalidade mais grave.</i>
h) Apresentar declaração ou documentação falsa exigida para o certame ou durante a licitação ou a execução do objeto;	<i>Declaração de inidoneidade para licitar ou contratar pelo período de 3 (três) a 6 (seis) anos.</i>



Poder Judiciário

Conselho Nacional de Justiça

i) Fraudar a licitação ou praticar ato fraudulento na execução do objeto;	<i>Declaração de inidoneidade para licitar ou contratar pelo período de 3 (três) a 6 (seis) anos.</i>
j) Comportar-se de modo inidôneo ou cometer fraude de qualquer natureza;	<i>Declaração de inidoneidade para licitar ou contratar pelo período de 3 (três) a 6 (seis) anos.</i>
k) Praticar atos ilícitos com vistas a frustrar os objetivos da licitação;	<i>Declaração de inidoneidade para licitar ou contratar pelo período de 3 (três) a 6 (seis) anos.</i>
l) Praticar ato lesivo previsto no art. 5º da Lei n. 12.846/ 2013.	<i>Declaração de inidoneidade para licitar ou contratar pelo período de 3 (três) a 6 (seis) anos.</i>

12.3. Nas condutas previstas nas letras “b”, “c”, “d”, “e”, “f” e “g” do item 12.2, quando justificada a imposição de penalidade mais grave, será aplicada a sanção de declaração de inidoneidade para licitar e contratar, que impedirá o responsável de licitar ou contratar no âmbito da Administração Pública direta e indireta de todos os entes federativos, pelo prazo mínimo de 3 (três) anos e máximo de 6 (seis) anos.

12.4. Quando a ação ou omissão ensejar a prática de mais de uma infração, será aplicada a mais grave das penas cabíveis ou, se iguais, somente uma delas, mas aumentada, em qualquer caso, de 1/3 até metade, justificadamente, em decorrência da gravidade da conduta.

12.4.1. A penalidade resultante da aplicação do item anterior não poderá ser maior do que as penalidades consideradas cumulativamente.

12.5. Às condutas praticadas durante o procedimento licitatório cujo valor estimado da contratação supere R\$ 500.000,00 (quinhentos mil reais) poderá ser



Poder Judiciário

Conselho Nacional de Justiça

cumulativamente aplicada a penalidade de multa no percentual de 1% (um por cento) do valor estimado da licitação.

12.6. A multa, calculada na forma do Anexo I (Termo de Referência), não poderá ser inferior a 0,5% (cinco décimos por cento) nem superior a 30% (trinta por cento) do valor do contrato licitado ou celebrado com contratação direta e será aplicada ao responsável por qualquer das infrações administrativas previstas no art. 155 da Lei n. 14.133/2021.

12.7. Se a multa aplicada e as indenizações cabíveis forem superiores ao valor de pagamento devido pela Administração à contratada, além da perda desse valor, a diferença será descontada da garantia prestada ou cobrada judicialmente.

12.7.1. Se a garantia contratual exigida for prestada por seguradora, esta será notificada da abertura de processo de apuração de responsabilidade de que possa resultar na aplicação da penalidade de multa à contratada.

12.8 O licitante ou contratado será notificado para apresentar defesa prévia no prazo de 15 (quinze) dias úteis a contar do recebimento da notificação. Da decisão que aplicar as sanções de advertência, multa e impedimento de licitar e contratar, caberá recurso administrativo, no mesmo prazo, a contar da intimação do ato.

12.9. A aplicação das sanções previstas neste edital não exclui, em hipótese alguma, a obrigação de reparação integral do dano causado à Administração.

12.10. A aplicação das sanções de impedimento de licitar e contratar e declaração de inidoneidade para licitar ou contratar, cumuladas ou não com multa, requererá a instauração de processo de responsabilização, a ser conduzido por comissão composta de no mínimo 2 (dois) servidores estáveis, que avaliará fatos e circunstâncias conhecidos e intimará o licitante ou o contratado para, no prazo de 15 (quinze) dias úteis contado da data de intimação, apresentar defesa escrita e especificar as provas que pretenda produzir.



Poder Judiciário

Conselho Nacional de Justiça

12.10.1. Deferido pedido de produção de novas provas ou de juntada de provas julgadas indispensáveis pela comissão, o licitante ou contratado poderá apresentar alegações finais no prazo de 15 (quinze) dias úteis contado da data da intimação.

12.11. Serão indeferidas pela comissão, mediante decisão fundamentada, provas ilícitas, impertinentes, desnecessárias, protelatórias ou intempestivas.

12.12. A prescrição da pretensão de aplicação das sanções ocorrerá em 5 (cinco) anos contados da ciência da infração pela Administração, e será interrompida e suspensa na forma da lei.

12.13. Excepcionalmente, desde que justificado pelo gestor do contrato no processo administrativo, o CNJ poderá, *ad cautelam*, efetuar a retenção do valor da multa presumida, em conformidade com o instrumento convocatório, TR ou contrato, e instaurar de imediato o procedimento administrativo para apurar responsabilidade por descumprimento, que deverá ter tramitação prioritária.

12.14. Todas as penalidades serão registradas no CEIS e no CNEP no prazo máximo de 15 dias úteis contado da data de aplicação da sanção.

12.15. Provido recurso ou reconsiderada decisão, os autos serão remetidos à Secretaria de Orçamento e Finanças para devolução à contratada dos valores eventualmente retidos.

12.16. Os instrumentos de requerimentos, de defesas prévias e de recursos eventualmente interpostos pelos licitantes, adjudicatários ou quaisquer interessados deverão ser instruídos com documentos aptos a provar as alegações neles contidas. Referidos documentos probatórios deverão ser apresentados em versão original ou versão conferida com o original por servidores da Administração Pública, sob pena de, a critério exclusivo do CNJ, não serem avaliados. Caso o fornecimento de cópias de documentos seja requerido ao CNJ, as despesas correspondentes deverão ser ressarcidas previamente em Guia de Recolhimento da União (GRU).



Poder Judiciário

Conselho Nacional de Justiça

SEÇÃO XIII – DO RECEBIMENTO

13.1. O objeto desta licitação será recebido observadas as condições e as especificações estabelecidas nos Anexos I e III do edital.

13.2. Constatadas outras inadequações, falhas ou incorreções na execução, fica a contratada obrigada a efetuar as correções necessárias, sem ônus para o CNJ.

13.3. O recebimento do objeto não exclui a responsabilidade civil, nem a ético-profissional pela perfeita execução do contrato, dentro dos limites legais.

13.4. Eventuais testes e demais provas para aferir a boa execução do objeto do contrato exigidos por normas técnicas oficiais correrão por conta da contratada.

SEÇÃO XIV – DO PAGAMENTO

14.1. O pagamento, observadas as condições estabelecidas nos Anexos I e III do edital, observará a ordem cronológica das fontes de recursos, no prazo de até 10 (dez) dias úteis contados da liquidação da despesa, nos termos da Instrução Normativa SEGES/ME n. 77/2022, desde que cumpridos os requisitos a seguir:

a) apresentação de nota fiscal conforme a legislação vigente à época da emissão (nota fiscal eletrônica, se for o caso), acompanhada da prova de regularidade junto às Fazendas Federal, Estadual e Municipal do domicílio ou sede da Contratada; da prova de regularidade junto à Seguridade Social; do CRF; e da CNDT;

b) inexistência de fato impeditivo para o qual tenha concorrido a contratada.

14.2. A contratada não poderá apresentar nota fiscal com número raiz do CNPJ diverso do registrado no preâmbulo do contrato.

14.3. A nota fiscal apresentada em desacordo com o estabelecido no edital, no contrato ou com qualquer circunstância que desaconselhe o pagamento será



Poder Judiciário

Conselho Nacional de Justiça

devolvida à contratada e, nesse caso, o prazo inicialmente fixado será interrompido e reiniciado a partir da respectiva regularização.

14.4. A nota fiscal apresentada em desacordo com o estabelecido na Ordem de Fornecimento poderá ser devolvida ao fornecedor, sendo garantido o pagamento da parcela incontroversa, sem prejuízo do reinício do prazo de pagamento a partir da regularização da parcela apresentada em desconformidade.

14.5. Os documentos de cobrança deverão ser entregues pela contratada no Protocolo do CNJ ou por e-mail, quando acordado com o gestor ou previsto no TR.

14.6. O pagamento será realizado apenas após o recebimento definitivo do objeto pelo CNJ, desde que não verificadas falhas na execução dos serviços, e os prazos inicialmente fixados serão contados a partir do recebimento definitivo.

14.7. No caso de controvérsia sobre a execução do objeto, quanto a dimensão, qualidade e quantidade, a parcela incontroversa deverá ser liberada no prazo previsto para pagamento.

14.8. A não manutenção das condições de habilitação pela contratada não ensejará a retenção de pagamento quando houver o atesto da efetiva e regular prestação dos serviços, mas poderá dar ensejo à extinção contratual, sem prejuízo das demais sanções cabíveis.

14.9. Ao longo da execução do contrato, a inclusão de estabelecimento integrante da pessoa jurídica no conjunto daqueles responsáveis pela execução do objeto poderá ocorrer, desde que mediante apresentação de documentos, referidos a todo o período de vigência já transcorrida do ajuste, hábeis à prova de regularidade do estabelecimento a ser acrescido junto à Fazenda Estadual/Distrital e Municipal, bem como de prévia formalização do acréscimo em termo aditivo ao contrato.

14.10. Não haverá pagamento antecipado, parcial ou total, relativo a parcelas contratuais vinculadas ao objeto, salvo para propiciar economia de recursos ou se representar condição indispensável à obtenção do bem ou à prestação do serviço,



Poder Judiciário

Conselho Nacional de Justiça

hipótese em que haverá obrigatoriamente justificativa técnica no processo licitatório e previsão neste edital.

SEÇÃO XVI – DOS RECURSOS ORÇAMENTÁRIOS

15.1 A despesa decorrente desta licitação correrá à conta de recursos do Orçamento Geral da União, Programa de Trabalho 02.032.0033.21BH.5664 - "Controle da atuação administrativa e financeira do Poder Judiciário, do cumprimento dos deveres funcionais dos juízes e Gestão de Políticas Judiciárias". Natureza da Despesa: 3.3.90.40.11.

SEÇÃO XVI – DA ATUALIZAÇÃO MONETÁRIA

16.1. Em caso de atraso no pagamento para o qual tal não tenha concorrido a contratada, incidirá atualização monetária sobre o valor devido pela variação acumulada do Índice de Custos de Tecnologia da Informação (ICTI) entre a data final prevista para o pagamento e a data da efetiva realização.

SEÇÃO XVII – DA ASSINATURA DO CONTRATO

17.1. Homologada a licitação, o CNJ convocará o licitante vencedor, durante a validade da sua proposta para assinatura, por meio eletrônico, do instrumento contratual, que se dará em até 5 (cinco) dias úteis, sob pena de decair o direito à contratação, sem prejuízo às sanções previstas neste edital.

17.1.1. O prazo de convocação poderá ser prorrogado 1 (uma) vez, por igual período, mediante solicitação da parte durante seu transcurso, devidamente justificada, e desde que o motivo apresentado seja aceito pela Administração.

17.2. Em caso de escolha da prestação de garantia na modalidade seguro-garantia pela contratada, o prazo para assinatura do contrato será de no mínimo um mês contado da homologação da licitação.



Poder Judiciário

Conselho Nacional de Justiça

17.3. Impreterivelmente dentro do prazo de 3 (três) dias úteis contados da data da convocação que lhe seja feita pelo CNJ, o licitante vencedor deverá requerer cadastro no Sistema Eletrônico de Informações (SEI) do CNJ, mediante observância da Instrução Normativa CNJ n. 67/2015.

17.4. O licitante vencedor deverá assinar o instrumento contratual por meio do SEI no prazo de 5 (cinco) dias úteis contados da convocação, sob as penas legais.

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

17.6. 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.

SEÇÃO XVIII– DA VIGÊNCIA DO CONTRATO

18.1. O contrato terá vigência de 60 (sessenta) meses a contar da sua assinatura, prorrogável nos termos da Lei.

18.2. A prorrogação de que trata este item é condicionada ao ateste, pela autoridade competente, de que as condições e os preços permanecem vantajosos para a Administração, permitida a negociação com o contratado.

18.3. Ressalta-se, que, de acordo com o inciso III, do art. 106, da Lei 14.133/2021, a Administração terá a opção de extinguir o contrato, sem ônus, quando não dispuser de créditos orçamentários para sua continuidade ou quando entender que o contrato não mais lhe oferece vantagem.

18.4. Para formalização da prorrogação do prazo de vigência, será verificada a regularidade fiscal da Contratada por meio de consulta ao Cadastro Nacional de Empresas Inidôneas e Suspensas (CEIS) e ao Cadastro Nacional de Empresas Punidas (CNEP), sem prejuízo da consulta de outros meios previstos na legislação.



Poder Judiciário

Conselho Nacional de Justiça

SEÇÃO XIX – DA GARANTIA CONTRATUAL

19.1. A contratada deverá apresentar garantia de 5% (cinco por cento) do valor anual do contrato em uma modalidade a seguir:

a) caução em dinheiro ou em títulos da dívida pública emitidos sob a forma escritural, mediante registro em sistema centralizado de liquidação e de custódia autorizado pelo Banco Central do Brasil (BCB), e avaliados por seus valores econômicos, conforme definido pelo Ministério da Economia;

b) seguro-garantia;

c) fiança bancária emitida por banco ou instituição financeira devidamente autorizada a operar no país pelo BCB;

d) título de capitalização custeado por pagamento único, com resgate pelo valor total.

19.2. O prazo para apresentação da garantia pela contratada nas modalidades caução ou fiança bancária será de **até 10 (dez) dias úteis** contados da publicação do extrato do contrato na Imprensa Oficial, prorrogáveis por igual período a critério da Administração.

19.3. O prazo para apresentação na modalidade seguro-garantia será de um mês contado da data de homologação da licitação e anterior à assinatura do contrato.

19.3.1. Após a homologação da licitação, o licitante terá prazo de 30 (trinta) dias corridos, prorrogável por igual período a critério da Administração, para enviar a comprovação do seguro-garantia e assinatura do contrato.

19.4. Quando a garantia for apresentada em dinheiro, ela será atualizada monetariamente, conforme os critérios estabelecidos pela instituição bancária em que for realizado o depósito.

19.5. Quando a garantia for apresentada na modalidade seguro-garantia, a apólice deverá:



Poder Judiciário

Conselho Nacional de Justiça

a) ser expedida exclusivamente por qualquer das entidades controladas e fiscalizadas pela Superintendência de Seguros Privados (SUSEP);

b) conter o número com que a apólice ou o endosso tenha sido registrado na SUSEP;

c) não estar integrada por cláusula compromissória nem por previsão de instauração de Juízo Arbitral; e

d) não poderá estabelecer franquias, participações obrigatórias do segurado (CNJ) e/ou prazo de carência.

19.6. Quando a garantia for apresentada na modalidade fiança bancária, o instrumento deverá ser expedido exclusivamente por entidade controlada e fiscalizada pelo BCB.

19.7. Quando a garantia for apresentada na modalidade fiança bancária, a instituição financeira fiadora deverá ser domiciliada ou possuir agência no Distrito Federal e demonstrar possuir bens suficientes à garantia integral da fiança prestada, conforme art. 825 da Lei n. 10.406/2002. A carta de fiança deverá conter cláusula expressa de renúncia do fiador ao benefício de ordem previsto no art. 827 da Lei n. 10.406/2002, conforme facultado pelo inciso I do art. 828 do mesmo diploma legal, e ser registrada no Registro de Títulos e Documentos, conforme previsto nos arts. 128, 129 e 130 da Lei n. 6.015/1973.

19.8. A garantia, em qualquer modalidade, assegurará o pagamento de:

a) prejuízos advindos do não cumprimento do objeto contratado e do não adimplemento das demais obrigações nele previstas;

b) prejuízos causados ao contratante, decorrentes de culpa ou dolo durante a execução do contrato;

c) multas moratórias e punitivas aplicadas pelo contratante à contratada;



Poder Judiciário

Conselho Nacional de Justiça

d) obrigações trabalhistas e previdenciárias de qualquer natureza, não adimplidas pela contratada, quando couber.

19.9. Alterado o valor do contrato, fica a contratada obrigada a apresentar garantia complementar ou substituí-la, nos mesmos percentuais e modalidades constantes desta seção, em **até 10 (dez) dias úteis** contados da publicação do termo de aditamento na Imprensa Oficial ou da assinatura da apostila de repactuação.

19.10. Prorrogada a vigência do contrato, fica a contratada obrigada a renovar a garantia, no mesmo percentual e modalidades constantes desta seção, em **até 10 (dez) dias úteis**, contados da publicação do termo aditivo na Imprensa Oficial.

19.11. A garantia apresentada em desacordo com os requisitos e coberturas previstas no contrato será devolvida à contratada, que disporá do prazo improrrogável de **10 (dez) dias úteis** para regularizar a pendência.

SEÇÃO XX – DO REAJUSTE

20.1. Após o interregno de um ano da data do orçamento estimado, e independentemente de pedido da contratada, os preços iniciais serão reajustados, mediante a aplicação, pelo contratante, do Índice de Custos de Tecnologia da Informação (ICTI), exclusivamente para as obrigações iniciadas e concluídas após a ocorrência da anualidade.

20.2. Para formalização da prorrogação do prazo de vigência, será verificada a regularidade fiscal da contratada por meio de consulta ao Cadastro Nacional de Empresas Inidôneas e Suspensas (CEIS) e ao Cadastro Nacional de Empresas Punidas (CNEP).

SEÇÃO XXI – DO ACOMPANHAMENTO E DA FISCALIZAÇÃO

21.1. O CNJ nomeará um gestor titular e um substituto para executar a fiscalização do contrato. As ocorrências e deficiências serão registradas em relatório, cuja cópia será enviada à contratada, objetivando a imediata correção das irregularidades apontadas.



Poder Judiciário

Conselho Nacional de Justiça

21.2. A contratada será responsável pelos danos causados diretamente ao CNJ ou a terceiros em razão da execução do contrato, e não excluirá nem reduzirá essa responsabilidade a fiscalização ou o acompanhamento pelo contratante.

21.3. Durante a vigência do contrato, é vedado à contratada contratar cônjuge, companheiro ou parente em linha reta, colateral ou por afinidade, até o terceiro grau, de dirigente do órgão ou entidade contratante ou de agente público que exerça função na licitação ou atue na fiscalização ou na gestão do contrato.

21.4. Somente a contratada será responsável pelos encargos trabalhistas, previdenciários, fiscais e comerciais resultantes da execução do contrato.

21.5. A inadimplência da contratada em relação aos encargos trabalhistas, fiscais e comerciais não transferirá ao CNJ a responsabilidade pelo seu pagamento e não poderá onerar o objeto do contrato.

SEÇÃO XXII – DA EXTINÇÃO DO CONTRATO

22.1. O inadimplemento de cláusula estabelecida neste edital ou no contrato, por parte da contratada, assegurará ao CNJ o direito de extinção, mediante notificação, com prova de recebimento.

22.2. Além de outras hipóteses expressamente previstas no art. 137 da Lei n. 14.133/2021, constituem motivos para a extinção do contrato:

a) não cumprimento ou cumprimento irregular de normas editalícias ou de cláusulas contratuais, de especificações, de projetos ou de prazos;

b) desatendimento das determinações regulares emitidas pela autoridade designada para acompanhar e fiscalizar sua execução ou por autoridade;

c) alteração social ou modificação da finalidade ou da estrutura da empresa que restrinja sua capacidade de concluir o contrato; e



Poder Judiciário

Conselho Nacional de Justiça

d) decretação de falência ou de insolvência civil, dissolução da sociedade ou falecimento do contratado.

22.3. Caso a contratada sofra fusão, cisão ou incorporação, será admitida a continuação do contrato, desde que a execução não seja afetada e que a contratada mantenha o fiel cumprimento dos termos contratuais e as condições de habilitação.

22.4. Ao CNJ é reconhecido o direito de extinção contratual unilateral, nos termos do art. 138, inciso I, da Lei n. 14.133/2021.

22.5. A extinção do contrato poderá ser consensual, por acordo entre as partes, por conciliação, por mediação ou por comitê de resolução de disputas, desde que haja interesse da Administração.

22.5.1. O contrato poderá ser rescindido antes do término acordado, mediante notificação à contratada com antecedência mínima de 30 (trinta) dias, em face da conclusão de procedimento licitatório contemplando o mesmo objeto.

22.6. A extinção poderá ser determinada por decisão arbitral, em decorrência de cláusula compromissória ou compromisso arbitral, ou por decisão judicial.

22.7. Os casos de extinção contratual serão formalmente motivados nos autos do processo, assegurado o contraditório e a ampla defesa.

SEÇÃO XXIII – DO PEDIDO DE ESCLARECIMENTO E DA IMPUGNAÇÃO

23.1. Qualquer interessado, antes de decidir participar do pregão, deverá providenciar exaustivo estudo do inteiro teor do edital e apresentar à CPC as dúvidas e impugnações (inclusive correlatas a eventuais irrazoabilidades, desproporcionalidades e/ou omissões) que entender existentes neste instrumento.

23.2. Ao participar desta licitação, o licitante declara-se ciente de que as condições editalícias, descrições de produtos, condições de fornecimento e outras fórmulas destinam-se a garantir, nos termos da lei, transparência, objetividade, certeza jurídica e isonomia a todos os participantes, bem como eficácia e celeridade ao processo seletivo do menor preço (ou maior desconto) e da melhor proposta.



Poder Judiciário

Conselho Nacional de Justiça

23.3. Qualquer pessoa é parte legítima para impugnar o edital por irregularidade na aplicação da lei ou para solicitar esclarecimento sobre os seus termos, devendo protocolar o pedido **até 3 (três) dias úteis antes da data de abertura do certame**, exclusivamente por meio do email cpc@cnj.jus.br.

23.4. A resposta a impugnação ou a pedido de esclarecimento será divulgada em sítio eletrônico oficial no prazo de até 3 (três) dias úteis, limitado ao último dia útil anterior à data da abertura do certame.

23.5. O pregoeiro poderá requisitar subsídios formais aos responsáveis pela elaboração do edital de licitação e dos anexos.

23.6. As respostas aos pedidos de esclarecimentos e impugnações serão divulgadas em sítio eletrônico oficial do órgão ou da entidade promotora da licitação e no sistema e vincularão os licitantes e o CNJ.

23.7. Impugnações e pedidos de esclarecimentos não suspendem os prazos previstos no certame.

23.8. Acolhida a impugnação ao ato convocatório, será designada nova data para a realização do certame.

SEÇÃO XXIV – DAS DISPOSIÇÕES FINAIS

24.1. O edital estará à disposição dos interessados na Comissão Permanente de Contratação (CPC), localizada no Ed. Sede do CNJ, SAF Sul, Quadra 2, Lotes 05/06, Bloco E, sala 003, CEP: 70070-600, Brasília/DF, nos dias úteis, das 12h às 19h, e na internet para *download*, nos endereços eletrônicos <https://www.gov.br/pncp/pt-br> e www.cnj.jus.br/transparencia.

24.2. O licitante poderá realizar vistoria técnica prévia para obter informações e condições necessárias à correta elaboração da proposta e execução dos serviços e conhecimento pleno das condições e peculiaridades do objeto. A vistoria poderá ser realizada **até o dia 18/06/2026**, das 12h às 19h, mediante agendamento prévio com a CPC pelo telefone **(61) 2326-5159**, devendo, ainda, ser observado o seguinte:



Poder Judiciário

Conselho Nacional de Justiça

a) ser realizada por profissional especialmente credenciado como representante do licitante;

b) em nenhuma hipótese o licitante poderá alegar desconhecimento, incompreensão, dúvida ou esquecimento de qualquer detalhe relativo à execução do objeto, arcando com quaisquer ônus disso decorrentes;

c) não se admitirá um mesmo profissional como representante de mais de um licitante;

d) dada a faculdade da vistoria prévia, os licitantes não poderão alegar desconhecer as condições e graus de dificuldade como justificativa para se eximir das obrigações assumidas ou em favor de eventuais pretensões de acréscimos de preços em decorrência da execução do objeto. Assim, **a vistoria poderá ser substituída por declaração formal** assinada pelo responsável técnico do licitante acerca do conhecimento pleno das condições e peculiaridades da contratação.

24.3. Todas as referências de tempo no edital, no aviso e durante a sessão pública, observarão obrigatoriamente o horário de Brasília /DF e serão assim registradas no sistema eletrônico e na documentação relativa ao certame.

24.4. Nenhuma indenização será devida aos licitantes pela elaboração de proposta ou apresentação de documentos relativos a esta licitação.

24.5. A indicação do lance vencedor, a classificação dos lances apresentados e demais informações relativas à sessão pública do pregão constarão de ata divulgada no sistema eletrônico.

24.6. Informações, pedidos de esclarecimentos e respostas a impugnações referentes a esta licitação estarão disponíveis no endereço **www.cnj.jus.br/transparencia**.

24.7. Compete exclusivamente aos licitantes, adjudicatários e demais interessados manter atualizados, junto ao CNJ, os respectivos endereços, inclusive eletrônicos (e-mail). O CNJ reserva-se o direito de considerar válidas comunicações



Poder Judiciário

Conselho Nacional de Justiça

enviadas a licitantes, adjudicatários e quaisquer outros interessados pelos endereços, inclusive eletrônicos, registrados nos autos ou no SICAF.

24.8. O pregoeiro poderá, no julgamento das propostas e da habilitação, sanar erros ou falhas que não alterem a substância e a validade jurídica dos documentos, mediante despacho fundamentado, registrado em ata e acessível a todos, e lhes atribuirá validade e eficácia para fins de habilitação e classificação, observado o disposto na Lei n. 9.784/1999.

24.9. As disposições deste edital serão interpretadas em favor da ampliação da disputa entre os interessados, resguardados o interesse da administração, o princípio da isonomia, a finalidade e a segurança da contratação.

24.10. Integram este edital, para todos os fins e efeitos, os seguintes anexos:

ANEXO I – Termo de Referência;

ANEXO II – Estimativa de preços;

ANEXO III – Minuta de Termo de Contrato.

24.11. Aplicam-se à presente licitação, subsidiariamente, as Leis n. 13.726/2018 e n. 10.406/2002, bem como as demais normas pertinentes.

Brasília, 03 de junho de 2026.

Bruno César de Oliveira Lopes

Diretor-Geral

Portaria n. 329/2025



Poder Judiciário

Conselho Nacional de Justiça

PREGÃO ELETRÔNICO N. 90012/2026

ANEXO I DO EDITAL - TERMO DE REFERÊNCIA

1. DO OBJETO

1.1. Definição do objeto

- 1.1.1. Contratação de Serviços Gerenciados de Segurança da Informação, de acordo com as especificações técnicas contidas neste Termo de Referência – TR e seus anexos.

1.2. Descrição detalhada do objeto

- 1.2.1. Serviços Gerenciados de Segurança da Informação é uma solução de serviços pela qual a empresa a ser contratada presta serviços de segurança, incluindo a administração e operação das ferramentas de segurança do ambiente do CNJ e de outras ferramentas a serem disponibilizadas pela contratada, descritos na tabela 01 a seguir, cujas especificações dos requisitos técnicos estão tratadas no ANEXO A – ESPECIFICAÇÃO DOS REQUISITOS TÉCNICOS do presente Termo de Referência, e envolvem:

Grupo	Item	Descrição	Catser	Unid.	Qtd.	Periodicidade/ Frequência
1	1	Serviço de administração, operação e manutenção e atendimento a requisições	27014	Mês	60	Rotineiro
	2	Serviço de gestão de vulnerabilidades	27014	Mês	60	Rotineiro
	3	Serviço de gestão de incidentes de segurança (CSIRT - <i>Blue Team</i>)	27014	Mês	60	Rotineiro
	4	Serviço de monitoramento e visibilidade de ataques cibernéticos	27014	Mês	60	Rotineiro
	5	Serviço de Conscientização em Segurança da Informação	27014	Mês	60	Rotineiro
Não agrupado	6	Serviço de testes de invasão (<i>Red Team</i>)	27014	Sistemas	80	Sob demanda

Tabela 1 – Objeto detalhado

- 1.2.2. Os Serviços Gerenciados de Segurança da Informação serão executados sem dedicação exclusiva de mão de obra e solicitados, mediante emissão de Ordem de Serviço (OS), SEM GARANTIA DE CONSUMO MÍNIMO.



Poder Judiciário

Conselho Nacional de Justiça

Os pagamentos dos serviços do grupo 01 serão efetuados mensalmente e o pagamento do serviço do item 6 não agrupado ocorrerá a qualquer tempo conforme quantidade de sistemas demandados.

- 1.2.3. O Serviço de administração, operação e manutenção e atendimento a requisições** (Grupo 01 - item 01) tem como objetivo sustentar e operar todas as soluções e produtos de segurança do CNJ, bem como a realização permanente de ações proativas (gap analysis) voltadas para a segurança do parque computacional do CNJ com o objetivo de mantê-lo estável, disponível e íntegro.
- 1.2.4. O Serviço de gestão de vulnerabilidades** (Grupo 01 - item 02) tem por objetivo, de forma proativa e recorrente, identificar possíveis vulnerabilidades de segurança da informação no ambiente e sistemas críticos do CNJ a fim de evitar que ataques cibernéticos obtenham sucesso explorando vulnerabilidades conhecidas.
- 1.2.5. O Serviço de gestão de incidentes de segurança (CSIRT - Blue Team)** (Grupo 01 - item 03) tem por objetivo 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.
- 1.2.6. O Serviço de monitoramento e visibilidade de ataques cibernéticos** (Grupo 01 - item 04) tem como objetivo o monitoramento contínuo e ininterrupto de ataques cibernéticos direcionados ao CNJ, 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.
- 1.2.7. O Serviço de Conscientização em Segurança da Informação** (Grupo 01 - item 05) tem como objetivo realizar ações educativas sobre boas práticas de proteção de dados, uso seguro de sistemas e prevenção a incidentes cibernéticos, incluindo a identificação proativa de usuários que seriam vetores de ataques e o desenvolvimento e a aplicação de campanhas, palestras, treinamentos e materiais informativos, com foco na mitigação de riscos humanos e na promoção de uma cultura organizacional de segurança da informação, em conformidade com as políticas internas e a legislação vigente.
- 1.2.8. Serviço de testes de invasão** (Grupo 02 - item 06) tem como objetivo principal identificar, mapear e documentar possíveis vulnerabilidades nos



Poder Judiciário

Conselho Nacional de Justiça

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. FUNDAMENTAÇÃO DA CONTRATAÇÃO

2.1. Motivação

- 2.1.1. Ao Departamento de Tecnologia da Informação, de acordo com o artigo 25 da Portaria 47 de 29 de novembro de 2017, dentre outros pontos, compete, implantar e gerenciar os controles relativos à gestão da segurança da informação para manter a confidencialidade, a integridade e a disponibilidade das informações e dos recursos de TIC.
- 2.1.2. Além disso, com base nas diretrizes definidas no Planejamento Estratégico do Conselho Nacional de Justiça (CNJ), aprovado pela Portaria nº 104 de 2020, vários investimentos em Tecnologia da Informação e Comunicação (TIC) estão sendo realizados para modernizar sua infraestrutura de TIC com a finalidade de alcançar os objetivos estratégicos estabelecidos, tais como, fomentar e incrementar a produção de soluções tecnológicas, com foco em inovação e transformação digital, aprimorar a governança e a gestão da tecnologia e comunicação sob a ótica de soluções colaborativas e garantir infraestrutura adequada ao funcionamento do CNJ.
- 2.1.3. A infraestrutura de TIC do CNJ dispõe de uma série de ativos heterogêneos agrupados em: rede de comunicação de dados, telefonia, banco de dados, servidores de rede, sistemas operacionais, sistemas de backup e recursos de armazenamento de dados que, dada a criticidade dos sistemas hospedados, deve operar em alta disponibilidade e resiliência a falhas. Por óbvio, a operação e sustentação dessa infraestrutura requer uma equipe técnica qualificada e igualmente diversificada, para tanto, o CNJ dispõe do Contrato 06/2024 que possui como objeto a prestação de serviços para suporte à infraestrutura e operações de tecnologia da informação e comunicação do Conselho Nacional de Justiça.
- 2.1.4. Buscando entregar serviços com adequado nível de qualidade e eficiência, a área de TI do CNJ investe no aprimoramento das práticas de



Poder Judiciário

Conselho Nacional de Justiça

gestão desse ambiente tecnológico com base em modelos de melhores práticas internacionalmente reconhecidos como ITIL® - composto por recomendações de boas práticas, organizadas por módulos de gerenciamento, a fim de otimizar processos de TI em organizações - e COBIT® - base de conhecimento mais reconhecida e utilizada no mercado para apoiar organizações na Governança de Tecnologia da Informação (TI) além de padrões ISO/IEC 20.000 - conjunto que define as boas práticas de gestão de serviços de TI. Relevante ainda citar a necessidade de aplicar recomendações e controles presentes em padrões internacionais afetos ao Sistema de Gestão da Segurança da Informação dentro do contexto da organização tais como a ISO/IEC 27001:2022 e ISO/IEC 27002:2022.

2.1.5. A infraestrutura de segurança atualmente implantada no CNJ é composta por diversas tecnologias heterogêneas de hardware e software, as quais fornecem serviços de segurança com o objetivo de proteger o ambiente computacional de TIC de ataques cibernéticos e outras ameaças externas e internas. Entre as tecnologias e soluções em uso, destacam-se:

- a. Solução de Firewall, Proxy/Web Filter, IPS/IDS, VPN e Gateway Web;
- b. Solução de Endpoint Detection and Response (EDR);
- c. Solução de Proteção de Aplicações Nativas em Nuvem (CNAPP);
- d. Solução de Security Information and Event Management (SIEM);
- e. Sistema Antispam;
- f. Solução de Web Application Firewall (WAF);
- g. Rede de entrega de conteúdo (CDN)
- h. Solução contra-ataque de Negação de Serviço Distribuído (DDoS);
- i. Sistema de Governança, Risco e Conformidade (GRC);
- j. Sistema de análise de vulnerabilidades de aplicações.



Poder Judiciário

Conselho Nacional de Justiça

- 2.1.6. O monitoramento e gerenciamento de segurança dessas diversas tecnologias requer profissionais altamente qualificados e com dedicação exclusiva para exercer suas atividades com uma maior eficácia e eficiência. A falta de recursos humanos compromete a detecção, resposta a incidentes e atividades de prevenção de ameaças.
- 2.1.7. Por outro lado, existe a dificuldade de contratar pessoal de segurança qualificado além de uma lista crescente de tecnologias de segurança que o CNJ necessita adquirir, gerenciar e operar para lidar com os novos cenários de ameaças. Além disso, há uma perspectiva se de obter um melhor retorno sobre os investimentos existentes e futuros em soluções de segurança ao se transferir sua operação e monitoração à especialistas experientes.
- 2.1.8. Além disso, a Resolução Nº 370 de 28/01/2021, que instituiu a Estratégia Nacional de Tecnologia da Informação e Comunicação do Poder Judiciário (ENTIC-JUD), em seu artigo 21, define que cada órgão, sempre que possível, deverá constituir e manter estruturas organizacionais adequadas e compatíveis de acordo com a demanda de TIC considerando, entre outros, o macroprocesso II – Segurança da Informação e Proteção de Dado, incluindo incidentes de segurança, riscos, continuidade de serviços essenciais e segurança dos serviços em nuvem.
- 2.1.9. O uso de serviços de segurança gerenciados (MSS) é uma abordagem cada vez mais popular para atingir as metas de segurança da informação, reduzir riscos e colmatar a lacuna de habilidades de segurança da organização e assim, aprimorar a qualidade e a percepção de entrega de valor dos serviços prestados pela Divisão de Segurança da Informação do Departamento de Tecnologia da Informação do CNJ.
- 2.1.10. Nesse contexto, O CNJ celebrou em 21/05/2021, com a empresa ISH Tecnologia S/A, o contrato nº. 08/2021 para prestação de serviços Gerenciados de Segurança da Informação, incluindo Serviços de Administração, Operação e Atendimento a Requisições, Gestão de Vulnerabilidades, Gestão de Incidentes, Monitoramento e Visibilidade de ataques Cibernéticos e Testes de Invasão de acordo com as especificações técnicas contidas neste Termo de Referência – TR e seus anexos, pelo período, inicial, de 24 (vinte e quatro) meses, podendo ser prorrogado nos termos da Lei n. 8.666/93.



Poder Judiciário

Conselho Nacional de Justiça

- 2.1.11. O procedimento licitatório que resultou na celebração do contrato foi o pregão eletrônico nº 03/2021, com fundamento legal Lei 10.520/2002, como consta do Processo Administrativo/CNJ/SEI nº 00131/2020.
- 2.1.12. Em 10/05/2023, O CNJ assinou o Terceiro Termo Aditivo ao contrato nº. 08/2021, prorrogando o prazo de vigência do contrato em 24 (vinte e quatro) meses, a contar de 21/05/2023 até 20/05/2025. Em 13/05/2025, O CNJ assinou o Quarto Termo Aditivo ao contrato nº. 08/2021, prorrogando o prazo de vigência do contrato em 12 (doze) meses, a contar de 21/05/2025 até 20/05/2026.
- 2.1.13. Com a proximidade do fim da vigência do Contrato nº. 08/2021, que ocorrerá em 20/05/2026, e de posse desses elementos informacionais preliminares, o presente documento tem como objetivo trazer os elementos capazes de subsidiar a decisão das áreas competentes deste CNJ quanto a necessidade de uma nova contratação de Serviços Gerenciados de Segurança (MSS) por um prazo de 60 (sessenta) meses.

2.2. Alinhamento Estratégico

- 2.2.1. A presente contratação encontra consonância com a Estratégia Nacional de Tecnologia da Informação e Comunicação do Poder Judiciário - ENTIC-JUD ([Resolução CNJ nº 370/2021](#)), por meio do “Objetivo 5 – Aperfeiçoar a Governança e a Gestão”, “Objetivo 7 – Aprimorar a Segurança da Informação e a Gestão de Dados” e “Objetivo 8 – Promover Serviços de Infraestrutura e Soluções Corporativas”.
- 2.2.2. Dentre os Objetivos Estratégicos estabelecidos na Estratégia Nacional de Segurança Cibernética do Poder Judiciário (ENSEC-PJ) conforme [Resolução nº 396, de 24/09/2021](#), encontra-se alinhamento com os seguintes objetivos: Objetivo II – aumentar a resiliência às ameaças cibernéticas; Objetivo III – estabelecer governança de segurança cibernética e fortalecer a gestão e coordenação integrada de ações de segurança cibernética nos órgãos do Poder Judiciário; e Objetivo IV – permitir a manutenção e a continuidade dos serviços, ou o seu restabelecimento em menor tempo possível.
- 2.2.3. No que tange ao Planejamento Estratégico do Conselho Nacional de Justiça para o período de 2021-2026, [Portaria nº. 104 de 30/06/2020](#), vislumbra-se o alinhamento aos objetivos estratégicos: XI: garantir infraestrutura adequada ao funcionamento do CNJ.
- 2.2.4. No âmbito do Plano Diretor de Tecnologia da Informação e Comunicação (PDTIC) do Conselho Nacional de Justiça 2023-2025 (CNJ), [PDTIC 2025](#),



Poder Judiciário

Conselho Nacional de Justiça

vislumbra-se alinhamento com o Objetivo Estratégico OE7 – Aprimorar a Segurança da Informação e a Gestão de Dados.

- 2.2.5. A presente contratação está contemplada no Plano Anual de Contratações 2026, item PCA 150, Plano Orçamentário SEG0 constante no Processo SEI 14769/2025.

Objetivos

- 2.2.6. A contratação visa dotar o Conselho Nacional de Justiça de meios para garantir a confidencialidade, integridade, disponibilidade e privacidade das informações produzidas e ou armazenadas além dos seguintes objetivos:
- 2.2.6.1. Dispor de meios para operação, administração e atendimento de requisições relacionadas às ferramentas e soluções de segurança disponíveis no ambiente tecnológico do Conselho Nacional de Justiça.
 - 2.2.6.2. Dispor de meios para identificação e correção de vulnerabilidades de segurança da informação no ambiente e sistemas críticos do CNJ a fim de evitar que ataques cibernéticos obtenham sucesso explorando vulnerabilidades conhecidas.
 - 2.2.6.3. Propiciar um ambiente mais seguro na rede corporativa do CNJ, minimizando ataques à infraestrutura e comportamentos maliciosos que possam comprometer a segurança da informação.
 - 2.2.6.4. Operacionalizar a Gestão do Acesso e Uso dos Recursos de Tecnologia da Informação e Comunicação, de acordo com o preconizado na Seção III da Portaria SG nº 47, de 29/11/2027 que instituiu a Política de Segurança da Informação do Conselho Nacional de Justiça.
 - 2.2.6.5. Operacionalizar a Gestão de Incidentes de Segurança da Informação, de acordo com o preconizado na Seção V da Portaria SG nº 47, de 29/11/2027 que instituiu a Política de Segurança da Informação do Conselho Nacional de Justiça.
 - 2.2.6.6. Propiciar a correlação de eventos de tráfego de rede com os eventos de segurança de maneira a ampliar a visibilidade e entendimento da dinâmica de incidente de segurança da informação.
 - 2.2.6.7. Implantar e fortalecer as equipes de tratamento de incidentes de segurança.



Poder Judiciário

Conselho Nacional de Justiça

- 2.2.6.8. Manter uma equipe ininterrupta de resposta rápida e efetiva a ataques e incidentes de segurança da informação.
- 2.2.6.9. Apoiar a Gestão de Políticas de Segurança da Informação e respectivas análises de conformidade.
- 2.2.6.10. Aumentar a consciência situacional do ambiente computacional do CNJ.

2.3. Referência aos Estudos Preliminares

- 2.3.1. Este Termo de Referência foi elaborado considerando o Documento de Oficialização da Demanda (DOD) encaminhado pelo Departamento de Tecnologia da Informação (DI) e os Estudos Preliminares constantes do Processo SEI nº 04520/2025.

2.4. Análise de Mercado de TIC

- 2.4.1. Considerando as necessidades e requisitos da demanda descritos no item 1.2 dos Estudos Preliminares, visualizou-se no mercado de TIC 03 (três) possíveis alternativas. As soluções de TIC identificadas são:

a) Solução 1 - Serviços Gerenciados de Segurança da Informação:

A solução 1 é integrada pela coletânea de serviços voltados a reduzir riscos e colmatar a lacuna de habilidades de segurança da entidade/órgão. Os serviços da solução 1 proporcionam o monitoramento de segurança e gerenciamento de dispositivos de segurança com diversos fornecedores (firewall, sistema de prevenção de intrusões de rede, gerenciamento unificado de ameaças e etc.) como também, provedores de detecção e resposta gerenciados.

Nesse cenário, o CNJ iria dispor de um modelo de gerenciamento das operações de segurança, comumente denominado Serviços Gerenciados de Segurança (ou MSS - Managed Security Services). Esses serviços são prestados por Provedores de Serviços de Segurança Gerenciados (MSSPs - Managed Security Services Providers), que operam remotamente e, de forma presencial, através de uma equipe de técnicos especializados em segurança através do uso compartilhado de Centros de Operação de Segurança (SOCs).

Há também a possibilidade de fornecimento de soluções de segurança como parte integrante do serviço fornecido. Nesse contexto, a administração pública, ao contratar os serviços do MSSP, deixa de se preocupar com a gestão e administração de suas



Poder Judiciário

Conselho Nacional de Justiça

soluções de segurança e proteção de dados e, com isso, é possível uma significativa redução de gastos com licenças, hardwares e softwares.

Assim, a Solução 01 caracteriza-se pela contratação de serviços gerenciados de segurança da informação associados ao fornecimento de plataformas e ferramentas de segurança sob modelo de subscrição, tais como gestão de vulnerabilidades, plataforma de campanhas de conscientização em Segurança da Informação e de serviço de Proteção contra riscos Digitais (Digital Risk Protection DRP), como parte integrante do contrato.

- b) Solução 2 – Modelo híbrido – Operação interna parcial:** A Solução 2 caracteriza-se pela contratação parcial de serviços gerenciados de segurança da informação associados ao fornecimento de plataformas e ferramentas de segurança e pela operação parcial dos serviços por servidores do quadro próprio da Divisão de Segurança (DISI) e Seção de Gestão da Segurança da Informação (SEGSi) do Departamento de TIC do CNJ.

Nessa alternativa, mantêm-se o Serviço de administração, operação e atendimento de requisições sob responsabilidade do CNJ, por meio da DISI/SEGSi. Os demais serviços são contratados, ficando a contratada responsável por executar as atividades típicas de um Centro de Operações de Segurança (SOC), incluindo triagem de alertas, correlação de eventos, análise de incidentes, resposta e investigação, associados ao fornecimento de plataformas e ferramentas de segurança sob modelo de subscrição. Os serviços previstos na solução 02 incluem: Serviço de gestão de vulnerabilidades, Serviço de gestão de incidentes de segurança (CSIRT - Blue Team), Serviço de monitoramento e visibilidade de ataques cibernéticos, Serviços de Conscientização em Segurança da Informação e Serviço de testes de invasão (Red Team).

- c) Solução 3 - Quadro próprio de servidores da DISI/SEGSi do CNJ:** Nesta alternativa de solução, os serviços necessários seriam prestados por servidores do quadro próprio da Divisão de Segurança (DISI) e Seção de Gestão da Segurança da Informação (SEGSi) do Departamento de TIC do CNJ, tais como administração, operação e atendimento de requisições, gerenciamento de vulnerabilidades, gestão de incidentes de segurança, monitoramento de ataques cibernéticos, testes de invasão e gestão de conscientização de segurança da informação. Além disso, seriam necessárias a



Poder Judiciário

Conselho Nacional de Justiça

contratação e/ou aquisição de soluções adicionais de segurança, bem com a realização de atividades de gerenciamento e monitoramento dessas e das demais soluções de segurança já instaladas no parque computacional do CNJ.

- 2.4.2. A análise comparativa de custos foi elaborada considerando as soluções técnicas e funcionalmente viáveis identificadas, com a finalidade de se fazer uma análise qualitativa de custos. Para estimativa dos custos totais da demanda, foram utilizadas as informações de preços levantadas nas contratações públicas similares. Assim, foram encontrados os seguintes editais cujos extratos estão incluídos no anexo “Contratações Públicas Similares” dos Estudos Preliminares:

Entidade/Órgão	Pregão	Status
FUNPRESP	Pregão Eletrônico nº 90001/2024	Contrato n. 03/2024 Contrato n. 05/2024
Conselho Nacional de Justiça	Pregão eletrônico nº 03/2021	Contrato n. 08/2021
TRF da 5ª. Região	Pregão Eletrônico nº 28/2023	Homologado Contrato 08/2024
Ministério da Saúde	Pregão Eletrônico nº 28/2023	Contrato n. 59/2013
Secretaria Fazenda do Rio Grande do Sul	Pregão Eletrônico nº 9097/2024	Homologado
Sebrae - MT	Pregão Eletrônico nº 013/2025	Contrato n. 0176.25
TCE-CE	Pregão Eletrônico nº 04/2024	Contrato. N.33/2024
COREN-SP	Pregão Eletrônico nº 12/2024	Homologado
TCU	Pregão Eletrônico nº 48/2024	Contrato 02/2025
STJ	Pregão Eletrônico nº 30/2024	Contrato 52/2023
FINEP	Pregão Eletrônico nº 03/2023	Contrato 20.23.0037.00
MP-BA	Pregão Eletrônico nº 33/2022	Contrato 002/2024
TRE-AM	Pregão Eletrônico nº 39/2023	Homologado
TJMA	Pregão Eletrônico nº 90.046/2024	Homologado
TRT 17.a Região	Pregão Eletrônico nº 23/2023	Contrato 21/2024



Poder Judiciário

Conselho Nacional de Justiça

2.4.3. A tabela abaixo apresenta o resumo comparativos dos custos totais das soluções presente no item 1.4.4 dos Estudos Preliminares:

1	Serviços gerenciados de segurança da informação	60	mensal	R\$ 240.677,05	R\$ 2.910.686,33	R\$ 14.553.431,63
2	Modelo Híbrido – Operação interna parcial	60	mensal	R\$ 139.102,76	R\$1.691.794,77	R\$ 8.458.973,90
3	Quadro próprio de servidores da DISI/SEGS do CNJ	60	mensal	R\$ 94.367,36	R\$ 1.132.408,34	R\$ 5.662.041,70

2.4.4. A **solução 01 (Serviços Gerenciados de Segurança)** foi objeto de contratação pelo CNJ por meio do Contrato nº. 08/2021, pregão eletrônico nº 03/2021, que teve como objetivo a prestação de serviços Gerenciados de Segurança da Informação, incluindo Serviços de Administração, Operação e Atendimento a Requisições, Gestão de Vulnerabilidades, Gestão de Incidentes, Monitoramento e Visibilidade de ataques Cibernéticos e Testes de Invasão.

2.4.5. Cabe destacar que a solução 01 proposta inclui o serviço de conscientização em Segurança da Informação e há a previsão de fornecimento de software de gestão de vulnerabilidade. Assim sendo, a **solução 1** se configura como uma **solução** tecnicamente e administrativamente **viável** atendendo plenamente as necessidades/requisitos traçados no item 1.2 dos Estudos Preliminares.

2.4.6. A **solução 02 (Modelo Híbrido – Operação interna parcial)** consiste em um modelo híbrido de execução, no qual parte das atividades permanece sob responsabilidade da equipe interna do CNJ (SEGS/DISI), e os demais serviços especializados são contratados junto ao mercado.

2.4.7. Nesse modelo, a SEGS/DISI executaria diretamente o Serviço de Administração, Operação, Manutenção e Atendimento de Requisições, enquanto a contratação abrangeria os demais serviços previstos na solução 01, incluindo gestão de vulnerabilidades, gestão de incidentes, monitoramento e visibilidade de ataques cibernéticos, testes de invasão e conscientização em segurança da informação, além do fornecimento de software de gestão de vulnerabilidades e plataforma de campanhas de conscientização em Segurança da Informação e de Proteção contra riscos Digitais (Digital Risk Protection DRP).

2.4.8. Embora essa alternativa possibilite maior participação institucional na operação, sua adoção implica riscos relevantes quanto à continuidade, à



Poder Judiciário

Conselho Nacional de Justiça

disponibilidade e ao cumprimento dos níveis de serviço exigidos, considerando que a execução do Serviço de Administração, Operação, Manutenção e Atendimento de Requisições demandaria atuação contínua e tempestiva para suportar a criticidade dos ativos e serviços de TIC do CNJ.

- 2.4.9. Adicionalmente, considerando o atual volume de demandas, o quantitativo de ativos de segurança existentes, a complexidade técnica das ferramentas envolvidas e a necessidade de atendimento com características compatíveis com o regime 24x7, conclui-se que a manutenção dessa atividade sob responsabilidade exclusiva da equipe interna pode comprometer o atingimento dos SLAs e a efetividade operacional da segurança cibernética institucional.
- 2.4.10. Em relação à **solução 03 (Quadro próprio de servidores da DISI/SEGSi do CNJ)**, observou-se como a opção mais vantajosa economicamente conforme pode ser visto na tabela de resumo comparativo de custos totais presente no subitem 2.4.3.
- 2.4.11. A solução 3 compreende na execução dos serviços diretamente pelos próprios servidores da Divisão de Segurança (DISI) e Seção de Gestão da Segurança da Informação (SEGSi) e na contratação de ferramentas de segurança adicionais de gerenciamento de vulnerabilidades, de plataforma de campanhas de conscientização em Segurança da Informação e de serviço de Proteção contra riscos Digitais (Digital Risk Protection - DRP).
- 2.4.12. Nesse cenário, as atividades de configuração, gerenciamento, administração e monitoramento das soluções de segurança também ficariam a cargo das equipes da DISI/SEGSi, que trabalham em regime 8x5 e 7x5. Além disso, os servidores necessitariam de capacitação, treinamento e especialização específica, o que seria inviável diante da enorme quantidade de requisições e de ativos de segurança a serem controlados atualmente, considerando o tamanho do parque tecnológico do CNJ e a relevância de suas atividades finalísticas para a sociedade.
- 2.4.13. Por outro lado, empresas de MSS operam com monitoramento contínuo (24 horas por dia, 7 dias por semana), o que exige escalas de trabalho e disponibilidade que são inviáveis com equipes internas limitadas. Essa capacidade operacional garante respostas mais rápidas e eficazes diante de incidentes de segurança.
- 2.4.14. Ainda, é importante considerar que a constante evolução das ameaças cibernéticas exige investimento contínuo em ferramentas, plataformas e capacitação. Provedores de MSS estão sempre se atualizando com as



Poder Judiciário

Conselho Nacional de Justiça

mais recentes tecnologias e práticas de mercado e podem possibilitar o início da operação em tempo significativamente menor, com soluções e processos já consolidados, algo de difícil execução com recursos internos.

- 2.4.15. Dessa forma, **recomenda-se tecnicamente a contratação de serviços gerenciados de segurança (MSS)** como alternativa mais eficiente e segura em comparação à criação de um Centro de Operação de Segurança próprio no âmbito do CNJ.
- 2.4.16. Portanto, a equipe de planejamento da contratação declara como mais viável que seja adotada a **solução 01 - Serviços Gerenciados de Segurança da Informação**, como alternativa de solução que atenderá plenamente a os requisitos listados o item 1.2 dos Estudos Técnicos Preliminares.

2.5. Benefícios

- 2.5.1. O CNJ visa com a solução selecionada, dispor de serviços especializados para tratar as tarefas e as rotinas de segurança com mais eficiência e/ou menor custo do que os empregados com o uso da própria força de trabalho, servidores, ou serviços acessórios que não possuem a mesma capacidade técnica necessários a garantir a integridades dos recursos e ativos tecnológicos e o aprimoramento das boas práticas de segurança.
- 2.5.2. Com isso, os benefícios esperados são:
- a. **Eficiência:** A solução escolhida atende as necessidades/requisitos que definem a demanda, irá aumentar o grau de satisfação dos usuários com os produtos e serviços fornecidos pela DTI/CNJ, uma vez que irá facilitar a identificação preventiva de ameaças emergentes ou invasões externas além de prevenir eventuais vazamentos de informações antes da divulgação pública;
 - b. **Eficácia:** a solução mostra-se eficaz por acolher todos os requisitos listados, efetivamente atendendo às necessidades identificadas pela área demandante com a melhoria da entrega dos serviços de Segurança aos usuários em decorrência da utilização de boas práticas dos processos de gerenciamento de serviços de TI.
 - c. **Economicidade:** A solução mostra-se economicamente viável sendo que sua divisão pode prejudicar o conjunto do objeto, além



Poder Judiciário

Conselho Nacional de Justiça

de gerar custos adicionais relacionadas à coexistência de diversos contratos.

- d. **Padronização:** 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 internacionais.

2.6. Relação entre a Demanda Prevista e a Contratada

- 2.6.1. Os SERVIÇOS GERENCIADOS DE SEGURANÇA, capazes de atender as necessidades/requisitos do CNJ, envolvem a prestação dos seguintes serviços aqui quantificados, sem garantia de consumo mínimo:

Grupo	Item	Descrição	Quantidade	Unidade
1	1	Serviço de administração, operação e manutenção e atendimento a requisições	60	Mensal
	2	Serviço de gestão de vulnerabilidades	60	Mensal
	3	Serviço de gestão de incidentes de segurança (CSIRT - Blue Team)	60	Mensal
	4	Serviço de monitoramento e visibilidade de ataques cibernéticos	60	Mensal
	5	Serviço de Conscientização da Segurança da Informação	60	Mensal
Não agrupado	6	Serviço de testes de invasão (Red Team)	80	Sistemas

- 2.6.2. Como forma de estimativa da demanda prevista para os serviços rotineiros 1, 2, 3, 4 e 5, estabeleceu-se como fundamento o ambiente tecnológico e **a plataforma de segurança do CNJ, disponível no ANEXO B – PLATAFORMA DE SEGURANÇA.**
- 2.6.3. Os serviços de gerenciados de segurança da informação devem contemplar o atendimento para cerca de 1500 (mil e quinhentos) usuários, 2600 (dois mil e seiscentos) computadores ativos na rede, 800 servidores, mais de 130 (cento e trinta) sistemas publicados e 02 (dois) ambientes de nuvem operando serviços críticos.



Poder Judiciário

Conselho Nacional de Justiça

- 2.6.4. Ademais, os serviços prestados devem atuar na operação e administração do conjunto de soluções de segurança atualmente disponíveis no ambiente do CNJ (**ANEXO B – PLATAFORMA DE SEGURANÇA**). A seguir são apresentados o resumo dos quantitativos de recursos disponíveis no ambiente tecnológico:

Estações de trabalho	1500
Firewalls	02
Ambientes de nuvem	02
Servidores	800
Usuários internos	1500
VPN ativas	30
Sistemas suportados	137

Resumo Ambiente Tecnológico em 05/05 /2026

- 2.6.5. Para o serviço 6, foi consignado o quantitativo de 137 sistemas listados nos [Portfólio de Tecnologia da Informação e Comunicação e Serviços Digitais do CNJ](#) de acordo com a Portaria Nº 311 de 27/10/2023. Dos 137 sistemas, o CNJ irá alçar, segundo seu interesse e necessidade, **até 80 sistemas** estratégicos para serem objeto dos serviços de teste de invasão.
- 2.6.6. O dimensionamento das equipes para execução adequada dos **Serviços Gerenciados de Segurança (MSS)** é de responsabilidade exclusiva da CONTRATADA, devendo ser suficiente para o cumprimento integral dos níveis de serviço exigidos, quantitativo mínimo de perfis profissionais e indicadores constantes neste Termo de Referência.

2.7. Impacto ambiental

- 2.7.1. A solução proposta vai ao encontro dos critérios de sustentabilidade ambiental e econômica na aquisição de bens, contratação de serviços ou obras, locação de máquinas e equipamentos consumidores de energia e sobre o uso da Etiqueta Nacional de Conservação de Energia – ENCE, no âmbito do Conselho Nacional de Justiça – CNJ, onde as empresas



Poder Judiciário

Conselho Nacional de Justiça

contratadas adotarão as seguintes práticas de sustentabilidade na execução dos serviços, quando couber:

1. Uso de produtos de limpeza e conservação de superfícies e objetos inanimados que obedeçam às classificações e especificações determinadas pela Agência Nacional de Vigilância Sanitária – ANVISA.
2. Observância da Resolução CONAMA 20, de 7 de dezembro de 1994, quanto aos equipamentos de limpeza que gerem ruído no seu funcionamento.
3. Fornecimento aos empregados, dos equipamentos de segurança necessários para a execução dos serviços.
4. Realização de programa interno de treinamento de seus empregados nos três primeiros meses de execução contratual, para redução de consumo de energia elétrica e de água e redução de produção de resíduos sólidos, observadas as normas ambientais vigentes.
5. Separação dos resíduos recicláveis descartados, na fonte geradora e, sua destinação às associações e cooperativas dos catadores de materiais recicláveis, que será realizada pela coleta seletiva do papel para reciclagem, quando couber, nos termos do Decreto 10.936, de 12 de janeiro de 2022.
6. Respeito às Normas Brasileiras – NBR, publicadas pela ABNT, sobre resíduos sólidos.
7. Previsão da destinação ambiental adequada das pilhas e baterias usadas ou inservíveis, segundo disposto na Resolução CONAMA 257, de 30 de junho de 1999.

- 2.7.2. A CONTRATADA deverá tomar conhecimento do Plano de Logística Sustentável - PLS, das Orientações do Controle Interno e demais procedimento do CNJ, ainda que a natureza dos serviços não se aplica, devidamente justificada pela inexistência de produtos ou atividades que se enquadrem nas condições exigidas nos critérios de Sustentabilidade Ambiental, Social e Econômica.

2.8. Impacto social e cultural

- 2.8.1. A presente contratação não produz qualquer tipo de impacto social ou cultural no curso de sua execução.

2.9. Conformidade Técnica e Legal

- 2.9.1. Os procedimentos de segurança da informação e o [processamento da informação](#) devem estar em conformidade com as políticas e normas de segurança adotadas pelo CNJ - [Portaria nº 47, de 29/11/2017](#).
- 2.9.2. Deverá ser mantida a conformidade com os direitos de propriedade intelectual do fabricante protegido por 50 (cinquenta) anos, nos termos do art. 2º, § 2º da [Lei nº 9.609/1998](#).
- 2.9.3. Deverá ser mantida a conformidade com a Estratégia Nacional de Tecnologia da Informação e Comunicação do Poder Judiciário - ENTIC-JUD ([Resolução CNJ nº 370/2021](#)).



Poder Judiciário

Conselho Nacional de Justiça

- 2.9.4. Deverá ser mantida a conformidade com os Objetivos Estratégicos estabelecidos na Estratégia Nacional de Segurança Cibernética do Poder Judiciário (ENSEC-PJ) conforme [Resolução nº 396, de 24/09/2021](#).
- 2.9.5. Deverá ser mantida a conformidade com o [Processo de Desenvolvimento e Sustentação de Sistemas](#) (PDS), utilizado no Departamento de Tecnologia da Informação e Comunicação (DTI) deste Conselho.
- 2.9.6. Deverá ser mantida a conformidade e observância as diretrizes e ações ordenadas pelo Comitê Gestor de Segurança da Informação (CGSI), instituído pela Portaria nº 112, de 11/07/2013 e suas alterações.
- 2.9.7. Deverá ser respeitada as orientações emanadas pela Lei nº 12.305, de 2 de Agosto de 2010 e seu regulamento, quanto a logística reversa para descarte de peças e produtos eletrônicos.
- 2.9.8. Deve garantir 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.

3. DA LICITAÇÃO

3.1. Da Pretensão da Contratação

- 3.1.1. Serviços Gerenciados de Segurança da Informação, incluindo Serviços de Administração, Operação e Atendimento a Requisições, Gestão de Vulnerabilidades, Conscientização em Segurança da Informação, Gestão de Incidentes, Monitoramento e Visibilidade de ataques Cibernéticos e Testes de Invasão, de acordo com as especificações técnicas contidas neste Termo de Referência – TR e seus anexos.
- 3.1.2. A prestação dos serviços deve ser baseada em modelo de remuneração em função dos resultados apresentados, em que os pagamentos são realizados após mensuração, avaliação e validação de métricas quantitativas e qualitativas, contendo metas e indicadores de desempenho, com Nível Mínimo de Serviço (NMS) definido em contrato, de modo a resguardar a eficiência e a qualidade na prestação dos serviços.
- 3.1.3. Assim, os níveis de serviço, devem ser registrados, monitorados e comparados às metas de desempenho e qualidade estabelecidas, em termos de prazo e efetividade.
- 3.1.4. O modelo de prestação dos serviços deve contemplar, ainda, processos de trabalho e atividades a serem demandadas pelo Conselho, tais como abertura de chamados técnicos para resolução de problemas e de



Poder Judiciário

Conselho Nacional de Justiça

consulta de informações, e aquelas a serem desenvolvidas periodicamente pela empresa, tais como monitoramento dos produtos ofertados, resposta a incidentes de segurança, análise de vulnerabilidades do parque computacional e apresentação tempestiva de indicadores, boletins e relatórios de segurança, conforme periodicidade e níveis de serviço definidos.

- 3.1.5. Cabe ressaltar que todos os serviços serão solicitados, 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.
- 3.1.6. 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 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.

3.2. Da Natureza do Objeto da Contratação

- 3.2.1. Os serviços pretendidos neste Termo de Referência seguem padrões e desempenho de mercado e, portanto, se enquadram como SERVIÇOS COMUNS ou usuais de mercado.
- 3.2.2. Como apontado no item 1.5.2 “Descrição da Solução” do Estudo Preliminar e reproduzido neste Termo de Referência no item 1.1, o arcabouço de serviços para a composição da estrutura de Gerenciamento de Segurança caracteriza-se pela aplicação de controles de segurança preventiva ou reativa sobre um conjunto de ativos com o objetivo de proteger, preservar o valor e garantir a confidencialidade, a integridade e a disponibilidade dos ativos a disposição do CNJ.
- 3.2.3. Por força dessas características, trata-se de serviço essencial e de natureza contínua, pois devem ser realizados ininterruptamente, e sua paralisação acarretará em suspensão ou o comprometimento das atividades prestadas pelos servidores e colaboradores do CNJ. Dentro deste cenário, fica evidente que se trata de uma despesa corrente, por não contribuir para a formação ou aquisição de um bem de capital.



Poder Judiciário

Conselho Nacional de Justiça

- 3.2.4. Não dispor da prestação do serviço, poderá impactar severamente, a integridade, disponibilidade e confidencialidade de sistemas providos pelo CNJ, como o Processo Judicial Eletrônico (PJe), o Sistema Eletrônico de Execução Unificado (SEEU), o Banco Nacional de Mandados de Prisão (BNMP), o Escritório Digital, as Metas Nacionais, entre outros sistemas importantes para o CNJ e para o Poder Judiciário.

3.3. Do Parcelamento e Adjudicação

- 3.3.1. Em função dos aspectos técnicos e requisitos que envolvem a contratação dos serviços e, também, considerando o grau de interação entre alguns itens dos serviços técnicos descritos no presente Termo de Referência, a natureza específica, o caráter contínuo, aliada a alta criticidade e complexidade do ambiente de TI do CNJ, optou-se por agrupar alguns itens da forma descrita na **Descrição detalhada do objeto**.
- 3.3.2. É de praxe do mercado, conforme pode ser visto nas contratações similares dos Estudos Técnicos preliminares (1.3.2- Contratações Públicas Similares (Art. 14, I, b), agrupar todos os itens descritos no objeto desta contratação. Contudo, para esta licitação os itens foram separados de modo a se alcançar o melhor sob dois aspectos. O primeiro em relação ao maior número de empresas que pudessem concorrer e o segundo em manter a coesão intrínseca entre itens, que para melhor governança e eficácia em seu gerenciamento, devem ser gerenciados pela mesma fornecedora.
- 3.3.3. Assim, com objetivo de aumentar a concorrência, os itens foram agrupados em um único grupo e um item sem agrupamento, alcançando assim a possibilidade de até 2 (duas) empresas serem contratadas. Isto permite que uma empresa que seja referência, por exemplo, em somente nos itens agrupados ou no item não agrupado, possa participar desta licitação.
- 3.3.4. A integração desses serviços apresenta coerência em termos de atendimento aos princípios de gestão, celeridade, economicidade e eficiência quanto à administração das requisições e identificação de vulnerabilidades.
- 3.3.5. O primeiro grupo, composto dos itens 1 ao 5 elencados no presente Termo de Referência, trata de serviços continuados, especializados e interdependentes, voltados à prevenção, detecção, resposta e mitigação de incidentes de segurança da informação e cibernética, bem como ao



Poder Judiciário

Conselho Nacional de Justiça

fortalecimento do fator humano, compondo um ecossistema integrado de governança e operação de segurança.

- 3.3.6. A contratação isolada desses serviços, de forma fragmentada, comprometeria a efetividade operacional, aumentaria os riscos de sobreposição de responsabilidades, elevaria o custo total e dificultaria a gestão contratual e a mensuração de resultados, contrariando os princípios da eficiência e da economicidade.
- 3.3.7. A aglutinação dos itens é tecnicamente justificada pela interdependência funcional direta entre os serviços:
 - 3.3.7.1. O Serviço de administração, operação, manutenção e atendimento a requisições constitui a base operacional necessária para sustentar e orquestrar todos os demais serviços, garantindo continuidade, disponibilidade e aderência aos níveis de serviço.
 - 3.3.7.2. O Serviço de gestão de vulnerabilidades fornece insumos estratégicos e operacionais que subsidiam tanto o monitoramento de ataques quanto a gestão de incidentes, permitindo atuação preventiva e priorização baseada em risco.
 - 3.3.7.3. O Serviço de gestão de incidentes de segurança (CSIRT – Blue Team) depende diretamente das capacidades de monitoramento, visibilidade, correlação de eventos e inteligência de ameaças, sendo ineficaz quando operado de forma dissociada desses componentes.
 - 3.3.7.4. O Serviço de monitoramento e visibilidade de ataques cibernéticos atua como elemento central de detecção e geração de alertas, que alimentam os processos de resposta a incidentes, gestão de crises e melhoria contínua.
 - 3.3.7.5. O Serviço de Conscientização de Segurança da Informação complementa os serviços técnicos ao atuar na redução do risco humano, alinhando-se aos incidentes recorrentes, às ameaças observadas e às vulnerabilidades comportamentais identificadas no ambiente monitorado.
- 3.3.8. Assim, os serviços formam um ciclo contínuo e integrado de prevenção, detecção, resposta, aprendizado e mitigação de riscos. A contratação conjunta dos serviços possibilita:
 - 3.3.8.1. Governança unificada, com responsabilidades claras e sem lacunas entre fornecedores;
 - 3.3.8.2. Integração nativa de processos, ferramentas, fluxos de atendimento e métricas;



Poder Judiciário

Conselho Nacional de Justiça

- 3.3.8.3. Padronização de procedimentos, metodologias e indicadores de desempenho;
 - 3.3.8.4. Redução de conflitos contratuais, especialmente quanto à apuração de causa raiz e responsabilidade por incidentes;
 - 3.3.8.5. Melhoria na rastreabilidade e auditoria, com visão ponta a ponta dos eventos de segurança.
- 3.3.9. Esses fatores elevam significativamente o nível de maturidade da gestão de segurança da informação do CNJ.
- 3.3.10. Por outro lado, o serviço do item 6, relacionado aos testes de invasão, pode ser prestado separadamente dos demais e, logicamente, por empresa distinta. Isto permitirá que um maior número de empresas especializadas em serviços de testes de invasão possa participar do certame, possibilitando uma ampla concorrência.
- 3.3.11. O CNJ dispõe de uma série de ativos heterogêneos agrupados em: rede de comunicação de dados, telefonia, banco de dados, servidores de rede, sistemas operacionais, sistemas de backup e recursos de armazenamento de dados que, dada a criticidade dos sistemas hospedados, deve operar em alta disponibilidade e resiliência a falhas. Por óbvio, os serviços de gerenciamento de segurança requerem equipe técnica qualificada e igualmente diversificada com o fito de manter a operacionalidade, os padrões técnicos e normativos estabelecidos para a estrutura física e lógica desta solução, em benefício da integral proteção, segurança, operação, disponibilidade e criticidade dos sistemas físicos e lógicos que compõem o ambiente do CNJ.
- 3.3.12. A distribuição e agrupamento de alguns itens do objeto, se torna viável, pelos seguintes aspectos:
- a) Modelo amplamente utilizado para as contratações de objeto análogo;
 - b) A simplificação da condução das atividades de gestão, fiscalização e controle do contrato;
 - c) A minimização de potenciais conflitos internos entre diferentes prestadores de serviços; e
 - d) O atingimento de níveis de desempenho em razão da continuidade da prestação que garantam de forma global a qualidade dos serviços executados, o que não se verifica na divisão dessas atividades.



Poder Judiciário

Conselho Nacional de Justiça

3.3.13. É importante também, se observar o posicionamento do Egrégio Tribunal de Contas da União e a literatura jurídica sob a matéria:

*15. Acerca da alegada possibilidade de fragmentação do objeto, vale notar que nos termos do art. 23, § 1º, da Lei n. 8.666/1993, exige-se o parcelamento do objeto licitado sempre que isso se mostre técnica e economicamente viável. A respeito da matéria, esta Corte de Contas já editou a Súmula n. 247/2004, **verbis**: “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...” (grifos não constam do original).*

16. Depreende-se, portanto, que a divisão do objeto deverá ser implementada sempre que houver viabilidade técnica e econômica para a sua adoção.

17. Nesse ponto, calha trazer à baila o escólio de Marçal Justen Filho: “O fracionamento em lotes deve respeitar a integridade qualitativa do objeto a ser executado. Não é possível desnaturar um certo objeto, fragmentando-o em contratações diversas e que importam o risco de impossibilidade de execução satisfatória.” (Comentários à Lei de Licitações e Contratos Administrativos. 10. ed. São Paulo: Dialética, 2004. p. 209).

3.3.14. Portanto, pode-se afirmar ser tecnicamente inadequado o desmembramento de todos os itens, sob pena de não se atender o objetivo buscado pelo CNJ, no sentido de fortalecer a disponibilidade, segurança, a preservação dos dados e ativos de TI do Conselho na manutenção e segurança da operabilidade do ambiente de TI. Sob o ponto de vista econômico, não há elementos nos autos que permitam concluir que a adoção do parcelamento total do objeto, seria, no caso concreto, mais vantajosa para o CNJ.

3.3.15. No contexto da solução apontada pela equipe de planejamento da contratação e de acordo com as necessidades e requisitos levantados no item 1.2.1 do Estudo Preliminar, recomenda-se que o objeto possa ser adjudicado por mais de uma empresa participante da licitação, de acordo com o agrupamento parcial dos itens demonstrados a seguir:

Grupo	Item	Descrição	Quantidade	Unidade
1	1	Serviço de administração, operação e manutenção e atendimento a requisições	60	Mensal
	2	Serviço de gestão de vulnerabilidades	60	Mensal



Poder Judiciário

Conselho Nacional de Justiça

	3	Serviço de gestão de incidentes de segurança (CSIRT - Blue Team)	60	Mensal
	4	Serviço de monitoramento e visibilidade de ataques cibernéticos	60	Mensal
	5	Serviço de Conscientização da Segurança da Informação	60	Mensal
Não agrupado	6	Serviço de testes de invasão (Red Team)	80	Sistemas

3.3.16. Assim, a contratação será composta por 05 (cinco) itens agrupados em **01 (único) grupo**, e **01 (um) item não agrupado**, possibilitando a adjudicação do objeto por mais de uma empresa participante da licitação.

3.3.17. Poderão participar dessa contratação consórcio de empresas, observadas as normas contidas no art. 15 da Lei 14.133/2021.

3.4. Modalidade e Tipo de Licitação

3.4.1. Os serviços pretendidos neste Termo de Referência seguem padrões e desempenho de mercado e, portanto, se enquadram como SERVIÇOS COMUNS ou usuais de mercado. Conforme prevê a alínea XLI do artigo 6º da Lei 14.133, de 1º de abril julho de 2001:

“Art. 6º Para os fins desta Lei, consideram-se:

XLI - pregão: modalidade de licitação obrigatória para aquisição de bens e serviços comuns, cujo critério de julgamento poderá ser o de menor preço ou o de maior desconto”.

3.4.2. Assim, propõe-se a utilização do pregão, na forma eletrônica, como modalidade de licitação do tipo **MENOR PREÇO**, desde que satisfeitos todos os termos estabelecidos no futuro ato convocatório.

3.5. Critérios de Habilitação

3.5.1. A habilitação jurídica limita-se à comprovação de existência jurídica da pessoa e, quando cabível, de autorização para o exercício da atividade a ser contratada, nos termos do art. 66 da Lei Federal nº 14.133/2021.

3.5.2. As licitantes deverão comprovar a habilitação econômico-financeira, restrita à apresentação da seguinte documentação, nos termos do art. 69 da Lei Federal nº 14.133/2021, conforme abaixo:



Poder Judiciário

Conselho Nacional de Justiça

- 3.5.2.1. Balanço patrimonial, demonstração de resultado de exercício e demais demonstrações contábeis dos 2 (dois) últimos exercícios sociais;
 - 3.5.2.1.1. Os documentos exigidos limitar-se-ão ao último exercício no caso de a participante ter sido constituída há menos de 2 (dois) anos.
- 3.5.2.2. Certidão negativa de feitos sobre falência expedida pelo distribuidor da sede do licitante.
- 3.5.2.3. Patrimônio líquido no valor mínimo de R\$ 1.711.737,22 (um milhão, setecentos e onze mil, setecentos e trinta e sete reais e vinte e dois centavos), correspondentes a 10% (dez por cento) do valor total estimado para a contratação;
- 3.5.2.4. Caso o balanço patrimonial apresente alguma irregularidade ou, embora regular, apresente índices de LG, SG e LC menores que 1 (um), poderá ser exigida declaração, assinada por profissional habilitado da área contábil, que ateste o atendimento pela participante dos índices econômicos previstos no instrumento de convocação.
- 3.5.3. As habilitações fiscal, social e trabalhista serão aferidas mediante a verificação dos seguintes requisitos, nos termos do art. 68 da Lei Federal nº 14.133/2021, conforme abaixo:
 - 3.5.3.1. Inscrição no Cadastro Nacional de Pessoa Jurídica (CNPJ);
 - 3.5.3.2. Inscrição no cadastro de contribuintes estadual e/ou municipal, se houver, relativo ao domicílio ou sede do licitante, pertinente ao seu ramo de atividade e compatível com o objeto contratual;
 - 3.5.3.3. Regularidade perante a Fazenda federal, estadual e/ou municipal do domicílio ou sede do licitante, ou outra equivalente, na forma da lei;
 - 3.5.3.4. Regularidade relativa à Seguridade Social e ao FGTS, que demonstre cumprimento dos encargos sociais instituídos por lei;
 - 3.5.3.5. Prova de regularidade perante a Justiça do Trabalho; e
 - 3.5.3.6. Apresentar declaração de cumprimento do disposto no inciso XXXIII do art. 7º da Constituição Federal.
- 3.5.4. É obrigatório às licitantes, apresentar atestado(s) ou certidão(ões) de capacidade técnico-operacional comprobatórios de que a empresa



Poder Judiciário

Conselho Nacional de Justiça

proponente tenha executado ou esteja executando, serviços de características técnicas semelhantes às do objeto do presente Edital.

3.5.5. A justificativa para a solicitação de atestado(s) de capacidade técnica como critério de habilitação das licitantes, no caso em exame, fundamenta-se:

3.5.5.1. No atendimento aos comandos legais contidos na Lei nº 14.133/2021, especialmente quanto à exigência de documentação relativa à qualificação técnica e à possibilidade de comprovação de aptidão para desempenho de atividade pertinente e compatível em características, quantidades e prazos com o objeto da contratação, conforme previsto nos arts. 62 a 67, em especial o art. 67, que dispõe sobre a necessidade de justificativa das exigências de qualificação técnica no processo de contratação.

3.5.5.2. Considerando que a contratação envolve serviços de natureza continuada e de elevada complexidade tecnológica e operacional, com impacto direto na segurança da informação institucional, justifica-se a exigência de comprovação de aptidão técnica por meio de atestados, com vistas a assegurar que a licitante possui experiência prévia compatível com o objeto, mitigando riscos relacionados à indisponibilidade, falhas de execução, baixa qualidade técnica e prejuízos à Administração.

3.5.5.3. As exigências de qualificação técnica previstas neste Termo de Referência foram definidas de forma proporcional e adequada ao objeto, com observância aos princípios da isonomia, competitividade, eficiência, motivação, planejamento, interesse público e julgamento objetivo, previstos na Lei nº 14.133/2021, de modo a não restringir indevidamente a participação de licitantes, mas garantir a seleção da proposta mais vantajosa e a adequada execução contratual.

3.5.5.4. Assim, a exigência de atestado(s) de capacidade técnica operacional busca demonstrar que a licitante já executou serviços similares, de complexidade tecnológica e operacional equivalente ou superior, compatíveis com as características do objeto, garantindo a aptidão necessária para atendimento aos níveis mínimos de qualidade, desempenho e segurança exigidos pela Administração.

3.5.6. O(s) 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:



Poder Judiciário

Conselho Nacional de Justiça

3.5.6.1. Grupo 1 – Item 1:

- a) Experiência na prestação de serviços de proteção de tráfego de borda, incluindo a administração de solução de Firewall, UTM ou NGFW, em ambiente com, no mínimo, 1000 ativos;
- b) Experiência na prestação de serviços de administração de solução de proteção de endpoints (antivírus, EDR ou equivalente), em ambiente com, no mínimo, 1000 endpoints;
- c) Experiência na prestação de serviços de administração de solução de segurança para gateway de e-mail, contemplando proteção antimalware e anti-spam em ambiente computacional com, no mínimo, 1000 caixas postais;
- d) Experiência na prestação de serviços de administração de solução de WAF (*Web Application Firewall*), destinada à proteção de aplicações web, contemplando controle e mitigação de ataques a aplicações, em ambiente computacional compatível com aplicações críticas ou de missão institucional;
- e) Experiência na prestação de serviços de administração de segurança nas soluções de segurança hospedadas em nuvem ou para a nuvem (tais como AWS, Azure, GCP ou equivalentes).

3.5.6.2. Grupo 1 – Item 2:

- a) Experiência na prestação de serviços de gestão de vulnerabilidades, incluindo identificação, análise, priorização e tratamento das vulnerabilidades encontradas em ambientes com, no mínimo, 750 (setecentos e cinquenta) ativos;
- b) Experiência na prestação de serviços de gerenciamento de patches, contemplando identificação, priorização, aplicação e validação de correções em ambientes com, no mínimo, 750 (setecentos e cinquenta) ativos.

3.5.6.3. Grupo 1 – Item 3: Experiência na prestação de serviços de monitoramento proativo e resposta a incidentes de segurança da informação em ambientes com, no mínimo, 1000 (mil) ativos;

3.5.6.4. Grupo 1 – Item 4:

- a) Experiência na prestação de serviços de administração de solução de Gerenciamento e Correlação de Eventos de Segurança da Informação (SIEM), em ambientes com, no



Poder Judiciário

Conselho Nacional de Justiça

mínimo, 1000 (mil) ativos ou volume mínimo de 1500 eventos por segundo (EPS).

- b) Experiência na prestação de serviços de detecção e resposta a ameaças em rede (NDR ou equivalentes), contemplando monitoramento de tráfego, identificação de comportamentos anômalos e apoio à resposta a incidentes de segurança da informação.
- c) Experiência na prestação de serviços de monitoramento de superfície de ataque externa, incluindo ativos expostos na internet e coleta e análise de informações em surface web, deep web e dark web, com identificação de riscos e comunicação de achados relevantes.

3.5.6.5. Grupo 1 – Item 5: Experiência na prestação de serviços de conscientização em segurança da informação, contemplando o planejamento, a execução e a avaliação de ações de capacitação para, no mínimo, 500 (quinhentos) usuários, admitindo-se o uso de plataformas automatizadas, desde que a licitante comprove sua atuação na execução, gestão e acompanhamento das ações.

3.5.6.6. Item 6: Experiência na prestação de serviços de testes de invasão (pentest) para exploração de vulnerabilidades de segurança da informação, em conformidade com boas práticas reconhecidas de mercado, tais como OWASP, NIST, PTES ou equivalentes.

3.5.7. Para fins de habilitação nos itens do Grupo 1 (Itens 1 a 5), a licitante deverá comprovar possuir, no mínimo, uma certificação vigente relacionada à gestão de serviços ou à segurança da informação, emitida por organismo de certificação acreditado, tais como:

3.5.7.1. ISO/IEC 27001;

3.5.7.2. ISO/IEC 20000;

3.5.7.3. ISO 9001.

3.5.8. Entende-se por similar, soluções ou produtos (equipamentos ou softwares) com funcionalidades equivalentes, escalabilidade compatível e porte corporativo aos listados no ANEXO B – PLATAFORMA DE SEGURANÇA.

3.5.9. 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.



Poder Judiciário

Conselho Nacional de Justiça

- 3.5.10. Será permitido o somatório de atestados para comprovação da capacidade técnica, desde que os serviços sejam compatíveis com o objeto da contratação.
- 3.5.11. O CONTRATANTE poderá diligenciar a pessoa jurídica indicada no Atestado de Capacidade Técnica, visando validar ou esclarecer informações sobre o serviço prestado.

3.6. Critério técnico de aceitação das propostas

- 3.6.1. A proposta de preços deverá ser redigida em língua portuguesa, sem alternativas, opções, emendas, ressalvas, borrões, rasuras ou entrelinhas.
- 3.6.2. 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.
- 3.6.3. 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.
- 3.6.4. Especificação clara, completa e minuciosa da solução ou produto ofertado para os serviços dos itens 2, 4 e 5 do Grupo 1, informando o nome, a descrição e o fabricante, bem como indicação precisa da comprovação de cada característica constante nas especificações técnicas deste Termo de Referência conforme modelo de planilha constante no ANEXO J – PLANILHA DE ATENDIMENTO AOS REQUISITOS TÉCNICOS:
- 3.6.4.1. Entende-se por documento (s) a documentação técnica oficial do fabricante da solução ou produto ofertado, seja em meio eletrônico ou materializada em papel;
- 3.6.4.2. Não serão aceitas declarações ou cartas de conformidade ou adequação ao solicitado e especificado no termo de referência em substituição ou complementação da documentação técnica oficial e original.



Poder Judiciário

Conselho Nacional de Justiça

3.7. Vistoria

- 3.7.1. A participante poderá realizar vistoria técnica prévia com vistas à obtenção de informações e condições necessárias à correta elaboração da proposta e execução dos serviços e conhecimento pleno das condições e peculiaridades do objeto.
- 3.7.2. É **facultado** ao licitante comparecer as instalações do CNJ. Caso faça esta opção será fornecida pelo CNJ, ao final da visita, DECLARAÇÃO DE VISTORIA TÉCNICA (conforme modelo no ANEXO F – DECLARAÇÃO DE VISTORIA).
- 3.7.3. A vistoria poderá ser realizada até o último dia da abertura da sessão, das 12h às 19h, mediante agendamento prévio com a Comissão Permanente de Contratação, pelo telefone (61) 2326-5317/ 2326-5318 ou através do e-mail dti@cnj.jus.br, devendo, ainda, ser observado o seguinte:
 - 3.7.3.1. ser realizada por profissional especialmente credenciado como representante da participante;
 - 3.7.3.2. em nenhuma hipótese a participante poderá alegar desconhecimento, incompreensão, dúvida ou esquecimento de qualquer detalhe relativo à execução do objeto, arcando com quaisquer ônus decorrentes desses fatos;
 - 3.7.3.3. não se admitirá um mesmo profissional como representante de mais de uma participante;
 - 3.7.3.4. tendo em vista a faculdade da realização da vistoria prévia, as participantes não poderão alegar o desconhecimento das condições e graus de dificuldade existentes como justificativa para se eximirem das obrigações assumidas ou em favor de eventuais pretensões de acréscimos de preços em decorrência da execução do objeto deste Pregão. Assim, a vistoria poderá ser substituída por declaração formal assinada pelo responsável técnico da participante acerca do conhecimento pleno das condições e peculiaridades da contratação.

4. DA EXECUÇÃO E GESTÃO DO CONTRATO

4.1. Papéis desempenhados na contratação

- 4.1.1. Para a execução do contrato, é mandatório que os seguintes papéis e responsabilidades sejam definidos:



Poder Judiciário

Conselho Nacional de Justiça

- 4.1.1.1. **Autoridade competente:** Titular da Diretoria-Geral ou autoridade delegada, responsável pela assinatura do Contrato, Termo de compromisso de manutenção de Sigilo e pela publicação da equipe de fiscalização;
- 4.1.1.2. **Gestor do Contrato:** Servidor com atribuições gerenciais, técnicas ou operacionais relacionadas ao processo de gestão do contrato, indicado por autoridade competente do órgão;
- 4.1.1.3. **Fiscal Técnico do Contrato:** Servidor representante da Área de Tecnologia da Informação e Comunicação, indicado pela respectiva autoridade competente para fiscalizar o contrato quanto aos aspectos técnicos da solução;
- 4.1.1.4. **Fiscal Administrativo do Contrato:** Servidor representante da Área Administrativa, indicado pela respectiva autoridade competente para fiscalizar o contato quanto aos aspectos administrativos da execução, especialmente os referentes ao recebimento, pagamento, sanções, aderência às normas, diretrizes e obrigações contratuais.
- 4.1.1.5. **Preposto:** funcionário representante da empresa CONTRATADA, responsável por acompanhar a execução do contrato e atuar como interlocutor principal junto ao órgão contratante, incumbido de receber, diligenciar, encaminhar e responder as questões técnicas, legais e administrativas referentes ao andamento contratual; e
- 4.1.1.6. **Representante da CONTRATADA:** Responsável legal da contratada para assinatura do contrato, caso tal poder não tenha sido delegado para o preposto.
- 4.1.1.7. **Equipe Técnica da CONTRATADA:** são os profissionais, envolvidos diretamente na prestação dos serviços contratados. É de competência da Contratada utilizar mão de obra capacitada a prover os serviços do escopo deste TR.
- 4.1.2. Não poderá participar da execução do objeto, direta ou indiretamente, aquele que mantenha vínculo de natureza técnica, comercial, econômica, financeira, trabalhista ou civil com dirigente do CNJ ou com agente público que desempenhe função na licitação ou atue na fiscalização ou na gestão do objeto, ou que deles seja cônjuge, companheiro ou parente em linha reta, colateral ou por afinidade, até o terceiro grau.



Poder Judiciário

Conselho Nacional de Justiça

4.2. Formas de comunicação/acompanhamento da execução do contrato

- 4.2.1. Serão utilizados os seguintes canais de comunicação e acompanhamento da execução do contrato:
- 4.2.1.1. O canal de comunicação entre a CONTRATANTE e CONTRATADA para assuntos relacionados à gestão e fiscalização contratual, ocorrerá preferencialmente através da figura do preposto;
 - 4.2.1.2. Correio eletrônico (e-mail);
 - 4.2.1.3. Processo administrativo eletrônico no Sistema Eletrônico de Informações (SEI) do CNJ;
 - 4.2.1.4. Atas de reunião redigidas por colaborador da CONTRATADA e validadas pela equipe de gerência de TI da CONTRATANTE.
- 4.2.2. As solicitações de serviços do objeto serão realizadas seguindo as diretrizes descritas em “4.4. Instrumentos formais de solicitação do objeto (Art. 18, § 3º, III, a, 3)”.

4.3. Dinâmica da Execução do contrato

- 4.3.1. A Tabela seguinte foi elaborada com os principais marcos e eventos relevantes que ocorrerão durante a execução da contratação:

Tabela 2 – Cronograma de Execução dos Serviços

ETAPA	DESCRIÇÃO	PRAZO	ATORES	ARTEFATO	CANAL
1	Assinatura do contrato.	Até 5 dias úteis da convocação para a assinatura do contrato	DG/Preposto ou Representante da contratada	Contrato assinado	Sistema Eletrônico de Informações (SEI)
	Assinatura do Termo de compromisso de manutenção de Sigilo e Termo de Responsabilidade e Compromisso com o Código de Conduta para Fornecedores de bens e serviços do CNJ			Termo de compromisso de manutenção de Sigilo e Termo de Responsabilidade e Compromisso com o Código de Conduta para Fornecedores de bens e serviços do CNJ assinados	
2	Publicação da Equipe de Fiscalização (Fiscal Técnico do Contrato e Fiscal	Após a assinatura do contrato	DG	Portaria de designação	Sistema Eletrônico de Informações (SEI)



Poder Judiciário

Conselho Nacional de Justiça

	Administrativo do Contrato)				
3	Reunião de alinhamento – Início do período de transição	Até o 5º (quinto) dia útil após a assinatura do contrato.	Gestor do Contrato/ Preposto	Ata de reunião de alinhamento	Sistema Eletrônico de Informações (SEI)
4	Apresentação de Plano de Operacionalização dos Serviços contendo o detalhamento das ações necessárias para a absorção dos conhecimentos e repasse dos serviços (exceto o serviço do item 6 – Não agrupado)	Até 10 (dez) dias úteis após a reunião de alinhamento	Contratada	Plano de Operacionalização	Correio eletrônico (e-mail)
5	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 (exceto o serviço do item 6 – Não agrupado)	Até 15 (quinze) dias úteis após a reunião de alinhamento	Preposto	Carta de apresentação; Relação de prestadores; Cópia documentos comprobatórios de vínculo empregatício, experiência, qualificações e certificações exigidas para o perfil profissional	Correio eletrônico (e-mail)
6	Início da prestação dos serviços	Até 20 (vinte) dias úteis após reunião de alinhamento	Contratante e Contratada	Ordem de Serviço Rotineira	Sistema Eletrônico de Informações (SEI)
		Serviço Item 06 - A qualquer tempo, conforme	Contratante e Contratada	Ordem de Serviço Exclusiva	Sistema Eletrônico de Informações (SEI)



Poder Judiciário

Conselho Nacional de Justiça

		demanda do CONTRATANTE			
7	Entrega dos relatórios gerenciais de serviços (RGS)	Até o 3º (terceiro) dia útil do mês posterior à prestação do serviço	Preposto	Relatórios Gerenciais de Serviços (RGS)	Correio eletrônico (e-mail)
8	Análise dos relatórios gerenciais de serviços	Até 5 (dias) úteis após o recebimento dos RGS	Gestor do contrato/Fiscal Técnico	Notificação de avaliação do Relatório Gerencial de Serviço (RGS)	Sistema Eletrônico de Informações (SEI)/Correio eletrônico (e-mail)
9	Envio da Nota Fiscal	Até 03 (três) dias úteis após a notificação de avaliação do RGS	Preposto	Nota Fiscal	Sistema Eletrônico de Informações (SEI)
10	Atesto da Nota Fiscal	Ateste em até 7 (sete) dias úteis	Gestor do Contrato	Despacho de atesto da Nota Fiscal	Sistema Eletrônico de Informações (SEI)

- 4.3.2. Os serviços quando prestados presencialmente no CONTRATANTE, deverão ser prestados nas dependências do Conselho Nacional de Justiça, na cidade de Brasília/DF, localizadas na SAF SUL Quadra 2 Lotes 5/6 CEP: 70070-600 (edifício sede) e no SEP 514, lote 7, Bloco B – CEP: 70.760-542 ou em outro local onde o CNJ porventura venha a se estabelecer.
- 4.3.3. A CONTRATADA deverá iniciar a prestação dos serviços objeto deste termo, de acordo com os cronogramas apresentados na Tabela 2 – Cronograma de Execução dos Serviços.
- 4.3.4. 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.
- 4.3.5. 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



Poder Judiciário

Conselho Nacional de Justiça

dos níveis de serviço estabelecidos devem ser imediatamente comunicados por escrito ao CONTRATANTE.

- 4.3.6. Após a assinatura do contrato, será realizada a reunião de alinhamento, etapa inaugural do período caracterizado como período de transição, com o objetivo de viabilizar a transferência de conhecimentos e o repasse dos serviços à nova CONTRATADA.
- 4.3.7. A CONTRATADA deverá apresentar, no prazo máximo de até 15 (quinze) dias úteis a partir da reunião de alinhamento, 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 prestarão os serviços. Para o serviço do item 06 não agrupado, a documentação comprobatória deverá ser entregue quando o serviço for solicitado pela CONTRATANTE após a emissão da Ordem de Serviço, em até 05 (cinco) dias úteis.
- 4.3.8. Quando da apresentação dos documentos comprobatórios de qualificação, a CONTRATADA deverá observar atentamente à qualificação exigida, conforme descrito no Item 4.6 - Qualificação Técnica dos 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.
- 4.3.9. Para fins de comprovação de atendimento aos requisitos de qualificação profissional serão aceitos:
 - 4.3.9.1. Cópia simples de certificados ou diplomas, acompanhado do original, ou 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;
 - 4.3.9.2. Todos os documentos apresentados estarão sujeitos à diligência do CONTRATANTE para fins de confirmação das informações prestadas;
 - 4.3.9.3. Caso uma certificação não seja mais válida, será aceita a nova certificação que substituiu a anterior;
 - 4.3.9.4. As certificações técnicas exigidas devem estar válidas.
- 4.3.10. O CNJ 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



Poder Judiciário

Conselho Nacional de Justiça

contar da data de recusa para apresentar a documentação do novo profissional.

- 4.3.11. 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.
- 4.3.12. A CONTRATADA deverá iniciar a prestação dos serviços em, no máximo, 20 (vinte) dias úteis após a realização da reunião de alinhamento (Início do período de transição), exceto o serviço do item 06 não agrupado, que poderá ser solicitado pela CONTRATANTE a qualquer tempo (sob demanda) após a Reunião de alinhamento e não haverá período de transição.
- 4.3.13. 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 Tabela 2 – Cronograma de Execução dos Serviços.
- 4.3.14. Desde já fica estabelecido que o contrato será considerado rescindido, bem como serão aplicadas as sanções contratuais, caso a empresa vencedora deixe de apresentar (exceto para o serviço do item 06 não agrupado):
 - 4.3.14.1. Plano de Operacionalização dos Serviços, no prazo de até 10 (dez) dias úteis corridos após a realização da reunião de alinhamento, contendo o detalhamento das ações necessárias para a absorção dos conhecimentos, e repasse dos serviços;
 - 4.3.14.2. Documentação com a relação completa dos profissionais que prestarão serviço, no prazo de até 15 (dias) úteis após a realização da reunião de alinhamento, acompanhada das devidas comprovações de qualificação e experiência exigidas para cada perfil estabelecido neste Termo de Referência e seus anexos.
- 4.3.15. 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 das tabelas do ANEXO C – NÍVEIS MÍNIMOS DE SERVIÇO conforme os seguintes critérios:
 - 4.3.15.1. Nos primeiros 30 (trinta) dias: aplicar-se-á efetivamente 25% (vinte e cinco por cento) dos pontos previstos na tabela do ANEXO C – NÍVEIS MÍNIMOS DE SERVIÇO para cada ocorrência de indicador de serviço não atingido;



Poder Judiciário

Conselho Nacional de Justiça

- 4.3.15.2. Do 31º ao 60º dia: aplicar-se-á efetivamente 50% (cinquenta por cento) dos pontos previstos na tabela do ANEXO C – NÍVEIS MÍNIMOS DE SERVIÇO para cada ocorrência de indicador de serviço não atingido;
- 4.3.15.3. Do 61º ao 90º dia: aplicar-se-á efetivamente 75% (setenta e cinco por cento) dos pontos previstos na tabela do ANEXO C – NÍVEIS MÍNIMOS DE SERVIÇO para cada ocorrência de indicador de serviço não atingido;
- 4.3.15.4. Após 90 (noventa): aplicar-se-ão integralmente os pontos previstos na tabela do ANEXO C – NÍVEIS MÍNIMOS DE SERVIÇO para cada ocorrência de indicador de serviço não atingido.
- 4.3.16. Caso haja prorrogação da vigência contratual, não haverá novo período de estabilização.
- 4.3.17. Ao final do contrato de prestação dos serviços, a empresa CONTRATADA deverá 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.
- 4.3.18. 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.
- 4.3.19. Quando houver necessidade de qualquer alteração na equipe de profissionais que prestam o serviços contratados, a CONTRATADA deverá apresentar os documentos comprobatórios de qualificação



Poder Judiciário

Conselho Nacional de Justiça

deste(s) profissional(ais) antes do início de suas atividades no CONTRATANTE.

4.3.20. Todos os profissionais da CONTRATADA alocados para a prestação dos serviços do objeto deverão ter vínculo com a CONTRATADA.

4.4. Instrumentos formais de solicitação do objeto

4.4.1. Os serviços deverão ser executados após a emissão de Ordens de Serviços, com a obrigatória autorização pelo CONTRATANTE, ou após abertura de chamado na central de serviços.

4.4.2. Solicitações por meio da central de serviços:

4.4.2.1. Todos os serviços do CNJ, excetuando-se os realizados por meio de Ordens de Serviço (4.4.3), deverão ser solicitados por meio da abertura de chamados por meio de sistema de acompanhamento de chamados (central de serviços), provido pela CONTRATADA para gestão dos serviços, preferencialmente, via sistema de informação na web. Destacam-se, mas não se limitam, os serviços descritos no ANEXO A – “2.3. Processo de atendimento para cumprimento de requisição de serviços”, “3.2. Processo de Gestão de Vulnerabilidades” e “4.2. Processo de resposta a incidente de segurança da informação”.

4.4.2.2. As solicitações de serviço também podem ser efetuadas por outros meios, tais como e-mail, telefone e WhatsApp (ou similares), cabendo a CONTRATADA registrar os chamados no sistema de acompanhamento de chamados.

4.4.2.3. Os chamados poderão ser abertos a qualquer hora do dia ou da noite, tanto em dias úteis, como nos finais de semana, feriados e pontos facultativos, e devem ser executados de acordo com os níveis de serviços estabelecidos neste Termo de Referência.

4.4.2.4. A CONTRATADA deverá ainda indicar endereços eletrônicos para recebimentos de chamados de suporte e demais comunicações para abertura de chamados sem intervenção humana.

4.4.2.5. Os chamados, especialmente os incidentes, podem ser abertos automaticamente na central de serviços pelas ferramentas de monitoramento existentes no ambiente da CONTRATANTE ou pelas ferramentas da CONTRATADA, em qualquer caso configuradas com o auxílio da CONTRATADA.



Poder Judiciário

Conselho Nacional de Justiça

- 4.4.2.6. Uma notificação da abertura dos chamados abertos será encaminhada para endereços eletrônicos indicados pela CONTRATANTE que fará uso do sistema de gestão de chamados, para atualizar as informações relacionadas ao atendimento de cada chamado.
- 4.4.2.7. Ao abrir um chamado, o CNJ poderá agendar data e hora para início do atendimento para a prestação do serviço.
- 4.4.2.8. Em caso de indisponibilidade do sistema de acompanhamento de chamados disponibilizado pela CONTRATADA, os chamados poderão ser abertos por meio de número de telefone local (DDD 61) ou de discagem gratuita (0800), e-mail e WhatsApp (ou similares) fornecidos pela CONTRATADA.
- 4.4.2.9. Todas as solicitações recepcionadas devem gerar um número de protocolo referente ao registro do atendimento no sistema de gerenciamento de chamado fornecido pela CONTRATADA, o que propicia a contabilização posterior dos contatos realizados e a extração de relatórios.
- 4.4.2.10. Os chamados deverão ser gerenciados exclusivamente por meio de chamado técnico, contendo, no mínimo, as seguintes informações: número de identificação exclusivo; data e hora do início da ocorrência; descrição da ocorrência; nível de severidade; providências adotadas para o diagnóstico; indicação de solução provisória e/ou definitiva; data e hora do término da ocorrência, com solução definitiva; identificação do técnico do CNJ que solicitou e validou o chamado técnico; identificação do técnico da contratada responsável pela execução do chamado técnico, bem como outras informações pertinentes.
- 4.4.3. Solicitação de serviços por meio de Ordens de Serviços (ANEXO D - MODELO ORDEM DE SERVIÇO):
- 4.4.3.1. As Ordens de Serviços deverão ser classificadas pelo CONTRATANTE, conforme nível e continuidade de execução:
- 4.4.3.1.1. 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;
- 4.4.3.1.2. Exclusiva:** atividades de natureza não contínua, emitidas a partir da demanda do CONTRATANTE.



Poder Judiciário

Conselho Nacional de Justiça

4.4.3.2. Nas Ordens de Serviços deverão constar:

- 4.4.3.2.1. Número de controle: identificação em ordem sequencial;
- 4.4.3.2.2. Área demandante: que deverá assinar a solicitação e o aceite e contabilização periódica das atividades, para efeito dos pagamentos;
- 4.4.3.2.3. Objetivo da tarefa: definição das expectativas e justificativas para realização das atividades;
- 4.4.3.2.4. 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;
- 4.4.3.2.5. Listagem das atividades a serem realizadas, especificadas, quantificadas e classificadas conforme complexidade;
- 4.4.3.2.6. Resultado e Nível de Qualidade definido para a tarefa;
- 4.4.3.2.7. Glosa e Penalidades, em caso de descumprimento, e de acordo com a previsão contratual;
- 4.4.3.2.8. Responsáveis pela fiscalização e autorização no CONTRATANTE;
- 4.4.3.2.9. Responsável pelo aceite na CONTRATADA.

4.4.3.3. Atestação técnica:

- 4.4.3.3.1. 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 CONTRATANTE;
- 4.4.3.3.2. Antes do fechamento de cada OS a CONTRATADA consultará o representante indicado pelo CONTRATANTE, que avaliará e atestará o serviço realizado;
- 4.4.3.3.3. 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.

4.5. Níveis de Serviços Exigidos (NSE)

- 4.5.1. A prestação dos serviços será baseada no modelo de remuneração em função dos resultados apresentados, em que os pagamentos serão feitos após a mensuração e verificação de métricas quantitativas e qualitativas, contendo indicadores de desempenho e metas, com Nível Mínimo de



Poder Judiciário

Conselho Nacional de Justiça

Serviço (NMS) definido em contrato, de modo a resguardar a eficiência e a qualidade na prestação dos serviços.

- 4.5.2. 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.
- 4.5.3. Os níveis mínimos de serviços estão detalhados no ANEXO C – NÍVEIS MÍNIMOS DE SERVIÇO.
- 4.5.4. 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 aplicação das Sanções Administrativas previstas neste Termo de Referência.
- 4.5.5. A CONTRATADA sofrerá glosa de 1% (um por cento), sobre o valor da fatura, a cada 20 pontos ou percentual proporcional ao número de pontos, levando em consideração a relação: glosa de 1% a cada 20 pontos.
- 4.5.6. As metas devem ser medidas do primeiro ao último dia de cada mês.
- 4.5.7. 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.
- 4.5.8. 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.
- 4.5.9. 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.
- 4.5.10. Os níveis de serviço serão mensurados de forma automatizada e não poderão ser manipulados pela CONTRATADA.
- 4.5.11. 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.
- 4.5.12. O termo “Hora do restabelecimento” refere-se a hora em que o incidente de indisponibilidade foi efetivamente resolvido.



Poder Judiciário

Conselho Nacional de Justiça

- 4.5.13. 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.
- 4.5.14. Por horário normal de produção entende-se sendo o período entre 08:00 e 20:00, de segunda à sexta-feira, excetuando-se os feriados.
- 4.5.15. Sobre o índice de supervisão e intervenção proativa:
- 4.5.15.1. 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 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;
- 4.5.15.2. 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;
- 4.5.15.3. 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.
- 4.5.16. A fiscalização técnica dos contratos deve avaliar constantemente a execução do objeto e, se for o caso, utilizará o Instrumento de Avaliação dos Serviços, conforme Tabela 3 – Instrumento de Avaliação dos Serviços, para aferição da qualidade da prestação dos serviços, devendo haver o redimensionamento no pagamento com base nos indicadores estabelecidos, sempre que a contratada:
- 4.5.16.1. Não produzir os resultados, deixar de executar, ou não executar com a qualidade mínima exigida as atividades contratadas;



Poder Judiciário

Conselho Nacional de Justiça

4.5.16.2. Deixar de utilizar materiais e recursos humanos exigidos para a execução do serviço, ou utilizá-los com qualidade ou quantidade inferior à demandada.

INDICADOR	
Nº + Título do Indicador que será utilizado	
Item	Descrição
Finalidade	
Metas a cumprir	
Instrumento de medição	
Forma de acompanhamento	
Periodicidade	
Mecanismo de Cálculo	
Início da Vigência	
Faixas de ajustes no pagamento	
Sanções	

Tabela 3 – Instrumento de Avaliação dos Serviços

4.6. Qualificação Técnica dos Profissionais

- 4.6.1. A CONTRATADA deverá dimensionar adequadamente a sua equipe de profissionais de forma a atingir os níveis de serviço estabelecidos neste Termo de Referência e seus anexos.
- 4.6.2. Todos os profissionais deverão possuir qualificação plena e conhecimento técnico compatível com a complexidade das demandas a serem atendidas.
- 4.6.3. A formação da equipe de profissionais é de exclusiva responsabilidade da CONTRATADA e serão gerenciados exclusivamente pelo PREPOSTO da empresa.
- 4.6.4. Os profissionais deverão conhecer o funcionamento dos negócios internos do DTI, e respectivas áreas do CNJ, bem como executar os procedimentos de acordo com as regras de segurança da informação.
- 4.6.5. Os profissionais deverão utilizar vestimenta compatível com a utilizada pelos servidores do CNJ e portar crachá de identificação durante toda a prestação de serviço nas dependências do CNJ.
- 4.6.6. Durante a execução dos serviços, a CONTRATADA se obriga, durante a execução do Contrato, a manter todos os profissionais com as



Poder Judiciário

Conselho Nacional de Justiça

qualificações especificadas no ANEXO A – ESPECIFICAÇÃO DOS REQUISITOS TÉCNICOS.

- 4.6.7. A comprovação das qualificações especificadas no ANEXO A – ESPECIFICAÇÃO DOS REQUISITOS TÉCNICOS, será na forma como preconizado no item 4.3.9.
- 4.6.8. Todos os documentos apresentados estarão sujeitos à diligência do CONTRATANTE para fins de confirmação das informações prestadas.
- 4.6.9. A CONTRATADA deverá promover, no prazo máximo de **04 (quatro) 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.

4.7. Forma de recebimento dos serviços e qualidade

- 4.7.1. O recebimento de todos os serviços do objeto seguirá os prazos estabelecidos na [Tabela 2 – Cronograma de Execução dos Serviços](#)
 - 4.7.1.1. Os serviços serão recebidos definitivamente em até 5 (dias) úteis após o recebimento do RGS (Relatórios Gerenciais de Serviços), prazo em que o fiscal do contrato deverá fazer a apuração dos chamados/pedidos atendidos pela CONTRATADA e emitir notificação de avaliação do RGS contendo a verificação de sua conformidade com as especificações constantes neste Termo de Referência.
 - 4.7.1.2. Os serviços poderão ser rejeitados, no todo ou em parte, quando em desacordo com as especificações constantes neste Termo de Referência e no contrato, devendo ser corrigidos/refeitos/substituídos no prazo fixado pelo fiscal do contrato, às custas da CONTRATADA, sem prejuízo da aplicação de penalidades.
 - 4.7.1.3. O gestor do contrato analisará os relatórios e toda documentação apresentada pela fiscalização técnica e, caso haja irregularidades que impeçam a liquidação e o pagamento da despesa, indicará as cláusulas contratuais pertinentes, solicitando à CONTRATADA, por escrito, as respectivas correções.
 - 4.7.1.4. O gestor emitirá termo circunstanciado para efeito de recebimento dos serviços prestados, com base nos relatórios e documentação apresentados, e comunicará a CONTRATADA para que emita a Nota Fiscal em até 03 (três) dias úteis após a notificação



Poder Judiciário

Conselho Nacional de Justiça

de avaliação do RGS com o valor exato dimensionado pela fiscalização com base no conjunto de indicadores de nível de serviço e desempenho.

4.7.1.5. As ocorrências relacionadas à execução do contrato deverão ser registradas em sistema ou instrumento próprio de acompanhamento e fiscalização, para fins de controle, gestão e adoção das providências necessárias ao fiel cumprimento das cláusulas contratuais, nos termos do art. 117 e do art. 119 da Lei nº 14.133/2021.

4.7.1.6. O recebimento do serviço não exclui a responsabilidade civil pela solidez e segurança dos serviços prestados nem a ético-profissional pela perfeita execução do contrato, dentro dos limites estabelecidos pela lei.

4.7.1.7. O modelo do Termo de Recebimento do Serviço encontra-se no ANEXO E - MODELO DE TERMO DE RECEBIMENTO DEFINITIVO DO SERVIÇO.

4.7.2. A avaliação de qualidade dos serviços será realizada sob o aspecto de atendimento ao padrão de qualidade dos serviços exigido pelo CNJ, portanto, a CONTRATADA deverá:

4.7.2.1. Prestar os serviços dentro dos parâmetros e rotinas estabelecidos, com observância às recomendações aceitas pela boa técnica, *frameworks*, normas e legislação, bem como observar conduta adequada na utilização dos materiais, equipamentos e ferramentas;

4.7.2.2. Fiscalizar regularmente os seus recursos técnicos designados para a prestação dos serviços verificando as condições em que as atividades estão sendo realizadas;

4.7.2.3. Refazer todos os serviços que, a juízo do representante do CNJ, de forma fundamentada, não forem considerados satisfatórios, sem que caiba qualquer acréscimo no custo contratado, independentemente das penalidades previstas;

4.7.2.4. Executar fielmente o objeto contratado de acordo com as normas legais, em conformidade com a proposta apresentada e com as orientações do CNJ, observando sempre os critérios de qualidade.



Poder Judiciário

Conselho Nacional de Justiça

- 4.7.3. Ainda, objetivando atender ao padrão de qualidade dos serviços e produtos entregues, a CONTRATADA deverá:
- 4.7.3.1. Efetuar adequação das instalações e procedimentos realizados quanto à eficiência, eficácia, ocorrência de reincidência, segurança, conformidade com as boas práticas e normas aplicáveis;
 - 4.7.3.2. Adequar a redação de documentos e relatórios quanto à clareza, objetividade, detalhamento técnico e conformidade com as boas práticas e normas aplicáveis;
 - 4.7.3.3. Caso os produtos entregues estejam fora dos padrões de qualidade será exigida a readequação dos mesmos, sem prejuízo das penalidades aplicáveis.

4.8. Forma de Pagamento

- 4.8.1. Os pagamentos dos serviços do grupo 1 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.
- 4.8.2. O pagamento do serviço do item 6 não agrupado ocorrerá a qualquer tempo conforme quantidade de sistemas demandados, após a efetiva realização dos procedimentos solicitados e a apresentação da referida Ordem de Serviço devidamente preenchida e assinada junto com o Relatório gerenciais de serviços - RGS.
- 4.8.3. 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.
 - 4.8.3.1. O documento fiscal deverá ser obrigatoriamente registrado no Portal do SIGEO-JT para efeito de atesto, liquidação e pagamento, sem prejuízo da entrega no Protocolo do CNJ, ou do envio por e-mail.
- 4.8.4. 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 03 (três) dias úteis da manifestação.



Poder Judiciário

Conselho Nacional de Justiça

- 4.8.5. A CONTRATADA só receberá pelos serviços que compõe o objeto contratual se houver abertura de Ordem de Serviço. Portanto, caso não haja a abertura de Ordem de Serviço em determinado mês ou período não haverá pagamento.
- 4.8.6. Obedecendo a pontuação atribuída no ANEXO C – NÍVEIS MÍNIMOS DE SERVIÇO para cada inadimplemento, o CONTRATANTE aplicará glosa de 1% (um por cento) sobre o valor da nota fiscal a cada 20 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.
- 4.8.7. A nota de cobrança emitida pela CONTRATADA deverá ser atestada em até 7 (sete) dias úteis pelo Gestor do contrato e encaminhada à área financeira para efetuar o pagamento, acompanhada dos relatórios gerenciais de serviços e documentação comprobatória do não atendimento dos resultados ou níveis de serviço exigidos.
- 4.8.8. 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.
- 4.8.9. O pagamento será realizado por meio de ordem bancária, para crédito em banco, agência e conta corrente indicados pelo contratado, no prazo de até 10 (dez) dias úteis contados da liquidação da despesa, nos termos da [Instrução Normativa SEGES/ME nº 77, de 2022](#), cumpridos os seguintes requisitos:
- 4.8.9.1. Apresentação de nota fiscal de acordo com a legislação vigente à época da emissão, acompanhada da Certidão Negativa de Débito – CND, comprovando regularidade com o INSS; do Certificado de Regularidade do FGTS – CRF, comprovando regularidade com o FGTS; da Certidão Conjunta Negativa de Débitos Relativos a Tributos Federais e à Dívida Ativa da União, expedida pela Secretaria da Receita Federal; e da Certidão Negativa de Débitos Trabalhistas – CNDT, emitida pela Justiça do Trabalho; e de prova de regularidade com as Fazendas Estadual e Municipal do domicílio ou sede da empresa.
- 4.8.10. Para os inadimplementos que não estão previstos ANEXO C – NÍVEIS MÍNIMOS DE SERVIÇO, o CONTRATANTE abrirá processo administrativo e seguirá o rito definido nas SANÇÕES ADMINISTRATIVAS.



Poder Judiciário

Conselho Nacional de Justiça

- 4.8.11. O pagamento também está condicionado a inexistência de fato impeditivo para o qual tenha concorrido.
- 4.8.12. Antes de cada pagamento à CONTRATADA, será realizada consulta ao SICAF para verificar a manutenção das condições de habilitação exigidas no edital.
- 4.8.13. Constatando-se, junto ao SICAF, a situação de irregularidade da CONTRATADA, será providenciada sua advertência, por escrito, para que, no prazo de 5 (cinco) dias, regularize sua situação ou, no mesmo prazo, apresente sua defesa. O prazo poderá ser prorrogado uma vez, por igual período, a critério da CONTRATANTE.
- 4.8.14. Não havendo regularização ou sendo a defesa considerada improcedente, a contratante deverá comunicar aos órgãos responsáveis pela fiscalização da regularidade fiscal quanto à inadimplência da CONTRATADA, bem como quanto à existência de pagamento a ser efetuado, para que sejam acionados os meios pertinentes e necessários para garantir o recebimento de seus créditos.
- 4.8.15. Persistindo a irregularidade, a contratante deverá adotar as medidas necessárias à rescisão contratual nos autos do processo administrativo correspondente, assegurada à contratada a ampla defesa.
- 4.8.16. Havendo a efetiva execução do objeto, os pagamentos serão realizados normalmente, até que se decida pela rescisão do contrato, caso a contratada não regularize sua situação junto ao SICAF.
- 4.8.17. Quando do pagamento, será efetuada a retenção tributária prevista na legislação aplicável.
- 4.8.18. As microempresas ou empresas de pequeno porte, optantes pelo Simples Nacional, poderão participar do certame, mas não poderão apresentar proposta com os benefícios da condição de optante e, caso venham a ser contratadas, estarão sujeitas à exclusão obrigatória do referido regime de tributação, em consequência do que dispõem o art. 17, inciso XII, o art. 30, inciso II, e o art. 31, inciso II, da Lei Complementar nº 123/2006.

4.9. Transferência de Conhecimento

- 4.9.1. A transferência de conhecimento será feita mediante a prestação de informações contidas nos Relatórios Gerenciais de Serviço (RGS).



Poder Judiciário

Conselho Nacional de Justiça

- 4.9.2. Os conhecimentos técnicos repassados para a equipe do Departamento de Tecnologia da Informação serão utilizados em casos de interrupção, transição e encerramento contratual, de modo a minimizar impactos e permitir que as necessidades do CNJ não sejam prejudicadas ou interrompidas.
- 4.9.3. O processo de transição do contrato se inicia a partir do momento em que a empresa a ser contratada assumir as responsabilidades, de forma gradual, pelos serviços prestados, preparando-se para o início efetivo da operação. Esse processo de transição contratual tem o propósito de preparar a empresa contratada a assumir integralmente as obrigações advindas com o contrato, e será baseada em reuniões e repasse de documentos técnicos e/ou manuais específicos das soluções adquiridas.
- 4.9.4. Ao final do contrato de prestação dos serviços, a empresa contratada deverá fornecer, pelo período de 90 (noventa) dias corridos, todas as informações necessárias à transição para a empresa sucessora à prestação dos serviços, 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.
- 4.9.5. A empresa 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.

4.10. Direitos de Propriedade Intelectual

- 4.10.1. Os conhecimentos produzidos no Relatório Gerencial de Serviço (RGS) serão de propriedade intelectual do CNJ.
- 4.10.2. Os direitos autorais e os direitos de propriedade intelectual da Solução de Tecnologia da Informação sobre os diversos artefatos e produtos produzidos ao longo do contrato, incluindo a documentação, o código fonte de aplicações, os modelos de dados e as bases de dados, pertencerão ao CNJ, devendo ser justificado os casos em que isso não ocorrer.
- 4.10.3. Portanto a empresa CONTRATADA cederá os direitos de propriedade intelectual e direitos autorais da Solução de Tecnologia da Informação sobre os diversos artefatos e produtos produzidos ao longo do contrato, incluindo a documentação, os modelos de dados e as bases de dados do CNJ.



Poder Judiciário

Conselho Nacional de Justiça

4.11. Obrigações da Contratante

- 4.11.1. O CNJ 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.
- 4.11.2. 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 CNJ.
- 4.11.3. Solicitar a substituição do profissional que tenha infringido às normas do CNJ, ainda que em parte, dos itens indicados no item 4.12 - Obrigações da Contratada.
- 4.11.4. Permitir acesso dos prestadores de serviço da CONTRATADA às suas dependências, aos equipamentos, softwares e sistemas de informação para a execução dos serviços contratados.
- 4.11.5. Comunicar oficialmente à CONTRATADA, quaisquer falhas verificadas no cumprimento do contrato.
- 4.11.6. Avaliar mensalmente o relatório gerencial de serviços, observando os indicadores e metas de níveis de serviço alcançados.
- 4.11.7. 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.
- 4.11.8. Fornecer as normas, rotinas, procedimentos e processos desenvolvidos pelo CNJ para que a CONTRATADA promova os devidos ajustes e implementações adicionais.
- 4.11.9. Prestar, por meio de seu gestor do contrato, as informações e os esclarecimentos pertinentes ao objeto contratado que venham a ser solicitados pela contratada, utilizando-se das formas de comunicação estabelecidas neste termo de referência.
- 4.11.10. Efetuar o pagamento devido nos prazos estipulados em cada etapa da execução e gestão do contrato, desde que cumpridas todas as formalidades e exigências contratuais, bem com as deste Termo de Referência.
- 4.11.11. Proporcionar os recursos técnicos e logísticos necessários para que a contratada possa executar os serviços conforme as especificações estabelecidas neste Termo de Referência.



Poder Judiciário

Conselho Nacional de Justiça

- 4.11.12. Exercer permanente fiscalização na execução do objeto, registrando ocorrências relacionadas a falhas no cumprimento do contrato, determinando ao preposto ou ao representante da contratada as medidas necessárias à sua regularização.
- 4.11.13. Proporcionar todas as facilidades indispensáveis ao bom cumprimento das obrigações contratuais.
- 4.11.14. Aplicar as penalidades previstas neste Termo de Referência, assegurando à contratada o contraditório e a ampla defesa.

4.12. Obrigações da Contratada

- 4.12.1.A CONTRATADA deverá atender aos Níveis Mínimos de Serviço estabelecidos pelos indicadores contidos no ANEXO C – NÍVEIS MÍNIMOS DE SERVIÇO deste Termo de Referência.
- 4.12.2.Cumprir os normativos e os procedimentos definidos pelo CONTRATANTE.
- 4.12.3.A CONTRATADA deverá declarar, no ato da assinatura do contrato, ciência do Código de Conduta dos servidores do Conselho Nacional de Justiça, instituído pela Portaria CNJ n. 56/2018.
- 4.12.4.A CONTRATADA deverá declarar no ato da assinatura do contrato ciência do Código de Conduta dos Fornecedores de Bens e Serviços para o Conselho Nacional de Justiça, por meio do Termo de Responsabilidade e compromisso com o Código de Conduta dos Fornecedores e compradores, instituído pela Portaria CNJ n. 18/01/2020 previsto no ANEXO K - TERMO DE RESPONSABILIDADE E COMPROMISSO COM O CÓDIGO DE CONDUTA PARA FORNECEDORES DE BENS E SERVIÇOS DO CONSELHO NACIONAL DE JUSTIÇA.
- 4.12.5.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.
- 4.12.6.Executar todos os serviços, tarefas e atividades demandadas pelo CONTRATANTE dentro do prazo contratado, atendendo o padrão de qualidade exigido.



Poder Judiciário

Conselho Nacional de Justiça

- 4.12.7. 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.
- 4.12.8. Os serviços deverão ser realizados em conformidade com os horários e períodos determinados pelo CONTRATANTE.
- 4.12.9. Elaborar relatório gerencial de serviços, apresentando-o ao CONTRATANTE, até o terceiro dia útil do mês subsequente ao da prestação dos serviços, devendo constar, quando aplicável ao objeto do contrato, dentre outras informações:
- 4.12.9.1. Os indicadores e níveis de serviços alcançados em relação ao previsto ANEXO C – NÍVEIS MÍNIMOS DE SERVIÇO deste Termo de Referência;
 - 4.12.9.2. Relatório de análise e diagnóstico das causas (causa raiz) dos incidentes e problemas ocorridos;
 - 4.12.9.3. Manutenções evolutivas e corretivas realizadas;
 - 4.12.9.4. Erros operacionais;
 - 4.12.9.5. Sugestões de melhorias;
 - 4.12.9.6. Painel de volumetria de chamados (requisições de serviço, incidentes, problemas etc.) divididos por grupos solucionadores e responsáveis, demonstrando graficamente a evolução destas informações;
 - 4.12.9.7. Indicadores de aferição da qualidade de novos produtos e/ou serviços que venham a ser implantados no decorrer da vigência contratual;
 - 4.12.9.8. Demais informações relevantes para as atividades demandadas nas Ordens de Serviços;
 - 4.12.9.9. Estatísticas de tratamento de e-mails suspeitos, spam etc.;
 - 4.12.9.10. Estatísticas de tratamento de malware (vírus, worms, trojan horses, spyware etc.);
 - 4.12.9.11. Relatório de resultados obtidos em testes de invasão;
 - 4.12.9.12. Relatório de vulnerabilidades de segurança nos sistemas de informação, aplicativos e serviços de TI;



Poder Judiciário

Conselho Nacional de Justiça

- 4.12.9.13. Sugestões de mitigação das vulnerabilidades de segurança encontradas;
 - 4.12.9.14. Eventos de segurança;
 - 4.12.9.15. Ações tomadas em reação aos eventos de segurança;
 - 4.12.9.16. Sugestões de mitigação de riscos.
- 4.12.10. Submeter seus profissionais aos regulamentos de segurança e disciplina instituídos pelo CONTRATANTE, durante o tempo de permanência nas suas dependências.
- 4.12.11. Responsabilizar-se por solicitar o credenciamento e credenciamento de acesso físico e lógico às dependências do CONTRATANTE bem como assumir quaisquer prejuízos porventura causados por seus profissionais.
- 4.12.12. 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.
- 4.12.13. Os serviços deverão ser prestados de forma ininterrupta, portanto o afastamento mencionado no subitem anterior não poderá prejudicar a qualidade dos serviços e nem descumprir quaisquer cláusulas contratuais.
- 4.12.14. Manter um Diário de Ocorrências que conste nos registros as eventuais ocorrências diárias relativas à execução dos trabalhos.
- 4.12.15. Selecionar e treinar adequadamente os profissionais alocados para prestação dos serviços, observando a boa conduta e a idoneidade moral destes.
- 4.12.16. 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.



Poder Judiciário

Conselho Nacional de Justiça

- 4.12.17. 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 CNJ, deverá ser comprovada por currículos e certificados oficiais.
- 4.12.18. Substituir por outro profissional de qualificação igual ou superior qualquer um dos seus profissionais cuja qualificação, atuação, permanência ou comportamento decorrentes da execução do objeto forem julgados prejudiciais, inconvenientes ou insatisfatórios à disciplina do órgão ou ao interesse do serviço público, sempre que exigido pelo Gestor do Contrato do CNJ.
- 4.12.19. A seleção, a designação e a manutenção do quadro de profissionais alocados ao contrato são de exclusiva responsabilidade da CONTRATADA.
- 4.12.20. Fiscalizar regularmente os seus profissionais designados para a prestação dos serviços verificando as condições em que as atividades estão sendo realizadas.
- 4.12.21. 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.
- 4.12.22. 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.
- 4.12.23. A CONTRATADA e seus profissionais que prestarão os serviços deverão assinar o Termo de Responsabilidade conforme modelo ANEXO G – TERMO DE CIÊNCIA INDIVIDUAL e ANEXO H - MODELO DE TERMO DE COMPROMISSO DE MANUTENÇÃO DE SIGILO e manter em caráter confidencial, mesmo após o término do prazo de vigência ou rescisão do contrato, as informações relativas:
- 4.12.23.1. As políticas e procedimentos de segurança da informação adotados pelo CONTRATANTE;
 - 4.12.23.2. As configurações de hardwares, de softwares, produtos, ferramentas e equipamentos;
 - 4.12.23.3. Aos processos internos do CONTRATANTE;
 - 4.12.23.4. As vulnerabilidades dos ativos de informação do CNJ;



Poder Judiciário

Conselho Nacional de Justiça

4.12.23.5. Mecanismos de criptografia e autenticação.

- 4.12.24. Acatar as determinações feitas pela fiscalização do CONTRATANTE no que tange ao cumprimento do objeto deste contrato.
- 4.12.25. Prestar, de imediato, todos os esclarecimentos solicitados pela fiscalização do CONTRATANTE no que diz respeito a execução do objeto contratado.
- 4.12.26. 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.
- 4.12.27. Permitir auditoria pelo CONTRATANTE, ou terceiro por ela designado, inclusive com a possibilidade de os atendimentos serem monitorados para verificação de procedimentos.
- 4.12.28. 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 DTI.
- 4.12.29. 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:
- 4.12.29.1. Assegurar de que as determinações do CNJ sejam disseminadas junto aos profissionais alocados com vistas à execução dos serviços contratados;
- 4.12.29.2. Informar formalmente e imediatamente ao gestor do contrato quaisquer problemas, anormalidades, erros e irregularidades que possam comprometer a execução do objeto, utilizando-se das formas de comunicação estabelecidas neste termo de referência;
- 4.12.29.3. 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;
- 4.12.29.4. O preposto não poderá ser contabilizado como profissional para execução dos serviços contratados;
- 4.12.29.5. Após a assinatura do contrato, conhecer o parque tecnológico e as atividades em andamento, visando à preparação da equipe que



Poder Judiciário

Conselho Nacional de Justiça

irá prestar os serviços, conhecer os modelos de serviços realizados, as normas internas, procedimentos de segurança e a definição dos requisitos necessários;

4.12.29.6. Deverá estar disponível, de segunda a sexta-feira, das 09 (nove) às 19 (dezenove) horas, e acessível por contato telefônico em qualquer outro horário;

4.12.29.7. 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;

4.12.29.8. 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.

4.12.30. 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.

4.12.31. Responsabilizar-se pela manutenção da limpeza e conservação dos ambientes onde desempenhe seus serviços.

4.12.32. 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.

4.12.33. 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.

4.12.34. Prestar os serviços de forma ininterrupta, em conformidade com o demandado pelas Ordens de Serviço.

4.12.35. Assumir todas as despesas relativas à execução dos serviços, tais como taxas, emolumentos e encargos sociais.

4.12.36. 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.

4.12.37. Cumprir às suas próprias expensas todas as cláusulas contratuais que definam suas obrigações.



Poder Judiciário

Conselho Nacional de Justiça

- 4.12.38. A CONTRATADA e seus profissionais que prestarão os serviços deverão assinar declaração de não nepotismo, conforme modelo do ANEXO I – DECLARAÇÃO DE NÃO-NEPOTISMO.
- 4.12.39. 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.
- 4.12.40. 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.
- 4.12.41. 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.
- 4.12.42. Responsabilizar-se por todos os encargos fiscais e comerciais resultantes desta contratação.
- 4.12.43. 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.
- 4.12.44. 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.
- 4.12.45. Responder integralmente por quaisquer perdas ou danos causados ao CNJ ou a terceiros, em decorrência de ação ou omissão, dolosa ou culposa, própria ou de seus empregados, prepostos ou profissionais vinculados à execução do objeto contratual, independentemente da aplicação de outras sanções contratuais ou legais, nos termos do art. 120 da Lei nº 14.133/2021.
- 4.12.46. Cumprir integralmente as disposições, condições e exigências previstas no edital de licitação, no termo de referência, na proposta apresentada e nos demais anexos, os quais passam a integrar o contrato para todos os fins, nos termos da Lei nº 14.133/2021.



Poder Judiciário

Conselho Nacional de Justiça

- 4.12.47. Manter, durante toda a execução do contrato, em compatibilidade com as obrigações assumidas, todas as condições de habilitação e qualificação exigidas no procedimento licitatório, comprovando-as sempre que solicitado pela Administração, nos termos do art. 92, inciso XVI, e do art. 156 da Lei nº 14.133/2021.
- 4.12.48. Não está prevista subcontratação parcial de outra empresa para a execução do objeto desta contratação, devido características técnicas de agrupamento dos itens que o compõe.
- 4.12.49. Manter seus profissionais nas dependências do CNJ adequadamente trajados e identificados com uso permanente de crachá, com foto e nome visível, de acordo com as regras estabelecidas na [Instrução Normativa CNJ nº 2, de 19/08/2020](#).
- 4.12.50. Cumprir as instruções e orientações emitidas pelo gestor e/ou fiscal do contrato, bem como reparar, corrigir, remover ou substituir, às suas expensas, no todo ou em parte, os bens, serviços ou entregas que constituem o objeto contratual, sempre que forem constatados vícios, defeitos, incorreções ou desconformidades, nos termos dos arts. 117 e 140 da Lei nº 14.133/2021.
- 4.12.51. No caso em que for configurado inexecução total do contrato, sem prejuízo de multa e demais sanções previstas em lei, a contratada deverá devolver o valor total pago antecipado, atualizado monetariamente pelo Índice de Custos de Tecnologia da Informação (ICTI), conforme [Portaria nº 6.432, de 11 de julho de 2018](#) do Ministério do Planejamento, Desenvolvimento e Gestão.
- 4.12.52. Para os serviços do **Grupo 1**:
- 4.12.52.1. Criar documentação técnica, operacional e de análise e controle, execução de rotinas proativas e reativas, análise de desempenho, monitoramento e operação dos serviços.
 - 4.12.52.2. 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 CNJ para esse fim.
 - 4.12.52.3. Formalizar ao CONTRATANTE a substituição de profissional, antes de sua efetiva substituição.
 - 4.12.52.4. As atividades que não possuam rotinas e procedimentos definidos deverão ser documentados após a sua realização como condição para a aceitação do serviço.



Poder Judiciário

Conselho Nacional de Justiça

- 4.12.52.5. 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.
- 4.12.52.6. 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.
- 4.12.52.7. 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.
- 4.12.52.8. A CONTRATADA deverá auxiliar o CONTRATANTE na comunicação junto aos fabricantes dos produtos utilizados pelo CONTRATANTE.

4.13. Da Estimativa de Preços

- 4.13.1. O valor total estimado para a contratação é de **R\$ 17.117.372,20** (dezessete milhões, cento e dezessete mil, trezentos e setenta e dois reais e vinte centavos).
- 4.13.2. Esse é o valor estimado pelo setor de compras deste Conselho após análise de propostas comerciais de potenciais fornecedores.
- 4.13.3. A estimativa de preços da contratação, bem como as fontes que fundamentaram a pesquisa se encontram registrados extensamente nos Estudos Preliminares.
- 4.13.4. Comenta-se também sobre as contratações públicas que deram origem à estimativa de preços na seção Análise de Mercado de TIC deste Termo de Referência.
- 4.13.5. Dessa forma, de posse dos dados da seção de Análise de mercado de TIC deste TR, registram-se os valores máximos admitidos por item, e para toda a contratação na tabela:

Estimativa de preço da contratação

Grupo	Item	Descrição	Catser	Unid.	Qtd.	Valor Unitário da contratação	Valor da contratação
1	1	Serviço de administração, operação e manutenção e atendimento a requisições	27014	Mês	60	R\$ 110.921,23	R\$ 6.655.273,80



Poder Judiciário

Conselho Nacional de Justiça

	2	Serviço de gestão de vulnerabilidades	27014	Mês	60	R\$ 64.665,54	R\$ 3.879.932,40
	3	Serviço de gestão de incidentes de segurança (CSIRT - <i>Blue Team</i>)	27014	Mês	60	R\$ 32.514,83	R\$ 1.950.889,80
	4	Serviço de monitoramento e visibilidade de ataques cibernéticos	27014	Mês	60	R\$ 47.713,06	R\$ 2.862.783,60
	5	Serviço de Conscientização em Segurança da Informação	27014	Mês	60	R\$ 18.962,57	R\$ 1.137.754,20
Não agrupado	6	Serviço de testes de invasão (<i>Red Team</i>)	27014	Sistemas	80*	R\$ 7.884,23	R\$ 630.738,40
Valor total estimado:							R\$ 17.117.372,20

Tabela 4 – Objeto detalhado (*sob demanda)

4.14. Da Adequação orçamentária

4.14.1. A despesa decorrente desta licitação correrá à conta de recursos do Orçamento Geral da União, Programa de Trabalho 02.032.0033.21BH.5664 - "Controle da atuação administrativa e financeira do Poder Judiciário, do cumprimento dos deveres funcionais dos juízes e Gestão de Políticas Judiciárias". Natureza da Despesa: 3.3.90.40.11.

4.15. Da Vigência Contratual

4.15.1. Para o fiel cumprimento das obrigações, será celebrado contrato de prestação de serviços com vigência de 60 (sessenta) meses a contar da data do início da prestação dos serviços, podendo ser prorrogado até o limite de 120 (cento e vinte) meses, nos termos da Lei.

4.15.2. A prorrogação de que trata este item é condicionada ao ateste, pela autoridade competente, de que as condições e os preços permanecem vantajosos para a Administração, permitida a negociação com o Contratado.

4.15.3. Para formalização da contratação, será verificada a regularidade fiscal da Fornecedorora por meio de consulta ao Cadastro Informativo dos Créditos não Quitados do Setor Público Federal (CADIN), Cadastro Nacional de Empresas Inidôneas e Suspensas (CEIS) e ao Cadastro Nacional de Empresas Punidas (CNEP), sem prejuízo da consulta de outros meios previstos na legislação.



Poder Judiciário

Conselho Nacional de Justiça

- 4.15.4. A fixação da vigência contratual em 60 (sessenta) meses justifica-se pela natureza continuada, estratégica e altamente sensível dos serviços gerenciados de segurança, os quais sustentam o monitoramento e a proteção de um ambiente tecnológico heterogêneo composto por múltiplas soluções de hardware e software, essenciais à integridade e confiabilidade do parque computacional do CNJ.
- 4.15.5. A contratação mostra-se indispensável para mitigar riscos relevantes de ataques cibernéticos, falhas operacionais e incidentes que podem comprometer sistemas críticos e estratégicos, como o PJe, o SEI e o BNMP, bem como outras soluções fundamentais ao cumprimento da missão institucional do CNJ. A interrupção ou descontinuidade desses serviços, especialmente diante do encerramento do Contrato nº 08/2021, pode ocasionar prejuízos significativos às atividades finalísticas e administrativas.
- 4.15.6. O prazo de 60 meses atende ao interesse público por proporcionar melhor relação custo-benefício, permitindo maior diluição dos custos diretos e indiretos de implantação, transição, capacitação e absorção do conhecimento técnico necessário à execução do objeto. Ademais, reduz-se o risco de interrupção prematura antes da completa estabilização do modelo de operação e da plena integração da contratada aos processos internos e às ferramentas de segurança do CNJ.
- 4.15.7. Além disso, a maior duração contratual contribui para mitigar a alta rotatividade de equipes técnicas, favorecendo a manutenção de profissionais qualificados e garantindo continuidade operacional, fator essencial em serviços de segurança da informação, cuja efetividade depende de histórico, maturidade de processos e conhecimento acumulado do ambiente monitorado.
- 4.15.8. Por fim, diante da complexidade do objeto, a vigência de 60 meses proporciona ganhos concretos de economia, eficiência e eficácia, ao viabilizar a consolidação de um novo modelo de gestão de segurança, com segregação adequada de funções, maior controle de acessos e redução de riscos operacionais, assegurando a continuidade e a melhoria progressiva dos níveis de proteção dos ativos críticos do CNJ, em conformidade com a legislação aplicável.

4.16. Reajuste

- 4.16.1. Após o interregno de um ano da data do orçamento estimado, e independentemente de pedido da CONTRATADA, os preços iniciais serão reajustados, mediante a aplicação, pelo CONTRATANTE, do



Poder Judiciário

Conselho Nacional de Justiça

Índice de Custo da Tecnologia da Informação – ICTI, exclusivamente para as obrigações iniciadas e concluídas após a ocorrência da anualidade.

- 4.16.2. Nos reajustes subsequentes ao primeiro, o interregno mínimo de um ano será contado a partir dos efeitos financeiros do último reajuste.
- 4.16.3. No caso de atraso ou não divulgação do índice de reajustamento, o CONTRATANTE pagará à CONTRATADA a importância calculada pela última variação conhecida, liquidando a diferença correspondente tão logo seja divulgado o índice definitivo.

4.17. Garantia Contratual

- 4.17.1. Será exigida a garantia da contratação de que tratam os [arts. 96 e seguintes da Lei nº 14.133, de 2021](#), no percentual de 5% (cinco por cento) do **valor anual**, conforme regras previstas na legislação.

4.18. Sanções Administrativas

- 4.18.1. Com fundamento no capítulo I do título IV da Lei Federal nº 14.113/2021, a Contratada ficará sujeita às sanções previstas em contrato no caso de descumprimento das obrigações pactuadas, sem prejuízo das responsabilidades civil e criminal, e assegurada a prévia e ampla defesa.
- 4.18.2. As sanções administrativas a seguir poderão ser aplicadas cumulativamente.
- 4.18.3. O licitante ou o contratado será responsabilizado administrativamente pelas seguintes infrações:
- i. dar causa à inexecução parcial do contrato;
 - ii. dar causa à inexecução parcial do contrato que cause grave dano à Administração, ao funcionamento dos serviços públicos ou ao interesse coletivo;
 - iii. dar causa à inexecução total do contrato;
 - iv. deixar de entregar a documentação exigida para o certame;
 - v. não manter a proposta, salvo em decorrência de fato superveniente devidamente justificado;
 - vi. não celebrar o contrato ou não entregar a documentação exigida para a contratação, quando convocado dentro do prazo de validade de sua proposta;



Poder Judiciário

Conselho Nacional de Justiça

- vii. ensejar o retardamento da execução ou da entrega do objeto da licitação sem motivo justificado;
- viii. apresentar declaração ou documentação falsa exigida para o certame ou prestar declaração falsa durante a licitação ou a execução do contrato;
- ix. fraudar a licitação ou praticar ato fraudulento na execução do contrato;
- x. comportar-se de modo inidôneo ou cometer fraude de qualquer natureza;
- xi. praticar atos ilícitos com vistas a frustrar os objetivos da licitação;
- xii. praticar ato lesivo previsto no art. 5º da Lei Federal nº 12.846, 2013.

4.18.4. Serão aplicadas ao responsável pelas infrações administrativas previstas na Lei Federal nº 14.133/2021 as seguintes sanções:

- a) advertência;
- b) multa;
- c) impedimento de licitar e contratar;
- d) declaração de inidoneidade para licitar ou contratar.

4.18.5. Na aplicação das sanções serão considerados:

- 1. a natureza e a gravidade da infração cometida;
- 2. as peculiaridades do caso concreto;
- 3. as circunstâncias agravantes ou atenuantes;
- 4. os danos que dela provierem para a Administração Pública;
- 5. a implantação ou o aperfeiçoamento de programa de integridade, conforme normas e orientações dos órgãos de controle.

4.18.6. A sanção prevista na alínea “a” do item 4.18.4 será aplicada exclusivamente pela infração administrativa prevista no inciso I do item 4.18.3, quando não se justificar a imposição de penalidade mais grave.

4.18.7. A sanção prevista na alínea “b” do item 4.18.4, calculada na forma do edital ou do contrato, não poderá ser inferior a 0,5% (cinco décimos por cento) nem superior a 30% (trinta por cento) do valor do contrato licitado ou celebrado com contratação direta e será aplicada ao responsável por qualquer das infrações administrativas previstas no 4.18.3.



Poder Judiciário

Conselho Nacional de Justiça

4.18.7.1. Será aplicada multa moratória sobre o valor da parcela inadimplida ou do valor total do contrato, conforme detalhamento constante da tabela a seguir:

Obrigações/Conduta	Prazo contratual	Multa Moratória	Base de cálculo
Reunião de alinhamento – Início do período de transição	Até o 5º (quinto) dia útil após a assinatura do contrato.	0,1% por dia atraso, limitada ao valor de 0,5%.	Valor total contratado do Grupo 01
Apresentação de Plano de Operacionalização dos Serviços (exceto o serviço do item 6 – Não agrupado)	Até 10 (dez) dias úteis após a reunião de alinhamento	0,1% por dia atraso, limitada ao valor de 1%.	Valor total contratado do Grupo 01
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 (exceto o serviço do item 6 – Não agrupado)	Até 15 (quinze) dias úteis após a reunião de alinhamento	0,5% por dia atraso, limitada ao valor de 10%.	Valor mensal contratado do serviço
Entrega dos relatórios gerenciais de serviços (RGS)	Até o 3º (terceiro) dia útil do mês posterior à prestação do serviço	0,5% por dia atraso, limitada ao valor de 10%.	Valor mensal contratado do serviço
Envio da Nota Fiscal	Até 03 (três) dias úteis após a notificação de avaliação do RGS	0,5% por dia atraso, limitada ao valor de 5%.	Valor mensal contratado do serviço

4.18.7.2. Será aplicada multa compensatória sobre o valor mensal do contrato e, para o item 6 não agrupado, sobre o valor da Ordem de Serviço, conforme detalhamento constante da tabela a seguir:

- de **2% (dois por cento)** por ocorrência em que o profissional **descumprir a norma sobre o controle de acesso**, a circulação e a permanência de pessoas no Conselho Nacional de Justiça;
- de **5% (cinco por cento)** por ocorrência em que a contratada deixar de afastar profissional que se conduza de modo inconveniente ou que não respeite as normas do CNJ ou que não atenda às necessidades, num período de 24 (vinte e quatro) horas corridas a contar da notificação do CONTRATANTE.



Poder Judiciário

Conselho Nacional de Justiça

c) de **5% (cinco por cento)** por ocorrência em que a contratada descumprir Política, Norma ou Procedimento de Segurança da Informação do CONTRATANTE.

d) de **10% (dez por cento)** por ocorrência em que a contratada 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.

e) de **10% (dez por cento)** por ocorrência em que a contratada por motivo de negligência, imprudência ou imperícia na execução das atividades contratuais, causar qualquer dano físico ou lógico aos equipamentos da CONTRATANTE.

f) de **10% (dez por cento)** pelo não atingimento de um mesmo nível de serviço previsto no ANEXO C, durante 3 (três) meses consecutivos ou 5 (cinco) meses alternados, apurados em um período de 12 (doze meses).

g) de **15% (quinze por cento)** pelo não atingimento de um mesmo nível de serviço previsto no ANEXO C, durante 6 (seis) meses consecutivos ou 10 (dez) meses não consecutivos, apurados em um período de 12 (doze meses).

4.18.8. A sanção prevista na alínea “c” do item 4.18.4 será aplicada ao responsável pelas infrações administrativas previstas nos incisos II, III, IV, V, VI e VII do item 4.18.3, quando não se justificar a imposição de penalidade mais grave, e impedirá o responsável de licitar ou contratar no âmbito da Administração Pública direta e indireta do ente federativo que tiver aplicado a sanção, pelo prazo máximo de 3 (três) anos.

4.18.9. A sanção prevista na alínea “d” do item 4.18.4 será aplicada ao responsável pelas infrações administrativas previstas nos incisos VIII, IX, X, XI e XII do item 4.18.3, bem como pelas infrações administrativas previstas nos incisos II, III, IV, V, VI e VII que justifiquem a imposição de penalidade mais grave que a sanção referida no item 4.18.7, e impedirá o responsável de licitar ou contratar no âmbito da Administração Pública direta e indireta de todos os entes federativos, pelo prazo mínimo de 3 (três) anos e máximo de 6 (seis) anos.



Poder Judiciário

Conselho Nacional de Justiça

- 4.18.10. A sanção estabelecida na alínea “d” do item 4.18.4 será precedida de análise jurídica, desde que observada, quando aplicada por órgãos dos Poderes Legislativo e Judiciário, pelo Ministério Público e pela Defensoria Pública no desempenho da função administrativa, será de competência exclusiva de autoridade de nível hierárquico equivalente autoridade máxima da entidade.
- 4.18.11. As sanções previstas nas alíneas “a”, “c” e “d” do item 4.18.4 poderão ser aplicadas cumulativamente com a prevista na alínea “b” do mesmo item.
- 4.18.12. Se a multa aplicada e as indenizações cabíveis forem superiores ao valor de pagamento eventualmente devido pelo CNJ ao contratado, além da perda desse valor, a diferença será descontada da garantia prestada ou será cobrada judicialmente.
- 4.18.13. A aplicação das sanções previstas neste tópico não exclui, em hipótese alguma, a obrigação de reparação integral do dano causado à Administração Pública.
- 4.18.14. Na aplicação da sanção prevista na alínea “b” do item 4.18.4, será facultada a defesa do interessado no prazo de 15 (quinze) dias úteis, contado da data de sua intimação.
- 4.18.15. A aplicação das sanções previstas nas alíneas “c” e “d” do item 4.18.4 requererá a instauração de processo de responsabilização, a ser conduzido por comissão composta de 2 (dois) ou mais servidores estáveis, que avaliará fatos e circunstâncias conhecidos e intimará o licitante ou o contratado para, no prazo de 15 (quinze) dias úteis, contado da data de intimação, apresentar defesa escrita e especificar as provas que pretenda produzir.
- 4.18.16. O atraso injustificado na execução do contrato sujeitará o contratado a multa de mora, na forma prevista em edital ou em contrato.
- 4.18.17. A aplicação de multa de mora não impedirá que o CNJ converta em compensatória e promova a extinção unilateral do contrato com a aplicação cumulada de outras sanções previstas na Lei Federal nº 14.133/2021.

5. REQUISITOS TÉCNICOS

- 5.1.1.A CONTRATADA poderá sugerir alterações nas metodologias, técnicas e ferramentas. As sugestões serão analisadas e poderão ser homologadas pelo CNJ e incorporadas ao acervo técnico, sem ônus adicional.



Poder Judiciário

Conselho Nacional de Justiça

- 5.1.2. As habilidades envolvidas refletem o entendimento acerca do funcionamento dos negócios internos da área de TI e respectivas áreas finalísticas do DTI envolvendo também a execução de procedimentos de acordo com as regras de segurança vigentes. Todas as competências de qualificação dos colaboradores envolvidos – como certificações profissionais, formação e experiência – estão diretamente ligados à qualidade que os serviços de TI do DTI exigem e devem ser prestados.
- 5.1.3. Ainda, a exigência de habilidades em plataformas tecnológicas específicas leva em consideração a especificidade do ambiente computacional do CNJ, dentro de toda sua complexidade, a criticidade de equipamentos e serviços, a essencialidade de seus serviços públicos, dentre outros fatores.
- 5.1.4. Além de seu aspecto quantitativo, os serviços de TI devem ser prestados com qualidade, controle e melhorias constantes, por meio da implantação e aplicação continuada das melhores práticas de Gerenciamento de Serviços de TI, com base nos processos e padrões aceitos internacionalmente.
- 5.1.5. As especificações dos requisitos técnicos para a prestação dos serviços estão pormenorizadas no ANEXO A – ESPECIFICAÇÃO DOS REQUISITOS TÉCNICOS deste Termo de Referência.

6. DOCUMENTOS ANEXOS

6.1. Integram o presente Termo de Referência, os anexos:

- 6.1.1. ANEXO A – ESPECIFICAÇÃO DOS REQUISITOS TÉCNICOS;
- 6.1.2. ANEXO B – PLATAFORMA DE SEGURANÇA;
- 6.1.3. ANEXO C – NÍVEIS MÍNIMOS DE SERVIÇO;
- 6.1.4. ANEXO D - MODELO DE ORDEM DE SERVIÇO ;
- 6.1.5. ANEXO E - MODELO DE TERMO DE RECEBIMENTO DEFINITIVO DO SERVIÇO;
- 6.1.6. ANEXO F – DECLARAÇÃO DE VISTORIA;
- 6.1.7. ANEXO G – TERMO DE CIÊNCIA INDIVIDUAL;
- 6.1.8. ANEXO H - MODELO DE TERMO DE COMPROMISSO DE MANUTENÇÃO DE SIGILO;
- 6.1.9. ANEXO I – DECLARAÇÃO DE NÃO-NEPOTISMO;
- 6.1.10. ANEXO J – PLANILHA DE ATENDIMENTO AOS REQUISITOS



Poder Judiciário

Conselho Nacional de Justiça

TÉCNICOS;

6.1.11. ANEXO K - TERMO DE RESPONSABILIDADE E COMPROMISSO COM O CÓDIGO DE CONDUTA PARA FORNECEDORES DE BENS E SERVIÇOS DO CONSELHO NACIONAL DE JUSTIÇA.

6.1.12. ANEXO L – CATÁLOGO DE SERVIÇO.



Poder Judiciário

Conselho Nacional de Justiça

ANEXO A – ESPECIFICAÇÃO DOS REQUISITOS TÉCNICOS

1. DOS SERVIÇOS GERENCIADOS DE SEGURANÇA

1.1. Condições Gerais do GRUPO 1

1.1.1.O Serviço de Administração, Operação e manutenção e Atendimento de Requisições (Item 1 Grupo 01) deverá ser prestado no período (24x7):

1.1.1.1. Das 08:00 às 20:00h, de segunda à sexta-feira, de forma predominantemente remota, com atuação presencial eventual, quando necessária e previamente autorizada, não caracterizando, em qualquer hipótese, alocação ou cessão de mão de obra nas dependências da CONTRATANTE;

1.1.1.2. Remotamente, por meio do Centro de Operações de Segurança (SOC), com atendimento de requisições e execução de atividades previstas, observados os níveis de serviços estabelecidos:

1.1.1.2.1. Das 08:00 às 20:00hs, aos sábados, domingos e feriados.

1.1.1.2.2. Das 20:00 às 08:00h, em todos os dias da semana, inclusive sábados, domingos e feriados.

1.1.1.3. Quando tecnicamente indispensável e mediante autorização formal da CONTRATANTE, a CONTRATADA deverá realizar atendimento presencial também fora do horário comercial, inclusive em finais de semana e feriados, observado o modelo de acionamento e os níveis de serviço definidos.

1.1.2.O Serviço de gestão de vulnerabilidades (Item 2 Grupo 01) deverá ser prestado em período integral (24x7) para o monitoramento contínuo das vulnerabilidades presentes no ambiente de TI do CNJ; e presencialmente, nas dependências do CONTRATANTE, em caso de ocorrência de grave incidente de segurança que implique em comprometimento de disponibilidade, integridade ou confidencialidade das informações do CNJ.

1.1.3.O Serviço de Gestão de Incidentes de Segurança (Item 3 Grupo 01) deverá ser prestado em período integral (24x7) para o tratamento de incidentes de segurança da informação e presencialmente, nas dependências do CONTRATANTE, em caso de ocorrência de grave incidente de segurança que implique em comprometimento de disponibilidade, integridade ou confidencialidade das informações do CNJ.



Poder Judiciário

Conselho Nacional de Justiça

- 1.1.4.O Serviço de monitoramento e visibilidade de ataques cibernéticos (Item 4 Grupo 01) deverá ser prestado em período integral (24x7) para a identificação e notificação concisa de incidentes iminentes; e presencialmente, nas dependências do CONTRATANTE, em caso de ocorrência de grave incidente de segurança previamente identificado que implique em comprometimento de disponibilidade, integridade ou confidencialidade das informações do CNJ.
- 1.1.5.O Serviço de Conscientização em Segurança da Informação (item 5 Grupo 01) deverá ser prestado na modalidade presencial ou de modo remoto das 09:00 às 19:00h, de segunda à sexta-feira.
- 1.1.6.Todos equipamentos e softwares ofertados pela CONTRATADA, quando for o caso e necessário à consecução das atividades de segurança, devem atender às 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).
- 1.1.7.Todos os equipamentos, quando for o caso e necessário à prestação dos serviços, devem ser novos e de primeiro uso. Além disso, os equipamentos e softwares não podem constar, no momento da apresentação da proposta técnica, em listas de end-of-sale, end-of-support, end-of-life ou similares do fabricante, ou seja, não podem ter previsão de descontinuidade de fornecimento, suporte ou vida.
- 1.1.8.Os softwares ofertados pela CONTRATADA devem ser instalados em sua versão mais estável e atualizada e estar cobertos por contratos de suporte e atualização de versão do fabricante durante a vigência do respectivo item de serviço. Da mesma maneira, os equipamentos fornecidos para a prestação dos serviços devem estar cobertos por contratos de garantia do fabricante.
- 1.1.9.O conjunto de requisitos especificados para cada serviço pode ser atendido por meio de composição com outros equipamentos ou softwares utilizados no atendimento aos demais itens, de maneira integrada, desde que não implique alteração da topologia de rede ou na exposição de ativos a riscos de segurança da informação, em termos de integridade, confidencialidade ou disponibilidade.
- 1.1.10.Deverá ser fornecido ao CONTRATANTE acesso à console dos produtos ofertados para que seja possível o acompanhamento, auditoria e direcionamento de ações no ambiente.
- 1.1.11.Durante a execução dos serviços, a CONTRATADA deverá disponibilizar o quantitativo de profissionais necessários para atender todos os perfis para o



Poder Judiciário

Conselho Nacional de Justiça

normal desenvolvimento dos serviços que compõe os Serviços Gerenciados de Segurança (MSS).

- 1.1.12. 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.
- 1.1.13. Não será exigida a dedicação exclusiva de profissionais na gestão e execução dos serviços demandados pela CONTRATANTE.
- 1.1.14. 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 CNJ 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.
- 1.1.15. 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 CNJ, devendo emitir nota técnica avaliando os riscos deste novo IC para o ambiente tecnológico. Com base na nota técnica elaborada o CNJ 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.
- 1.1.16. A CONTRATADA deverá monitorar permanentemente 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.
- 1.1.17. 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.
- 1.1.18. As manutenções programadas, que impliquem em extensiva parada do ambiente serão realizadas durante um final de semana. Tais atividades



Poder Judiciário

Conselho Nacional de Justiça

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.

- 1.1.19. Todos os serviços de manutenção corretiva e preventiva são considerados de natureza contínua e deverão minimizar a necessidade de parada do ambiente em produção.
- 1.1.20. Testar todos os serviços após a realização de manutenções preventivas e/ou corretivas, ficando sua aceitação final dependente da área demandante e/ou de fiscalização do CONTRATANTE, que avaliará as características esperadas para o serviço.
- 1.1.21. 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.
- 1.1.22. A CONTRATADA deverá produzir mensalmente informações acerca 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.
- 1.1.23. Será de responsabilidade da CONTRATADA o monitoramento constante dos acessos e dos Itens de Configuração IC's que suportem os serviços de segurança, gerando uma base histórica de monitoramento destes Itens.
- 1.1.24. Os serviços devem ser executados de acordo com normas, procedimentos e técnicas adotadas pelo CNJ.
- 1.1.25. Os Serviços Gerenciados de Segurança que não forem presenciais deverão ser prestados por meio de estrutura de SOC's - Security Operation Center.
- 1.1.26. A CONTRATADA deverá ser capaz entregar todos os serviços definidos no catálogo de serviços (descrito no ANEXO L – CATÁLOGO DE SERVIÇO). O catálogo de serviço deverá ser mantido e administrado através do sistema de ITSM de responsabilidade da CONTRATADA, estando este disponível de forma on line para a CONTRATANTE, onde o mesmo poderá consultar a qualquer tempo os serviços disponíveis.
- 1.1.27. Os SOC's devem estar ativos e deverão atender aos seguintes requisitos mínimos:



Poder Judiciário

Conselho Nacional de Justiça

- 1.1.27.1. Utilizar sistema de gerenciamento de CFTV, que viabilizem o rastreamento de pessoas dentro do ambiente da CONTRATADA e cujas imagens possam ser recuperadas;
 - 1.1.27.2. Filmar toda a área, mantendo as imagens armazenadas por no mínimo 90 (noventa) dias;
 - 1.1.27.3. Efetuar registro de entrada e saída dos visitantes, com identificação individual, em todos os acessos ao SOC por no mínimo 90 dias;
 - 1.1.27.4. Possuir solução de monitoramento de disponibilidade e desempenho;
 - 1.1.27.5. O perímetro deve protegido contra intrusão e acesso indevido;
 - 1.1.27.6. Ser vigiado de forma ininterrupta por segurança especializada em regime de 24x7x365;
 - 1.1.27.7. Ter controle de acesso físico com pelo menos 2 (dois) fatores de autenticação;
 - 1.1.27.8. Ser configurado de forma que a falha de um dos equipamentos isoladamente NÃO interrompa a prestação dos serviços;
 - 1.1.27.9. Dispor de 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;
 - 1.1.27.10. Ter componentes de segurança necessários para garantir a preservação dos dados em casos de incêndio e execução de plano de recuperação de catástrofes;
 - 1.1.27.11. Deverá possuir processos implementados que garantam a segurança das informações do CONTRATANTE, em conformidade com a norma ABNT NBR ISO/IEC 27001.
- 1.1.28. A CONTRATADA deverá fornecer o link de comunicação dedicado principal, cuja utilização não deverá ultrapassar 90% (noventa por cento) de sua capacidade. Para fins de redundância, poderá ser utilizado o link de comunicação do CONTRATANTE, mediante estabelecimento de VPN via internet, garantindo a continuidade da conectividade em caso de indisponibilidade do link principal.
- 1.1.29. A CONTRATADA será responsável pela aplicação de controles de segurança adequados (criptografia) para garantir a confidencialidade de qualquer dado ou



Poder Judiciário

Conselho Nacional de Justiça

informação do CONTRATANTE que receber em seu ambiente ou em terceiro contratado.

1.1.30.A CONTRATADA deverá comunicar formalmente o CONTRATANTE sempre que identificar algum serviço com falhas de implementação e que tornem o ambiente vulnerável a indisponibilidade.

1.1.31.A CONTRATADA deverá disponibilizar mecanismos de consolidação, visualização e correlação de dados de segurança, podendo utilizar ferramentas próprias, do CONTRATANTE ou de terceiros, desde que garanta visão unificada e integrada dos serviços.

2. GRUPO 1 – Item 01: SERVIÇO DE ADMINISTRAÇÃO, OPERAÇÃO E MANUTENÇÃO E ATENDIMENTO DE REQUISIÇÕES

2.1. Condições Gerais

2.1.1.Tem por objetivo sustentar e operar as soluções e produtos de segurança do CNJ, através de um catálogo de serviços pré-estabelecido pelo CNJ, anexo do presente termo, porém, não se limitando apenas a este.

2.1.2.A CONTRATADA também deverá realizar permanente ações proativas voltadas para a segurança do parque computacional do CNJ, descritas no ANEXO B – PLATAFORMA DE SEGURANÇA e outras soluções que vierem a integrar o ambiente de segurança da CONTRATANTE, a fim de e mantê-lo estável, disponível e integro.

2.1.3.Para fins de dimensionamento da equipe, a tabela abaixo apresenta o histórico da volumetria de chamados relacionados à segurança atendidos no período compreendido entre janeiro de 2023 a dezembro de 2025:

	2023	2024	2025
JAN	49	83	50
FEV	61	76	64
MAR	57	142	140
ABR	40	148	66
MAI	50	111	78



Poder Judiciário

Conselho Nacional de Justiça

JUN	34	75	175
JUL	94	98	275
AGO	105	85	432
SET	101	77	383
OUT	135	58	356
NOV	120	53	116
DEZ	55	62	177
Média	75	89	193
Total	901	1068	2312

2.1.4.A CONTRATADA deverá realizar, nos primeiros 60 (sessenta) dias de execução deste serviço, 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.

2.1.5.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, ou o *NIST Cybersecurity Framework*.

2.1.6.A análise deverá incluir todas as camadas de segurança dos produtos instalados nas dependências e na nuvem do CNJ (ex. Teams, Exchange Online, OneDrive, Office 365, SharePoint, CASB, etc.). Para a nuvem, a análise deverá contemplar, no mínimo, os itens listados no *assessment* padrão da Microsoft e AWS.

2.1.7.A análise deverá ser conduzida por profissional com certificação CISSP (*Certified Information Systems Security*), CISM (*Certified Information Security Manager*), CIA (*Certified Intrusion Analyst*), GSEC (*GIAC Security Essentials*), GCIH (*GIAC Certified IncidentHandler*) ou GMON (*GIAC Continuous Monitoring*), que será responsável pela apresentação dos resultados da análise ao gestor, fiscais do contrato e gestores de TI do CNJ.



Poder Judiciário

Conselho Nacional de Justiça

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

- 2.1.8.1. Acompanhar a execução dos serviços para o cumprimento dos níveis de serviço estabelecidos;
- 2.1.8.2. Priorizar os atendimentos críticos, conforme definição do CONTRATANTE;
- 2.1.8.3. Monitorar permanentemente e avaliar criticamente os produtos e serviços de segurança do CONTRATANTE;
- 2.1.8.4. Atuar proativamente na antecipação e identificação de incidentes de segurança, antes mesmo do impacto nos serviços;
- 2.1.8.5. 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;
- 2.1.8.6. 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;
- 2.1.8.7. Prover os fiscais do contrato com os relatórios técnicos e gerenciais suficientes para a comprovação dos serviços realizados;
- 2.1.8.8. Supervisionar sua equipe na execução dos serviços de SI;
- 2.1.8.9. Elaborar e propor plano de execução dos serviços;
- 2.1.8.10. Organizar a alocação de turnos e de profissionais de sua equipe;
- 2.1.8.11. Definir plano de treinamento inicial e contínuo dos profissionais que executam os serviços;
- 2.1.8.12. Executar outros serviços correlatos à supervisão dos profissionais na execução dos Serviços Gerenciados de Segurança;
- 2.1.8.13. Orientar a atuação da equipe técnica em situações críticas de trabalho, bem como interagir com os usuários quando a situação requerer;
- 2.1.8.14. Fornecer sugestões e auxiliar na construção e manutenção contínua, com o apoio e aprovação do CNJ, de procedimentos sistematizados e da base de conhecimento, contemplando todas as soluções de problemas resolvidos com respostas padronizadas;
- 2.1.8.15. Receber as demandas dos serviços relativas à área de segurança da informação e providenciar a execução e alocação de recursos de trabalho;



Poder Judiciário

Conselho Nacional de Justiça

- 2.1.8.16. Consolidar os relatórios de atividades mensais (mês calendário), referente aos Serviços Gerenciados de Segurança, provendo informações gerenciais ao CONTRATANTE;
- 2.1.8.17. Supervisionar sua equipe de profissionais na execução das ações conjuntas com a área de infraestrutura, cumprindo a política de segurança da informação do CNJ e aplicando as melhores práticas de segurança;
- 2.1.8.18. Consolidar em manuais de procedimentos e em base de conhecimento todas as soluções adotadas na execução das atividades;
- 2.1.8.19. Elaborar mensalmente relatórios de desempenho, auditoria e operação dos ativos sob sua administração;
- 2.1.8.20. Implantar as melhorias solicitadas pelos servidores do CONTRATANTE através das aberturas de chamados no sistema de gestão de serviços de TI;
- 2.1.8.21. Sugerir novas tecnologias para modernizar o ambiente tecnológico, buscando subsidiar a equipe do CONTRATANTE na gestão de segurança da informação;
- 2.1.8.22. 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;
- 2.1.8.23. Consolidar as sugestões de melhoria;
- 2.1.8.24. Executar as tarefas de implantação, substituição e atualização de soluções destinadas à área de segurança da informação, prevendo prazos, custos, recursos, qualidade conforme as práticas de Gerenciamento de Projetos – PMI;
- 2.1.8.25. Administrar solução de Gerenciamento Unificado de Ameaças – UTM;
- 2.1.8.26. Administrar solução de Firewall de Aplicação Web - WAF;
- 2.1.8.27. Administrar solução de Proteção de Aplicações Nativas em Nuvem (CNAPP);
- 2.1.8.28. Administrar solução contra-ataque de Negação de Serviço Distribuído (DDoS);



Poder Judiciário

Conselho Nacional de Justiça

- 2.1.8.29. Administrar solução de proteção de gateway de e-mail, contemplando proteção antimalware e AntiSpam, filtragem de conteúdo e prevenção contra perda de dados;
- 2.1.8.30. Administrar solução de antivírus para servidores de rede, storage, ambiente virtualizado e estações de trabalho;
- 2.1.8.31. Administrar solução de Endpoint Detection and Response (EDR);
- 2.1.8.32. Administrar solução de gerenciamento unificado de ponto de extremidade (UEM);
- 2.1.8.33. Administrar solução de proteção contra ameaças avançadas – APT para endpoint, rede e e-mail.
- 2.1.8.34. Criar e configurar regras de firewall, IDS, IPS, filtro de conteúdo, controle de aplicações, antivírus, proxy, AntiSpam, CASB e DLP;
- 2.1.8.35. Criar e configurar os túneis de VPN para intercomunicação com outros órgãos e parceiros via rede Wan e Internet e acessos remotos de usuários
- 2.1.8.36. 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;
- 2.1.8.37. Executar a atualização de versão de todos os softwares e hardwares do parque tecnológico que sustenta a segurança da informação;
- 2.1.8.38. 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;
- 2.1.8.39. Apoiar tecnicamente na elaboração de relatório detalhado das funcionalidades necessárias de equipamentos e softwares a serem adquiridos, conforme demandado pelo CONTRATANTE;
- 2.1.8.40. Subsidiar tecnicamente, quando demandado, os processos de aquisição;
- 2.1.8.41. Participar da implantação de projetos/soluções, substituição e atualização de soluções destinadas à Segurança da Infraestrutura de rede;



Poder Judiciário

Conselho Nacional de Justiça

- 2.1.8.42. Auxiliar na homologação das soluções destinadas à Segurança da Informação;
- 2.1.8.43. Subsidiar tecnicamente os servidores do CONTRATANTE quanto ao dimensionamento da capacidade de hardware e configuração dos ativos de segurança;
- 2.1.8.44. Abrir chamados técnicos para os serviços de suporte técnico remoto das soluções de hardware e software de TI do CONTRATANTE;
- 2.1.8.45. 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;
- 2.1.8.46. Receber as diretrizes relacionadas à área de Segurança da Informação e providenciar a execução e alocação de recursos de trabalho;
- 2.1.8.47. Apoiar e participar na implementação dos processos bem como na mensuração dos indicadores de objetivos instituídos pelo CONTRATANTE;
- 2.1.8.48. Realizar as atividades em estrita observância na Política de Segurança da Informação (PSI) e demais normas estipuladas pelo CONTRATANTE;
- 2.1.8.49. Consolidar em manuais e scripts todos os serviços e soluções adotadas sejam eles novos ou já implantados no CONTRATANTE;
- 2.1.8.50. Auxiliar na elaboração dos procedimentos e metodologias, e verificar e reportar o cumprimento dos mesmos pelas demais áreas de TI;
- 2.1.8.51. Apoiar o CONTRATANTE na análise e definição das regras de uso dos recursos computacionais do CONTRATANTE;
- 2.1.8.52. Implantar as melhorias solicitadas pelos servidores do CONTRATANTE através das ordens de serviço;
- 2.1.8.53. Monitorar e propor soluções aos projetos/atividades em andamento otimizando-os quanto aos requisitos de Segurança da Informação;
- 2.1.8.54. Participar, quando solicitado, de reunião com os gerentes e participantes dos projetos de desenvolvimento e manutenção de



Poder Judiciário

Conselho Nacional de Justiça

sistemas e administração de dados, a fim de prover soluções para projetos/atividades em andamento;

- 2.1.8.55. Auxiliar o CONTRATANTE nos projetos de Segurança da Informação;
- 2.1.8.56. Propor procedimentos de Segurança da Informação;
- 2.1.8.57. Implantar serviço de disseminação de alertas relacionados à Segurança da Informação;
- 2.1.8.58. Executar periodicamente testes de alta disponibilidade na infraestrutura do CONTRATANTE com o objetivo de validar o seu funcionamento;
- 2.1.8.59. Elaborar um plano de teste do ambiente de infraestrutura de segurança do CONTRATANTE, que deverá ser mantido atualizado continuamente;
- 2.1.8.60. Este plano servirá de referência para elaboração de um Plano de Continuidade dos Serviços de Segurança da Informação;
- 2.1.8.61. Executar atividades relativas aos normativos e governança do CONTRATANTE naquilo que forem relativas à sua área de atuação.

2.1.9. Os produtos listados abaixo devem ser criados e atualizados em conformidade com os padrões e necessidade do CNJ e homologados formalmente junto ao DTI:

- 2.1.9.1. Guia de procedimentos de sustentação do serviço de proteção de e-mail;
- 2.1.9.2. Guia de procedimentos de sustentação do serviço de antivírus;
- 2.1.9.3. Guia de procedimentos de sustentação do serviço de proteção unificada;
- 2.1.9.4. Guia de procedimentos de sustentação do serviço de gestão unificado de ameaças;
- 2.1.9.5. Guia de procedimentos de sustentação do serviço de firewall de aplicação;
- 2.1.9.6. Guia de procedimentos de sustentação do serviço de gerenciamento de vulnerabilidades;
- 2.1.9.7. 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 Nacional de Justiça

- 2.1.9.8. Documento contendo os requisitos de segurança da informação para a homologação e liberação de serviços, aplicações e servidores de rede;
- 2.1.9.9. Catálogo de Serviços e Base de Itens de Configuração;
- 2.1.9.10. Base de Conhecimento acerca de todos os atendimentos realizados.
- 2.1.10.A CONTRATADA deverá apoiar o CONTRATANTE em caso de mudanças requeridas por conta de atualizações ou remanejamentos de infraestrutura;
- 2.1.11.A CONTRATADA deverá realizar a configuração das ferramentas que compõem as soluções, a fim de garantir o uso eficiente delas;
- 2.1.12. Sempre que houver atendimento, a CONTRATADA deverá enviar relatório de atividades por e-mail para o CONTRATANTE;
- 2.1.13.A CONTRATADA deverá acionar o fabricante das ferramentas sempre que necessário, sem nenhum custo adicional para o CONTRATANTE.

2.2. Ferramentas

2.2.1.Segurança de Perímetro (NGFW)

- 2.2.1.1. A CONTRATADA deverá utilizar e ser capaz de administrar, operar, sustentar e apresentar melhorias da solução de segurança de perímetro NGFW (2 x Fortinet modelo Fortigate 18000F e 1 x FortiAnalyzer VM).

2.2.2.Segurança Integrada para Detecção e Resposta a Ameaças em Rede, Nuvem e Endpoints

- 2.2.2.1. A CONTRATADA deverá utilizar e ser capaz de administrar, operar, sustentar e promover melhorias contínuas da solução de segurança integrada de Detecção e Resposta a ameaças (XDR), voltada à prevenção, detecção, investigação e resposta a incidentes de segurança da informação, incluído ameaças avançadas do tipo APT (*Advanced Persistent Threat*), baseada no ecossistema Microsoft, contemplando no mínimo:

- 2.2.2.1.1. **Microsoft Defender XDR**, para detecção, correlação e resposta estendida a ameaças em endpoints, identidades, e-mails, aplicações e cargas de trabalho, com recursos de EDR, antivírus, análise comportamental e resposta automatizada a incidentes;



Poder Judiciário

Conselho Nacional de Justiça

2.2.2.1.2. Microsoft Defender for Cloud, para proteção de ambientes em nuvem e híbridos, incluindo avaliação contínua de postura de segurança, detecção de ameaças, recomendações de hardening e monitoramento de workloads;

2.2.2.1.3. Microsoft Intune, para gerenciamento unificado de dispositivos (UEM), aplicação de políticas de segurança, controle de conformidade, proteção de endpoints e integração nativa com as soluções Microsoft Defender para prevenção, detecção e resposta a incidentes.

2.2.2.2. As soluções deverão operar de forma integrada, possibilitando visibilidade unificada, correlação avançada de eventos, resposta automatizada a incidentes e aplicação consistente de políticas de segurança, alinhadas às boas práticas internacionais e às diretrizes de segurança da informação adotadas pela CONTRATANTE.

2.2.3. Firewall de Aplicação (WAF) e Proteção Contra Ataques de Negação de Serviço (Anti-DDoS)

2.2.3.1. A CONTRATADA deverá utilizar e ser capaz de administrar, operar, sustentar e promover a melhoria contínua da Plataforma Integrada de Proteção de Aplicações Web (WAF) e Mitigação de Ataques de Negação de Serviço (DDoS) direcionados a aplicações e serviços do CNJ expostos à internet, baseada no ecossistema AWS, contemplando, no mínimo:

2.2.3.1.1. Amazon CloudFront, para distribuição segura de conteúdo, redução de superfície de ataque e absorção de tráfego malicioso em escala global, com integração nativa aos mecanismos de proteção de aplicações e mitigação de ataques volumétricos.

2.2.3.1.2. AWS WAF, para inspeção e filtragem de requisições HTTP/HTTPS, aplicação de regras de segurança personalizadas e gerenciadas, proteção contra ataques do tipo OWASP Top 10 (como SQL Injection, Cross-Site Scripting – XSS) e controle de acesso baseado em padrões de tráfego.

2.2.3.1.3. AWS Shield, para proteção contra ataques distribuídos de negação de serviço (DDoS), incluindo mecanismos automáticos de detecção, mitigação em tempo real e resposta a ataques volumétricos, de protocolo e de camada de aplicação.



Poder Judiciário

Conselho Nacional de Justiça

2.2.4. Apesar de tais soluções (*item 2.2 - Ferramentas*) serem propriedade do CNJ, e não pertencer a este termo de referência sua aquisição e/ou renovação, será responsabilidade da CONTRATADA operar, administrar, manter e apresentar melhorias contínuas das ferramentas durante todo o período de vigência dessa contratação.

2.2.5. Ressalta-se que para execução e entrega do serviço, a CONTRATADA deverá complementar, se for necessário para garantir o cumprimento dos acordos de níveis de serviços estabelecidos no ANEXO C – NÍVEIS MÍNIMOS DE SERVIÇO, com ferramentas de sua propriedade sem incorrer em custos adicionais para a CONTRATANTE, as quais para serem habilitadas e/ou utilizadas, precisam de avaliação e autorização prévia da equipe técnica do CNJ.

2.2.6. Ressalta-se ainda que, sobre nenhuma hipótese, tais soluções de segurança poderão ser substituídas pela CONTRATADA, apenas poderão ser complementadas seguindo os processos de homologação e aprovação estabelecidos no item 2.2.5.

2.2.7. Dado que a CONTRATADA irá utilizar tais ferramentas para entrega do serviço em questão, é de responsabilidade da CONTRATADA realizar uma avaliação e propor melhoria para o ambiente, antes do início da operação do serviço.

2.3. Processo de atendimento para cumprimento de requisição de serviços

2.3.1. Ao receber uma solicitação de requisição de serviço via e-mail ou telefone, de servidores autorizados da CONTRATANTE, o analista da central de serviços deve registrar ou complementar as informações da requisição.

2.3.2. Para requisições de serviços abertas via web, o sistema de acompanhamento de chamados fornecido pela CONTRATADA deve automaticamente realizar o registro da requisição de serviço. Além disso, o sistema de acompanhamento de chamados da CONTRATADA deve permitir integração com as principais ferramentas ITSM do mercado.

2.3.3. Quando o requisitante realiza a requisição através de e-mail ou telefone, o analista da central de serviços deve, após registrar ou complementar a requisição, fazer a categorização e priorização da requisição de serviços.

2.3.4. A categorização deve ser realizada pelo analista da central de serviços relacionando o item de configuração com o seu grupo definido em catálogo de



Poder Judiciário

Conselho Nacional de Justiça

serviços. As demais informações levantadas devem ser documentadas na requisição de serviço.

- 2.3.5. Quando o meio de solicitação for via web, o sistema de acompanhamento de chamados deve realizar a categorização e priorização da requisição de serviço automaticamente, obedecendo as mesmas regras seguidas pelo processo de registro via e-mail ou telefone.
- 2.3.6. O sistema de acompanhamento de chamados deve identificar automaticamente se o serviço é ou não elegível em primeiro nível.
- 2.3.7. Caso o serviço seja elegível para primeiro nível, o analista da central de serviço deverá atuar, desde que exista procedimento pré-estabelecidos e aprovados pela CONTRATANTE.
- 2.3.8. É de responsabilidade da CONTRATADA manter uma base de conhecimento, com todos os procedimentos pré-estabelecidos e aprovados pela CONTRATANTE. Tal base de conhecimento deve fazer parte do sistema de acompanhamento de chamados, e a qualquer tempo deve estar acessível à CONTRATANTE para consultas e aprovações de novos procedimentos.
- 2.3.9. Também é de responsabilidade da CONTRATADA a criação, revisão e manutenção de tais procedimentos operacionais, sendo de responsabilidade da CONTRATANTE apenas participar como aprovador sempre que um procedimento for criado e/ou sofrer algum tipo de alteração.
- 2.3.10. O analista da central de serviços que atuou no cumprimento da requisição deve fazer o registro da sua atuação, descrevendo informações relevantes para o cumprimento daquele serviço em particular.
- 2.3.11. Em caso de solução, o analista da central de serviços que atuou no cumprimento da requisição deve registrar no sistema de acompanhamento de chamados que a requisição de serviço foi resolvida, devendo: Informar o(s) item(ns) de configuração envolvido(s) com a requisição; e corrigir a categorização da requisição de serviços, se necessário.
- 2.3.12. O analista da central de serviços, ao identificar que a requisição não é elegível em primeiro nível, deve encaminhá-la para o grupo solucionador indicado. Esse encaminhamento poderá ser automático, quando o grupo solucionador e a elegibilidade do serviço estiverem determinados em catálogo de serviços.



Poder Judiciário

Conselho Nacional de Justiça

- 2.3.13. Ao receber uma requisição de serviço, o grupo solucionador deve analisá-la para verificar se compete ao grupo ou se deve ser encaminhada a outro grupo solucionador e se, para atendê-la, será necessária uma mudança.
- 2.3.14. Ao identificar que uma requisição de serviços encaminhada para a fila do grupo não faz parte do seu escopo, o analista do grupo solucionador deve redirecioná-la ao grupo mais indicado para atender a requisição. Se compete ao grupo solucionador, esse atua no cumprimento da requisição.
- 2.3.15. Caso seja necessária uma mudança para executar o serviço requisitado, o fluxo segue para o processo de gestão de mudança. A governança sobre processo de gestão de mudança não pertence ao objeto deste termo, a CONTRATADA apenas participará quando convocada pelo processo gestão de mudança já estabelecido pela CONTRATANTE.
- 2.3.16. Se ao buscar atender à requisição de serviço o grupo solucionador identificar que para seu atendimento é necessário direcionar a solicitação a um fornecedor externo (de serviços ou de infraestrutura), deve acionar o fornecedor conforme as regras que serão estabelecidas pelo CONTRATANTE.
- 2.3.17. Nesse ponto, o status do chamado no sistema de acompanhamento de chamados deve ser atualizado para "encaminhado para fornecedor" e ficará aguardando seu retorno.
- 2.3.18. O registro da requisição de serviço na ferramenta do fornecedor, quando for o caso, deve ser documentado no registro da requisição no sistema de acompanhamento de chamados da CONTRATADA. Caberá ao grupo solucionador acompanhar e monitorar o fornecedor no atendimento da solicitação.
- 2.3.19. Cabe ao grupo solucionador avaliar e validar a entrega efetuada pelo fornecedor. São elementos de controle de qualidade e desempenho dessa atividade os níveis mínimos de serviço ou as regras definidas no instrumento contratual.
- 2.3.20. O grupo que atuou no cumprimento da requisição de serviço deve fazer o registro da sua atuação no sistema de acompanhamento de chamados, descrevendo as informações relevantes para o cumprimento daquele serviço em particular.
- 2.3.21. Em caso de solução o grupo que atuou no cumprimento da requisição deve registrar no sistema de acompanhamento de chamados que a requisição de serviço foi resolvida, devendo: Informar o(s) item(ns) de configuração



Poder Judiciário

Conselho Nacional de Justiça

envolvido(s) com a requisição; e corrigir a categorização da requisição de serviços, se necessário.

2.3.22. Após ser resolvida, a requisição de serviço deve ficar por 2 (dois) dias úteis com status igual a resolvida, podendo ser reaberta pelo CONTRATANTE no determinado período, caso este entenda que tal requisição não foi resolvida de fato. Ao final de 2 (dois) dias úteis, caso não haja nenhuma intervenção da CONTRATANTE, a requisição deverá ser alterada para o status fechada.

2.3.23. O processo descrito é o mínimo esperado a ser seguido e executado pela CONTRATADA, todavia como o objeto do presente termo de referência se trata de um serviço continuado, logo se espera da CONTRATADA a apresentação da melhoria contínua deste, a qual pode ser alterado desde que aprovado pela CONTRATANTE.

2.4. Grupo técnico de administração, operação e manutenção e atendimento de requisições

2.4.1.A CONTRATADA deverá manter uma equipe denominada GRUPO SOLUCIONADOR, com objetivo e foco de trabalhar no processo de administração, operação e manutenção e atendimento de requisições.

2.4.2. Este grupo deverá ser exclusivo para trabalhar no GRUPO TÉCNICO DE ADMINISTRAÇÃO, OPERAÇÃO E MANUTENÇÃO E ATENDIMENTO A REQUISIÇÕES. Não podem os profissionais pertencentes a este grupo serem compartilhados e/ou atuarem, com os demais serviços descritos no objeto do presente termo de referência.

2.4.3. Todos os profissionais que integram o GRUPO SOLUCIONADOR, devem obrigatoriamente compor o quadro de colaboradores da CONTRATADA em regime de trabalho CLT (Consolidação das Leis do Trabalho), não havendo possibilidade a terceirização ou subcontratação de tal serviço.

2.4.4. Deverá ser de responsabilidade da CONTRATADA dimensionar o número de profissionais adequado para entrega de tal serviço, sem que haja impacto no acordo de nível de serviço estabelecido no ANEXO C – NÍVEIS MÍNIMOS DE SERVIÇO.

2.4.5. Com o objetivo de garantir que os profissionais envolvidos têm conhecimento e habilidade, para resolver as requisições de serviço baseado nas tecnologias e fabricantes que compõe o parque de segurança da CONTRATANTE, a CONTRATADA obrigatoriamente deverá compor o GRUPO SOLUCIONADOR



Poder Judiciário

Conselho Nacional de Justiça

composta **por no mínimo 03 (três) perfis profissionais**, divididos da seguinte forma:

2.4.5.1.1. Profissional de Network Security: 1 (um) profissional para a operação e administração das soluções de segurança de perímetro e proteção de aplicações, incluindo Firewall, Amazon CloudFront, AWS WAF e AWS Shield.

2.4.5.1.2. Profissional de Cloud Security: 1 (um) profissional para operação das soluções de segurança e postura de ambientes em nuvem e híbridos, incluindo Microsoft Defender For Cloud, Serviços de segurança e conformidade em ambientes cloud e integração com soluções de gestão de vulnerabilidades e correção (patch management);

2.4.5.1.3. Profissional de Cyber Security: 1 (um) profissional para a operação das soluções de soluções de detecção, investigação e resposta a incidentes cibernéticos, incluindo Microsoft Defender XDR, Microsoft Intune (gestão e proteção de endpoints) e análise de alertas, correlação de eventos e respostas a incidentes.

2.4.6.O profissional deverá possuir no mínimo 02 (duas) certificações indicadas no respectivo perfil, ou equivalentes, podendo um mesmo profissional atuar em mais de um perfil, desde que comprovada a qualificação técnica exigida abaixo:

Perfis	Certificações
Network Security	<ul style="list-style-type: none">• Fortinet NSE 4 ou superior (ou certificações equivalentes em NGFW);• AWS Certified Security – Specialty ou equivalente;• AWS Certified Advanced Networking – Specialty ou equivalente;• Certificação em administração de solução DDoS;• Certificação em Web Application Firewall;• CCNA Security+ ou equivalente;• CompTIA Security+ ou equivalente.
Cloud Security	<ul style="list-style-type: none">• AWS Certified Security – Specialty ou equivalente;• Microsoft Certified: Azure Security Engineer Associate (AZ-500) ou equivalente;• CompTIA Cloud+ ou equivalente;• CompTIA Security+ ou equivalente.
Cyber Security	<ul style="list-style-type: none">• Microsoft Certified: Security Operations Analyst Associate (SC-200) ou equivalente;• Microsoft Certified: Endpoint Administrator Associate (MD-102) ou equivalente;



Poder Judiciário

Conselho Nacional de Justiça

	<ul style="list-style-type: none">• Microsoft Certified: Identity and Access Administrator Associate (SC-300) ou equivalente;• Microsoft Security, Compliance, and Identity Fundamentals (SC-900) ou equivalente• CompTIA Security+ ou equivalente;• CompTIA CySA+;• Certificação em administração de solução de Endpoint ou EDR.
--	---

TABELA 01 – CERTIFICAÇÕES GRUPO SOLUCIONADOR

2.4.7. Durante a execução do contrato, a CONTRATADA se obriga a manter todos os profissionais com os requisitos abaixo:

2.4.7.1. Diploma, devidamente registrado, de curso de nível superior de graduação na área de Tecnologia da Informação ou de graduação em qualquer curso superior, acrescido de certificado de curso de pós-graduação em área de Tecnologia da Informação de, no mínimo, 360 (trezentos e sessenta) horas, fornecido por instituição reconhecida pelo Ministério da Educação (MEC);

2.4.7.2. Conhecimento avançado em segurança da informação, com experiência comprovada de no mínimo 06 (meses) em operação, sustentação e suporte a ambientes similares ao supracitado.

2.4.8. Não existe restrição ou limite para acúmulo de certificações em um mesmo profissional, uma vez que é de responsabilidade da CONTRATADA definir o quantitativo de profissionais envolvidos no GRUPO SOLUCIONADOR, porém conforme já fora mencionado no presente termo de referência, este(s) deve(m) compor único e exclusivamente o time denominado GRUPO SOLUCIONADOR.

2.4.9. Será exigido da CONTRATADA a apresentação das seguintes documentações do(s) profissionais que participarão do GRUPO SOLUCIONADOR, os quais devem comprovar as exigências e obrigações descritas no presente termo de referência: carteira de trabalho devidamente assinada pela CONTRATADA, curriculum vitae para comprovação de habilidades, e as devidas certificações técnicas para comprovação do conhecimento.

2.5. Das entregas

2.5.1. Para acompanhamento e avaliação do serviço a ser ofertado pela CONTRATADA, a CONTRATANTE definiu os seguintes indicadores chave de desempenho, que reunidos vão compor um único relatório a ser entregue de



Poder Judiciário

Conselho Nacional de Justiça

forma online e em tempo de execução, através do portal de segurança da CONTRATADA, a saber:

DENOMINAÇÃO	FORMA DE CÁLCULO	FILTRO	AGRUPADOR	DESCRIÇÃO
Quantitativo de requisições abertas	Soma de requisições abertas	Requisições abertas	Requisições	Número total de requisições abertas
Quantitativo de requisições por função	Soma de requisições abertas por função	Requisições por função	Requisições por função	Número total de requisições por função
Quantitativo de requisições concluídas	Soma de requisições concluídas	Requisições concluídas	Requisições concluídas	Número total de requisições concluídas
Quantitativo de requisições em backlog	Soma de requisições em backlog	Requisições em backlog	Requisições em backlog	Número total de requisições em backlog
TOP 10 – Ativos configurados	Soma do número de configurações por ativo	Requisições por ativo	ativo	TOP do número de requisições por ativo
TOP 10 – Requisições por origem	Soma do número de requisições por origem	Requisições por origem	Origem	TOP do número de requisições por origem

TABELA 02 - INDICADORES ESTRATÉGICOS DE ADMINISTRAÇÃO, OPERAÇÃO, MANUTENÇÃO E ATENDIMENTO DE REQUISIÇÕES

2.5.2. Tais relatórios e indicadores devem ser apresentados e discutidos em reunião mensal, com presença de profissional que conheça todos os serviços. Nesse contexto, o profissional deve apresentá-lo de forma presencial nas dependências da CONTRATANTE em Brasília-DF ou de forma virtual, por meio de solução de videoconferência.

3. GRUPO 1 – Item 02: SERVIÇO DE GESTÃO DE VULNERABILIDADES

3.1. Condições Gerais

3.1.1. Tem por objetivo, de forma proativa e recorrente, identificar possíveis vulnerabilidades de segurança da informação, na infraestrutura e aplicações do CNJ, a fim de evitar que ataques cibernéticos obtenham sucesso explorando vulnerabilidades conhecidas.

3.1.2. O serviço gestão de vulnerabilidade deverá ser dimensionado para, no mínimo, 2050 ativos. A tabela abaixo apresenta o quantitativo de dispositivos ou IPs no ambiente de TI do CNJ que devem fazer parte do escopo do serviço:

DESCRIÇÃO	QUANTIDADE
-----------	------------



Poder Judiciário

Conselho Nacional de Justiça

Aplicações Web	50
Servidores físicos e Virtuais	800
Estações de trabalho (por amostragem)	500
Containers (por amostragem)	200
Ativos de rede e segurança (on-premises e cloud)	200
Telefones VoIP, câmeras IP, impressoras etc. (por amostragem)	300

3.1.3.A CONTRATADA deverá garantir cobertura recorrente de todo o parque contemplado no escopo contratual, observando, no mínimo, a execução mensal de varreduras sobre 30 aplicações e 1000 ativos. Embora esses números sejam o mínimo a ser considerado no serviço mensal, a CONTRATADA deverá ser responsável pelo acompanhamento contínuo do ciclo de vida das vulnerabilidades identificadas nos demais ativos do CNJ conforme disposto no item 3.2 - Processo de Gestão de Vulnerabilidades.

3.1.4.A CONTRATADA deverá prover serviço de gestão de correções (patch management) de forma contínua, contemplando identificação, priorização, teste, distribuição, aplicação, validação e acompanhamento das atualizações e correções de segurança em ativos de TI, observados os processos de mudança e as responsabilidades operacionais definidas pela CONTRATANTE.

3.1.5.A CONTRATADA deverá prover serviço de Breach and Attack Simulation (BAS) contemplando a execução controlada de simulações de ataques, com foco em validação contínua da postura de segurança.

3.1.6.O serviço de gestão de vulnerabilidades deverá contemplar, no mínimo, as seguintes atividades:

3.1.6.1. Preparação e realização de varreduras para análise de vulnerabilidades de ativos de infraestrutura de TI e aplicações Web e elaboração de relatório da análise;

3.1.6.2. Instalação, configuração e documentação das ferramentas fornecidas, inclusive suas integrações;

3.1.6.3. Apoio na manutenção preventiva, corretiva e atualizações das ferramentas fornecidas;



Poder Judiciário

Conselho Nacional de Justiça

- 3.1.6.4. Gerar mensalmente relatório com serviços realizados no mês, vulnerabilidades não corrigidas e tempos de atendimento. O relatório mensal poderá ser customizado de acordo com a necessidade do CNJ;
- 3.1.6.5. Identificar possíveis vulnerabilidades de segurança da informação, a fim de apoiar a definição de plano de ação mensal e evitar que ataques cibernéticos obtenham sucesso explorando vulnerabilidades conhecidas; e
- 3.1.6.6. A CONTRATADA deve apresentar relatório das principais remediações para o tratamento das vulnerabilidades mais comuns, das vulnerabilidades mais críticas e dos exploits conhecidos.

3.2. Processo de Gestão de Vulnerabilidades

3.2.1. Processo de Gestão Contínua da Exposição a Ameaças (Continuous Threat Exposure Management – CTEM)

- 3.2.1.1. A CONTRATANTE disponibilizará à CONTRATADA uma lista de ativos e recursos que integrarão o processo de gestão de vulnerabilidades. Essa lista poderá ser revisada e atualizada ao longo de toda a vigência contratual e deverá conter, no mínimo, as seguintes informações:
 - 3.2.1.1.1. Nome do ativo e/ou serviço;
 - 3.2.1.1.2. Grupo de serviço;
 - 3.2.1.1.3. IP;
 - 3.2.1.1.4. Janela de análise (Horário permitido para análise);
 - 3.2.1.1.5. Prioridade.
- 3.2.1.2. A CONTRATADA deverá realizar, de forma contínua, avaliação prévia do ambiente computacional da CONTRATANTE, a fim de consultivamente sugerir a inclusão, exclusão ou atualização da lista de ativos e recursos fornecida pela CONTRATANTE.
- 3.2.1.3. Com base nos critérios e variáveis definidos no catálogo de serviço, bem como na lista de ativos e recursos da CONTRATANTE, a CONTRATADA deverá executar rotinas de checagens (scans) e varreduras para identificação de vulnerabilidades de segurança no



Poder Judiciário

Conselho Nacional de Justiça

ambiente da CONTRATANTE, utilizando as ferramentas e soluções definidas no presente termo de referência.

- 3.2.1.4. Após o término das rotinas de checagens (scans) e varreduras no ambiente, a CONTRATADA deverá realizar a análise de falsos positivos das vulnerabilidades identificadas, devendo reportar à CONTRATANTE apenas aquelas comprovadamente existentes no ambiente.
- 3.2.1.5. Após análise de falso positivo, a CONTRATADA deverá comunicar formalmente à CONTRATANTE as vulnerabilidades encontradas, obedecendo os critérios e requisitos estabelecidos no tópico ENTREGAS A SEREM REALIZADAS.
- 3.2.1.6. Para as vulnerabilidades encontradas no ambiente que ainda não tiverem soluções conhecidas, caberá a CONTRATADA apresentar medidas de contorno, que para aplicá-las ao ambiente, deverá obedecer ao ciclo de mudança estabelecido nos parágrafos anteriores.
 - 3.2.1.6.1. Medidas de contorno podem ser, por exemplo, criação de regras de isolamento dos ativos vulneráveis em firewall, WAF, IPS, ou outros controles disponibilizados pela CONTRATANTE.
- 3.2.1.7. Para vulnerabilidades conhecidas e catalogadas em bases públicas ou privadas (tais como CVE, CVSS ou outras), a CONTRATADA deverá apresentar relatório detalhado, especificando a vulnerabilidade e propondo a solução, como por exemplo, a aplicação de patch do fabricante ou aplicação de blindagem por meio de patch virtual.
- 3.2.1.8. Após a apresentação do relatório com as vulnerabilidades identificadas, caberá à CONTRATANTE definir a estratégia de tratamento aplicável (remediação, mitigação, aceite de risco ou outra medida cabível), bem como autorizar a aplicação das correções propostas e definir as respectivas janelas de manutenção.
- 3.2.1.9. Após a autorização da CONTRATANTE, a CONTRATADA deverá realizar o acompanhamento do processo de tratamento das vulnerabilidades, incluindo a abertura, encaminhamento e acompanhamento de chamados junto às equipes técnicas responsáveis pela execução das correções.
 - 3.2.1.9.1. A CONTRATADA deverá acompanhar e coordenar o tratamento das vulnerabilidades identificadas, podendo



Poder Judiciário

Conselho Nacional de Justiça

executar diretamente ações de remediação relacionadas ao processo de gerenciamento de correções (patch management), especialmente aplicação de patches e atualizações suportadas pelas ferramentas e ativos sob sua gestão operacional.

3.2.1.9.2. Quando as vulnerabilidades dependerem de atuação específica de equipes da CONTRATANTE, outros contratos, fabricantes ou responsáveis pelos ativos, a CONTRATADA deverá acompanhar o tratamento até sua efetiva remediação, mitigação ou aceite formal do risco.

3.2.1.10. Após a implementação das medidas de tratamento, a CONTRATADA deverá executar nova validação técnica para confirmar a efetiva correção ou mitigação da vulnerabilidade, bem como atualizar os registros, indicadores e controles definidos no tópico ENTREGAS A SEREM REALIZADAS.

3.2.1.11. O processo descrito é o mínimo esperado a ser seguido e executado pela CONTRATADA, todavia como o objeto do presente termo de referência se trata de um serviço continuado, logo se espera da CONTRATADA a apresentação da melhoria contínua deste, a qual pode ser alterado desde que aprovado pela CONTRATANTE.

3.2.1.12. O ciclo de vida do processo de gestão de vulnerabilidade deve ser executado de forma recorrente. O início do processo não se limita apenas em rotinas de tempo definidas, mas poderá a CONTRATANTE também solicitar análises sob demanda a qualquer tempo.

3.2.2. Processo de Gerenciamento de Correções (Patch Management)

3.2.2.1. A CONTRATADA deverá realizar o processo contínuo de gestão de patches, contemplando a identificação, avaliação, priorização, teste e aplicação de atualizações de segurança e correções em sistemas operacionais, aplicações suportadas pelas ferramentas disponibilizadas, estações de trabalho, servidores e demais ativos elegíveis definidos pela CONTRATANTE.

3.2.2.2. A CONTRATADA deverá manter inventário atualizado dos ativos sob gestão, incluindo servidores, estações de trabalho e softwares instalados, como base para o processo de patch management.



Poder Judiciário

Conselho Nacional de Justiça

- 3.2.2.3. A CONTRATADA deverá monitorar continuamente boletins de segurança dos fabricantes e bases de vulnerabilidades, avaliando criticidade e exposição do ambiente.
- 3.2.2.4. A CONTRATADA deverá classificar e priorizar patches com base em criticidade, risco de exploração, impacto ao negócio e acordos de nível de serviço (SLA) definidos.
- 3.2.2.5. A CONTRATADA deverá executar testes prévios de patches em ambientes controlados, quando aplicável, a fim de mitigar riscos de indisponibilidade ou impacto operacional.
- 3.2.2.6. A CONTRATADA deverá realizar a aplicação dos patches em janelas de manutenção previamente acordadas, garantindo o menor impacto possível aos serviços.
 - 3.2.2.6.1. A aplicação de patches deverá sempre respeitar os processos de mudança da CONTRATANTE, incluindo aprovação prévia e definição de janelas de manutenção.
 - 3.2.2.6.2. A CONTRATADA poderá executar rotinas automatizadas de deployment de patches, desde que previamente autorizadas pela CONTRATANTE e integradas aos processos de mudança.
- 3.2.2.7. A CONTRATADA deverá implementar procedimentos de rollback em caso de falhas decorrentes da aplicação de patches.
- 3.2.2.8. A CONTRATADA deverá gerar relatórios periódicos contendo status de atualização, ativos vulneráveis, patches pendentes e indicadores de conformidade.
- 3.2.2.9. A CONTRATADA deverá manter níveis mínimos de conformidade de patches conforme políticas de segurança definidas pela CONTRATANTE.
- 3.2.2.10. A CONTRATADA deverá integrar o processo de patch management com a gestão de vulnerabilidades e demais ferramentas de segurança existentes no ambiente.
- 3.2.2.11. A CONTRATADA deverá registrar e documentar todas as atividades realizadas, incluindo evidências de aplicação, falhas e exceções.
- 3.2.2.12. A CONTRATADA deverá tratar exceções de aplicação de patches, mediante justificativa formal e aprovação da CONTRATANTE.



Poder Judiciário

Conselho Nacional de Justiça

3.2.2.13. A CONTRATADA deverá atuar proativamente na remediação de vulnerabilidades críticas dentro dos prazos estabelecidos em SLA.

3.2.2.14. Após a aplicação das correções ou medidas de mitigação, a CONTRATADA deverá executar nova validação técnica, a fim de confirmar a efetiva remediação da vulnerabilidade e registrar as evidências correspondentes.

3.2.3. Processo de Breach Attack Simulation (BAS)

3.2.3.1. A CONTRATADA deverá configurar e manter cenários de simulação de ataques baseados em ameaças reais, alinhados a frameworks reconhecidos de mercado, como MITRE ATT&CK, garantindo a aderência às táticas, técnicas e procedimentos (TTPs) atualizados.

3.2.3.2. Toda simulação BAS deverá ocorrer mediante escopo previamente aprovado pela CONTRATANTE, com definição de janelas, critérios de interrupção e plano de contingência.

3.2.3.3. A CONTRATADA deverá executar simulações automatizadas e contínuas de ataques cibernéticos, sem impacto na disponibilidade dos ambientes de produção, validando controles de segurança existentes.

3.2.3.4. A CONTRATADA deverá avaliar a eficácia dos controles de segurança, incluindo ferramentas de detecção, prevenção e resposta, identificando falhas, lacunas e oportunidades de melhoria.

3.2.3.5. A CONTRATADA deverá gerar relatórios executivos e técnicos contendo os resultados das simulações, evidências de exploração, nível de exposição e recomendações de remediação.

3.2.3.6. A CONTRATADA deverá apoiar o processo de priorização e tratamento de vulnerabilidades, com base em evidências obtidas nas simulações de ataque.

3.2.3.7. A CONTRATADA deverá manter atualizados os cenários de ataque e indicadores de compromisso (IoCs), acompanhando a evolução do cenário de ameaças.

3.2.3.8. A CONTRATADA deverá validar continuamente a eficácia das ações de remediação implementadas, por meio da reexecução das simulações.



Poder Judiciário

Conselho Nacional de Justiça

3.2.3.9. A CONTRATADA deverá garantir a rastreabilidade e histórico das execuções de simulações, permitindo auditoria e análise evolutiva do ambiente.

3.3. Ferramentas

3.3.1. Para a prestação deste serviço deverão ser utilizadas ferramentas para descoberta de vulnerabilidades de aplicações e infraestrutura, bem como para gestão de todo o ciclo de vida das vulnerabilidades encontradas, desde a descoberta até a correta mitigação.

3.3.2. Deverá ser fornecida pela CONTRATADA, pelo menos:

3.3.2.1. 01 (uma) ferramenta de análise de vulnerabilidade com foco em infraestrutura e em aplicações WEB;

3.3.2.2. 01 (uma) ferramenta de Simulação de Brechas e Ataques (BAS – Breach and Attack Simulation), destinada à simulação controlada de ataques e validação contínua da efetividade dos controles de segurança do ambiente; e

3.3.2.3. 01 (uma) ferramenta de gerenciamento de correções (patch management).

3.3.3. Será de responsabilidade da CONTRATADA operar, sustentar, suportar e apresentar a melhoria contínua das ferramentas ofertadas durante todo o período de vigência do contrato.

3.3.4. A CONTRATADA deverá garantir atualização contínua das assinaturas, mecanismos de detecção, feeds de inteligência, bases de vulnerabilidades e componentes das soluções utilizadas durante toda a vigência contratual.

3.3.5. Os requisitos técnicos previstos neste item poderão ser atendidos por uma ou mais soluções integradas, do mesmo fabricante ou de fabricantes distintos, desde que operem de forma integrada e atendam integralmente às funcionalidades e níveis de serviço exigidos neste Termo de Referência.

3.3.6. Solução de Gestão de Vulnerabilidades

3.3.6.1. A solução de gestão de vulnerabilidades a ser ofertada pela CONTRATADA deverá realizar varredura e descoberta de vulnerabilidades para os ativos que compõem o ambiente computacional do CONTRATANTE, incluindo estações de trabalho, notebooks, switches,



Poder Judiciário

Conselho Nacional de Justiça

roteadores, access points, servidores de rede, servidores de aplicações, servidores de banco de dados, entre outros.

3.3.6.2. A ferramenta de gestão de vulnerabilidades deverá ser capaz de escanear e gerenciar o parque da CNJ, podendo ser estações de trabalho, notebooks, switches, roteadores, access points, servidores de rede, servidores de aplicações, servidores de banco de dados, aplicações Web, APIs, contêineres entre outros, conforme as quantidades abaixo:

3.3.6.2.1. Possibilidade de analisar até 50 (cinquenta) aplicações Web e APIs;

3.3.6.2.2. Possibilidade de analisar até 2000 (dois mil) dispositivos/IPs.

3.3.6.3. A solução deverá realizar descoberta de topologia de ativos de rede, com base em informações de endereço IP e subrede.

3.3.6.4. A solução deverá permitir agrupamento lógico e dinâmico de ativos, com base em atributos como sistema operacional, endereço IP, DNS, NetBIOS Host, MAC Address, software instalado e demais atributos disponíveis.

3.3.6.5. A solução deverá permitir a seleção e inclusão de faixas de endereços IP para varredura, bem como a definição de faixas de exclusão.

3.3.6.6. A solução deverá suportar varreduras de ativos de modo intrusivo e não intrusivo.

3.3.6.7. A solução deverá permitir a definição de templates de configuração de varreduras (scans), incluindo agendamento e periodicidade.

3.3.6.8. A solução deverá permitir configuração de usuário e senha para realização de varredura autenticada em sistemas operacionais e aplicações Web.

3.3.6.9. A solução deverá permitir a configuração de frequência e periodicidade de varreduras na rede.

3.3.6.10. A solução deverá suportar varreduras autenticadas e não autenticadas, podendo utilizar mecanismos com agente, sem agente, ativos ou passivos, de forma isolada ou combinada, desde que atendidos os requisitos funcionais previstos neste Termo de Referência.



Poder Judiciário

Conselho Nacional de Justiça

- 3.3.6.11. A solução deverá ser capaz de realizar varredura de ativos na rede interna, ativos expostos em redes externas, bem como ativos em nuvens públicas amplamente utilizadas pelo mercado, tais como AWS, Microsoft Azure e Google Cloud Platform (GCP).
- 3.3.6.12. A solução deverá detectar vulnerabilidades em sistemas operacionais, protocolos de rede, aplicações Web, banco de dados, aplicativos para escritório e demais softwares presentes no ambiente.
- 3.3.6.13. A solução deverá detectar vulnerabilidades em ambiente Linux e Microsoft Windows, incluindo hotfixes, Service Packs e registros de sistema operacional.
- 3.3.6.14. A solução deverá detectar vulnerabilidades em ambientes Oracle, SQL Server, Microsoft Exchange, contêineres e VMware.
- 3.3.6.15. A solução deverá integrar-se à base de vulnerabilidades CVE (Common Vulnerabilities and Exposures), mantendo atualização contínua de assinaturas e base de conhecimento.
- 3.3.6.16. A solução deverá permitir geração de tickets para vulnerabilidades encontradas, possibilitando o acompanhamento do tratamento, marcação como corrigida, mitigada ou aceita/ignorada.
- 3.3.6.17. A solução deverá fornecer recurso para acompanhamento da evolução das remediações de vulnerabilidades encontradas, com histórico de indicadores ao longo do tempo.
- 3.3.6.18. A solução deverá permitir acompanhamento histórico do nível de exposição do CONTRATANTE, com registro de evolução das vulnerabilidades, ativos e indicadores de risco ao longo do tempo.
- 3.3.6.19. A solução deverá apresentar procedimentos necessários para eliminar, remediar ou mitigar vulnerabilidades encontradas, tais como indicação de atualizações de software.
- 3.3.6.20. A solução deverá prover visão sobre quais ações de remediação reduzem o maior nível de risco do ambiente, possibilitando priorização objetiva das correções.
- 3.3.6.21. A solução deverá possuir, no mínimo, 3 (três) níveis de criticidade de vulnerabilidades.



Poder Judiciário

Conselho Nacional de Justiça

- 3.3.6.22. A solução deverá apresentar graduação de riscos baseada em pontuação, permitindo medir o nível de risco dos recursos e sistemas encontrados, bem como priorizar ameaças conforme critérios definidos para o ambiente.
- 3.3.6.23. A solução deverá utilizar sistema de pontuação e priorização das vulnerabilidades, considerando, no mínimo, os seguintes critérios:
- 3.3.6.23.1. CVSS Impact Score;
 - 3.3.6.23.2. Existência de códigos de exploração da vulnerabilidade encontrada (exploit);
 - 3.3.6.23.3. Existência de evidências de explorabilidade da vulnerabilidade, incluindo a disponibilidade de técnicas ou mecanismos de exploração em ferramentas automatizadas, públicas ou comerciais, ou ainda informações provenientes de fontes de inteligência de ameaças.
- 3.3.6.24. A solução deverá realizar levantamento e classificação da criticidade dos ativos, considerando a importância do ativo e as vulnerabilidades encontradas.
- 3.3.6.25. A solução deverá permitir a alteração manual da classificação de criticidade dos ativos, possibilitando sobrescrever a classificação atribuída automaticamente.
- 3.3.6.26. A solução deverá possuir painéis gerenciais (dashboards) pré-definidos para rápida visualização dos resultados, permitindo também a criação e customização de painéis personalizados.
- 3.3.6.27. Os dashboards deverão ser apresentados em diversos formatos, incluindo gráficos e tabelas, possibilitando a exibição de informações em diferentes níveis de detalhamento.
- 3.3.6.28. A solução deverá permitir customização de dashboards e relatórios gerenciais.
- 3.3.6.29. A solução deverá apresentar relatórios analíticos contendo dados, informações, indicadores e métricas que permitam avaliar a exposição do parque computacional do CNJ em relação aos riscos de segurança em TI, contendo, no mínimo: hosts encontrados, topologia de rede, serviços,



Poder Judiciário

Conselho Nacional de Justiça

vulnerabilidades descobertas, nível de risco por plataforma e por vulnerabilidade.

3.3.6.30. A solução deverá permitir exportação de relatórios, no mínimo, nos formatos HTML, PDF e CSV.

3.3.6.31. A solução deverá possuir gerenciamento por interface Web (WebUI) via HTTPS e console gráfica centralizada.

3.3.6.32. Os requisitos de implantação e operação da solução poderão ser atendidos por modelo local (on-premises), em nuvem (SaaS) ou híbrido, não sendo obrigatória a instalação integral da solução em ambiente da CONTRATANTE, desde que atendidos os requisitos funcionais, de segurança e de integração previstos neste Termo de Referência.

3.3.6.33. A solução deverá possuir gerenciamento único e centralizado, responsável pela aplicação de políticas de segurança, administração e controle das funcionalidades dos serviços, incluindo scanners, sensores e agentes.

3.3.6.34. A solução deverá permitir o agrupamento lógico de scanners e sensores para facilitar o gerenciamento e aplicação de políticas.

3.3.6.35. A solução deverá suportar múltiplos usuários simultâneos, em quantidade compatível com as necessidades operacionais e administrativas da CONTRATANTE.

3.3.6.36. A solução deverá possuir API para automação de processos e integração com produtos de terceiros.

3.3.6.37. A solução deverá suportar operações de consulta, inclusão, atualização e remoção via API.

3.3.6.38. A solução deverá possuir gerenciamento com perfis de acessos distintos para administração de funcionalidades, acesso a logs e emissão de relatórios.

3.3.6.39. A solução deverá fornecer controle de acesso baseado em função (RBAC - Role Based Access Control), permitindo controle de acesso do usuário a conjuntos de dados e funcionalidades.



Poder Judiciário

Conselho Nacional de Justiça

- 3.3.6.40. A solução deverá ser capaz de definir e gerenciar grupos de usuários, incluindo limitação de funções de varredura e acesso a relatórios e dashboards.
- 3.3.6.41. A solução deverá suportar autenticação utilizando base local e mecanismos de federação de identidade, incluindo SAML (Security Assertion Markup Language), OAuth 2.0 ou OpenID Connect (OIDC), possibilitando integração com SSO.
- 3.3.6.42. A solução deverá criptografar os resultados de varreduras e as informações inseridas na plataforma, tanto em repouso quanto em trânsito.
- 3.3.6.43. A solução deverá possuir recurso de auditoria de alteração de configurações e acesso à ferramenta de administração, incluindo usuário, data e horário de acesso e ações realizadas.
- 3.3.6.44. A solução deverá apresentar, para cada vulnerabilidade encontrada, descrição detalhada e os passos recomendados para correção.
- 3.3.6.45. A solução deverá apresentar, para cada vulnerabilidade encontrada, evidências técnicas por meio de saídas das verificações realizadas (outputs).
- 3.3.6.46. Os detalhes das vulnerabilidades deverão conter descrição da falha, referências para consulta e soluções propostas para mitigação ou remediação.
- 3.3.6.47. A solução deverá permitir alertas automáticos por e-mail sobre vulnerabilidades encontradas e/ou mudanças relevantes de exposição.
- 3.3.6.48. A solução deverá ser capaz de analisar, testar e reportar falhas de segurança em aplicações Web como parte dos ativos a serem inspecionados.
- 3.3.6.49. A solução deverá ser capaz de executar varreduras em sistemas Web através de seus endereços IP ou FQDN (DNS).
- 3.3.6.50. A solução deverá avaliar, no mínimo, os padrões OWASP Top 10.
- 3.3.6.51. Para varreduras extensas e detalhadas em aplicações Web, a solução deverá ser capaz de varrer e auditar, no mínimo, os seguintes elementos: cookies, headers, formulários, links, nomes e valores de parâmetros da aplicação e elementos JSON e XML.



Poder Judiciário

Conselho Nacional de Justiça

- 3.3.6.52. A solução deverá permitir a identificação de links em aplicações Web e navegação pelos links identificados (crawler).
- 3.3.6.53. A solução deverá permitir a execução exclusiva da função crawler para navegação e descoberta das URLs existentes na aplicação.
- 3.3.6.54. A solução deverá permitir excluir determinadas URLs da varredura através de expressões regulares.
- 3.3.6.55. A solução deverá permitir excluir determinados tipos de arquivos através de suas extensões.
- 3.3.6.56. A solução deverá permitir parametrização das rotinas de navegação e varredura em aplicações Web, incluindo mecanismos de controle de escopo, desempenho e impacto operacional.
- 3.3.6.57. A solução deverá ser compatível com avaliação de Web Services REST e SOAP.
- 3.3.6.58. Para vulnerabilidades de injeção de código (SQL, XSS, XSRF, entre outras), a solução deverá apresentar evidências detalhadas, incluindo payload injetado, resposta da aplicação, detalhes da requisição HTTP e detalhes da resposta HTTP.
- 3.3.6.59. A solução deverá ser capaz de analisar e identificar vulnerabilidades específicas para o Active Directory, incluindo verificações relacionadas a configurações inseguras e fragilidades de autenticação Kerberos.
- 3.3.6.60. A solução deverá incluir a opção de utilização de agentes instalados e licenciados em estações de trabalho e servidores, para varredura diretamente no sistema operacional.
- 3.3.6.61. Os agentes deverão ser gerenciados pela mesma interface/console da plataforma de gestão de vulnerabilidades.
- 3.3.6.62. A solução deverá possuir capacidade de realizar o escaneamento de vulnerabilidades em imagens e contêineres, podendo integrar-se a pipelines CI/CD ou mecanismos equivalentes de automação de desenvolvimento e implantação.
- 3.3.6.63. A solução deverá analisar, testar e reportar falhas de segurança em aplicações em contêineres Docker como parte dos ativos a serem inspecionados.



Poder Judiciário

Conselho Nacional de Justiça

- 3.3.6.64. A solução deverá ser capaz de analisar imagens preparadas pelos desenvolvedores na esteira DevOps em busca de vulnerabilidades identificadas e malware residente no sistema de arquivos.
- 3.3.6.65. A solução deverá integrar-se à esteira DevOps através de API, permitindo envio de imagens para análise, inclusive, quando aplicável, por meio de componentes implantados em infraestrutura da CONTRATANTE, de modo a evitar o envio de imagens e propriedade intelectual para ambientes externos.
- 3.3.6.66. A solução deverá inventariar o sistema operacional de cada imagem analisada e reportar vulnerabilidades encontradas.
- 3.3.6.67. A solução deverá permitir rastreabilidade e comparação entre imagens analisadas, versões e componentes identificados ao longo do ciclo de desenvolvimento e implantação.
- 3.3.6.68. A solução deverá informar os CVEs para cada vulnerabilidade encontrada nos pacotes e bibliotecas residentes na imagem.
- 3.3.6.69. A solução deverá ter capacidade de reavaliar automaticamente imagens previamente analisadas sempre que uma nova vulnerabilidade for publicada e atualizada na base de dados, sem intervenção manual.
- 3.3.6.70. A solução deverá inventariar pacotes e bibliotecas, com suas respectivas versões, e listar tais informações nos relatórios de análise.
- 3.3.6.71. A solução deverá possuir conectores e permitir importação de imagens com repositórios amplamente utilizados pelo mercado, tais como Docker Registry, Azure Container Registry, Docker EE, AWS ECR, Google Artifact Registry, JFrog Artifactory ou equivalentes.
- 3.3.6.72. A solução deverá disponibilizar scanner em formato contêiner (Docker) para implementação local e análise de imagens sem necessidade de envio para repositório remoto externo ao ambiente do CONTRATANTE.

3.3.7. Solução de Breach and Attack Simulation (BAS)

- 3.3.7.1. A solução de Breach and Attack Simulation (BAS) a ser ofertada pela CONTRATADA deverá permitir a execução automatizada e controlada de simulações de ataques, com foco em validação contínua da postura de segurança.



Poder Judiciário

Conselho Nacional de Justiça

3.3.7.2. A solução deverá possuir capacidade técnica para execução de simulações de ataques em ativos e aplicações do ambiente do CONTRATANTE, observando-se, como escopo operacional mínimo mensal do serviço, a realização de simulações controladas sobre ao menos 30 (trinta) endereços IP e 5 (cinco) aplicações. A tabela abaixo apresenta o quantitativo inicial de referência para execução das simulações previstas neste serviço:

DESCRIÇÃO	QUANTIDADE
Endereços IP	30
Aplicações	05

3.3.7.3. A solução deverá permitir simulações de ataques com base em frameworks reconhecidos, incluindo, no mínimo, MITRE ATT&CK.

3.3.7.4. A solução deverá possibilitar simulações recorrentes, com agendamento e execução automática, permitindo avaliações contínuas do ambiente.

3.3.7.5. A solução deverá permitir a criação e execução de campanhas de simulação com diferentes níveis de complexidade e escopo.

3.3.7.6. A solução deverá permitir simulações em ambientes on-premises e em ambientes em nuvem amplamente utilizados pelo mercado, tais como, AWS, Microsoft Azure e Google Cloud Platform (GCP).

3.3.7.7. A solução deverá suportar simulações de ataques relacionados, no mínimo, a:

3.3.7.7.1. movimentação lateral;

3.3.7.7.2. execução remota de comandos;

3.3.7.7.3. elevação de privilégio;

3.3.7.7.4. persistência;

3.3.7.7.5. exploração de vulnerabilidades conhecidas;

3.3.7.7.6. exfiltração de dados simulada;

3.3.7.7.7. comunicação com infraestrutura simulada de comando e controle (C2);



Poder Judiciário

Conselho Nacional de Justiça

3.3.7.7.8. ataques de força bruta;

3.3.7.7.9. técnicas de evasão e bypass de controles de segurança.

3.3.7.8. A solução deverá permitir execução de simulações voltadas à validação de detecção de malware e/ou ransomware, de forma segura e controlada.

3.3.7.9. A solução deverá suportar simulações voltadas à validação de segurança em ambientes de identidade corporativa, incluindo Active Directory, podendo contemplar técnicas relacionadas a autenticação, exposição de serviços e privilégios.

3.3.7.10. A solução deverá permitir simulação de ataques contra aplicações Web e APIs, incluindo exploração de falhas comuns.

3.3.7.10.1. Deverá permitir simulação de ataques alinhados ao OWASP Top 10.

3.3.7.10.2. Deverá permitir execução de testes controlados de SQL Injection, XSS, CSRF, autenticação fraca e falhas de autorização.

3.3.7.10.3. Deverá permitir validação de mecanismos de proteção como WAF, rate limiting e políticas de autenticação.

3.3.7.11. A solução deverá ser capaz de validar a efetividade de controles de segurança existentes no ambiente, incluindo controles como:

3.3.7.11.1. EDR/XDR;

3.3.7.11.2. antivírus corporativo;

3.3.7.11.3. SIEM;

3.3.7.11.4. SOAR;

3.3.7.11.5. IDS/IPS;

3.3.7.11.6. firewalls e NGFW;

3.3.7.11.7. WAF;

3.3.7.11.8. DLP.



Poder Judiciário

Conselho Nacional de Justiça

- 3.3.7.12. A solução deverá permitir integração com soluções de terceiros por meio de API.
- 3.3.7.13. A solução deverá permitir integração ou correlação de resultados com eventos registrados em soluções SIEM ou equivalentes, possibilitando evidenciar se a simulação gerou alertas ou não.
- 3.3.7.14. A solução deverá gerar evidências técnicas completas das simulações executadas, incluindo registro detalhado das etapas realizadas e dos resultados obtidos.
- 3.3.7.15. A solução deverá produzir relatórios gerenciais e técnicos, contendo, no mínimo:
- 3.3.7.15.1. descrição do cenário simulado;
 - 3.3.7.15.2. técnicas e táticas executadas;
 - 3.3.7.15.3. resultados obtidos (detecção, bloqueio, falha, parcial);
 - 3.3.7.15.4. controles que responderam adequadamente ou falharam;
 - 3.3.7.15.5. indicadores de maturidade e gaps identificados;
 - 3.3.7.15.6. recomendações de melhoria.
- 3.3.7.16. A solução deverá permitir exportação de relatórios, no mínimo, nos formatos PDF, CSV e HTML.
- 3.3.7.17. A solução deverá disponibilizar dashboards com indicadores de desempenho e evolução do ambiente ao longo do tempo.
- 3.3.7.18. A solução deverá manter histórico das simulações executadas e seus resultados, permitindo comparação evolutiva.
- 3.3.7.19. A solução deverá permitir configuração centralizada, com interface de gerenciamento via WebUI.
- 3.3.7.20. A solução deverá permitir definição de escopo de simulação, incluindo seleção de ativos, redes, ambientes e aplicações.
- 3.3.7.21. A solução deverá permitir definição de janelas de execução, evitando impactos operacionais e respeitando períodos críticos do CONTRATANTE.



Poder Judiciário

Conselho Nacional de Justiça

3.3.7.22. A solução deverá permitir execução segmentada e controlada, com mecanismos de segurança para evitar indisponibilidade ou impactos no ambiente produtivo.

3.3.7.23. A solução deverá possuir ou utilizar base atualizada de cenários e técnicas de ataque, com atualização contínua durante toda a vigência contratual.

3.3.8. Solução de Gerenciamento de Correções (Patch Management)

3.3.8.1. A solução para patch management deverá ser dimensionada para, no mínimo, 1500 dispositivos. A tabela abaixo apresenta o quantitativo de dispositivos no ambiente de TI do CNJ que devem fazer parte do escopo do serviço:

DESCRIÇÃO	QUANTIDADE
Servidores Físicos, Virtuais ou Estações de trabalho	1500

3.3.8.2. A CONTRATADA deverá prover, obrigatoriamente, solução de **gestão de correções (patch management)** complementar às ferramentas já utilizadas pela CONTRATANTE, notadamente Microsoft Intune e Microsoft Defender.

3.3.8.3. Para fins deste Termo de Referência, considera-se que as soluções Microsoft Intune e Microsoft Defender já atendem parcialmente à gestão de atualizações de sistemas operacionais e aplicações Microsoft, cabendo à solução a ser fornecida pela CONTRATADA complementar as seguintes capacidades:

3.3.8.3.1. Gestão e aplicação de patches em **aplicações de terceiros (third-party)** não cobertas nativamente pelo Intune/Defender;

3.3.8.3.2. Identificação, priorização e remediação de vulnerabilidades associadas a softwares instalados nos ativos inventariados;

3.3.8.3.3. Correlação entre vulnerabilidades identificadas (CVE) e patches disponíveis, permitindo priorização baseada em risco;

3.3.8.3.4. Visibilidade consolidada do nível de atualização de ativos, incluindo softwares, bibliotecas e componentes não Microsoft;



Poder Judiciário

Conselho Nacional de Justiça

- 3.3.8.3.5. Suporte à aplicação de patches em ambientes heterogêneos, incluindo sistemas Windows e Linux, quando aplicável;
- 3.3.8.3.6. Capacidade de geração de relatórios gerenciais e técnicos sobre o estado de atualização e conformidade dos ativos.
- 3.3.8.4. A solução de patch management fornecida deverá operar de forma integrada ou complementar, não substituindo as ferramentas já existentes no ambiente da CONTRATANTE.
- 3.3.8.5. A CONTRATADA deverá garantir que a solução proposta seja compatível com o ambiente atual da CONTRATANTE, observando-se a necessidade de evitar sobreposição desnecessária de funcionalidades já atendidas de maneira satisfatória pelas soluções atualmente utilizadas pela CONTRATANTE. Poderão existir funcionalidades coincidentes, desde que agreguem ganho operacional, ampliação de cobertura técnica, melhoria da visibilidade, correlação de vulnerabilidades, automação de remediação ou evolução da gestão de vulnerabilidades e correções.
- 3.3.8.6. Deve suportar o gerenciamento de patches (atualizações corretivas) em software, com as seguintes características mínimas:
 - 3.3.8.6.1. Deve correlacionar vulnerabilidades e patches automaticamente para os hosts;
 - 3.3.8.6.2. Realizar distribuição e aplicação (deploy) de patches para ativos Windows e Linux.
- 3.3.8.7. Ter a capacidade de realizar reversão (rollback) de patch minimamente em sistemas operacionais Windows.
- 3.3.8.8. Agendar tarefas de execução de forma pontual ou recorrentes para ativos Windows e Linux.
- 3.3.8.9. Mostrar de forma clara patches ativos e ausentes para sistemas operacionais Windows.
- 3.3.8.10. Deve mostrar patches faltantes mesmo que não exista correlação com uma vulnerabilidade existente.
- 3.3.8.11. Deve permitir acompanhar a aplicação de patches por meio de console administrativa ou painéis (dashboards).



Poder Judiciário

Conselho Nacional de Justiça

- 3.3.8.12. Deve mostrar ativos que não possuem patches de segurança instalados.
- 3.3.8.13. Deve mostrar ativos pendente de reinicialização do sistema operacional para aplicação de patches.
- 3.3.8.14. Deve mostrar status de aplicação (sucesso, pendência, falha etc.) de patches.
- 3.3.8.15. Deve mostrar Patches faltantes por severidade.
- 3.3.8.16. Deve conter uma lista de produtos e softwares priorizados, permitindo visualizar patches relevantes a esses produtos.
- 3.3.8.17. Deve permitir a criação de tarefas de instalação a partir de produtos e softwares priorizados.
- 3.3.8.18. Deve ser capaz de apresentar informações de patches que já consideram e resolvem correções anteriores.
- 3.3.8.19. Deve apontar todas as versões da aplicação que são afetadas e precisam de correção.
- 3.3.8.20. A solução deverá permitir identificar ativos não cobertos por políticas de patching.
- 3.3.8.21. Deve suportar tarefas de instalação e remoção dos patches.
- 3.3.8.22. A solução deverá permitir identificar quantidade de patches aplicados em determinado período.
- 3.3.8.23. Deve permitir a execução de scripts personalizados durante a tarefa de instalação de patches.
- 3.3.8.24. Deve ser possível executar scripts Powershell antes e depois da instalação de correções.
- 3.3.8.25. A solução deverá permitir identificar dispositivos offline que não estão recebendo atualizações.
- 3.3.8.26. Deve permitir customização de mensagens para o usuário antes aplicação de patches.



Poder Judiciário

Conselho Nacional de Justiça

- 3.3.8.27. Deve enviar notificação quando uma tarefa automática de aplicação de patch é executada, incluindo e-mail, Microsoft Teams ou outros canais equivalentes.
- 3.3.8.28. Deve permitir a configuração da frequência em que a solução alerta o usuário da necessidade de reinicialização da estação de trabalho para que os patches sejam aplicados.
- 3.3.8.29. Permitir forçar a reinicialização da estação de trabalho após avisar ao usuário que é necessária a aplicação de novos patches.
- 3.3.8.30. Deve permitir a criação de fluxo de aprovação, para que determinados patches só sejam aplicados após a aprovação de um gerente ou responsável previamente definido.

3.3.9. Solução de Application Security Test (AST)

- 3.3.9.1. A CONTRATADA poderá disponibilizar, de forma opcional, funcionalidades relacionadas à análise de segurança de aplicações, incluindo **SAST (Static Application Security Testing)**, **IAST (Interactive Application Security Testing)** e **SCA (Software Composition Analysis)**, com o objetivo de apoiar a evolução da maturidade de segurança no desenvolvimento de software da CONTRATANTE.
- 3.3.9.2. A disponibilização dessas funcionalidades:
 - 3.3.9.2.1. Não constitui requisito obrigatório para fins de habilitação ou julgamento das propostas;
 - 3.3.9.2.2. Não deverá ser considerada para fins de composição de preços da proposta;
 - 3.3.9.2.3. Não configura obrigação contratual inicial da CONTRATADA.
- 3.3.9.3. Caso a CONTRATADA opte por disponibilizar tais funcionalidades durante a execução contratual, sua oferta deverá ocorrer **sem ônus adicional para a CONTRATANTE**, não implicando em qualquer tipo de cobrança direta ou indireta.
- 3.3.9.4. A eventual ativação dessas funcionalidades no ambiente da CONTRATANTE estará condicionada à avaliação técnica e à



Poder Judiciário

Conselho Nacional de Justiça

conveniência administrativa, podendo ocorrer mediante termo aditivo, quando aplicável, e desde que atendidos critérios objetivos de maturidade e necessidade.

3.3.9.5. A CONTRATANTE poderá autorizar a utilização dessas funcionalidades quando verificado, no mínimo, 01 (um) dos seguintes critérios:

- 3.3.9.5.1. Existência de processo contínuo de desenvolvimento de software, caracterizado por manutenção evolutiva ativa, desenvolvimento de novas aplicações ou APIs, com volume mínimo de 2 (duas) implantações mensais em ambiente de produção;
- 3.3.9.5.2. Existência de aplicações classificadas como críticas ou sensíveis, que tratem dados institucionais relevantes, estejam expostas à internet ou suportem serviços essenciais ao funcionamento institucional;
- 3.3.9.5.3. Identificação recorrente de vulnerabilidades em aplicações, a partir do processo de gestão de vulnerabilidades, caracterizada por ocorrência de vulnerabilidades críticas ou altas em aplicações por 3 (três) ciclos consecutivos de varredura, ou reincidência de falhas de mesma natureza;
- 3.3.9.5.4. Implantação ou evolução de esteira de desenvolvimento contínuo (CI/CD), com uso de versionamento de código, automação de builds e processos de entrega contínua;
- 3.3.9.5.5. Evidência de risco real de exploração de vulnerabilidades em aplicações, identificada por meio de simulações controladas (BAS) ou testes de invasão (Red Team);
- 3.3.9.5.6. Solicitação formal da área responsável pelo desenvolvimento de sistemas ou da área de segurança da informação, devidamente justificada e aprovada pela CONTRATANTE.

3.3.9.6. A eventual adoção dessas funcionalidades deverá observar:

- 3.3.9.6.1. Análise de viabilidade técnica e operacional;
- 3.3.9.6.2. Avaliação de custo-benefício;
- 3.3.9.6.3. Disponibilidade orçamentária, quando aplicável;



Poder Judiciário

Conselho Nacional de Justiça

3.3.9.6.4. Planejamento de integração ao ambiente tecnológico da CONTRATANTE.

3.3.9.7. A presente previsão possui caráter exclusivamente **evolutivo e não vinculante**, visando permitir a adoção futura de práticas de segurança de aplicações de forma gradual e alinhada à maturidade do ambiente, não gerando qualquer obrigação imediata à CONTRATADA.

3.3.10. As ferramentas a serem utilizadas para prestação do Serviço de Gestão de Vulnerabilidades deverão ser instaladas na CONTRATANTE ou, mediante solicitação justificada da CONTRATADA, a CONTRATANTE poderá permitir a instalação em ambiente da CONTRATADA ou em NUVEM, de modo a prover varredura, simulações, identificação, validação e gestão de vulnerabilidades do parque computacional da CONTRATANTE.

3.3.11. Apesar de ser necessário e permitido a utilização de ferramentas automatizadas para descoberta de vulnerabilidades, simulação controlada de ataques e gestão de correções (patch management) no ambiente do CNJ, espera-se que a CONTRATADA se utilize também de métodos e técnicas assistidas, incluindo análise manual e validações direcionadas, de forma complementar, para identificar, confirmar e priorizar vulnerabilidades e exposições relevantes no ambiente do CNJ, bem como validar a efetividade dos controles de segurança existentes.

3.3.12. A fim de mitigar e prever possíveis impactos durante as rotinas de validação de vulnerabilidade, antes do início da execução do serviço, as ferramentas adotadas para execução deverão ser apresentadas ao time de segurança da informação do CNJ, que avaliará sua aderência aos requisitos técnicos, operacionais e de segurança previstos neste Termo de Referência.

3.3.13. A CONTRATADA deve apresentar relatório das principais remediações para o tratamento das vulnerabilidades mais comuns, das vulnerabilidades mais críticas e dos exploits conhecidos.

3.4. Grupo de gestão de vulnerabilidades

3.4.1. Este grupo deverá ser exclusivo para trabalhar na gestão de vulnerabilidades e não podem os profissionais pertencentes a este grupo serem compartilhados e/ou atuarem, com os demais serviços descritos no objeto do presente termo de referência.



Poder Judiciário

Conselho Nacional de Justiça

3.4.2. Todos os profissionais que integram O GRUPO DE GESTÃO DE VULNERABILIDADES devem obrigatoriamente compor o quadro de colaboradores da CONTRATADA em regime de trabalho CLT (Consolidação das Leis do Trabalho), não havendo possibilidade a terceirização ou subcontratação de tal serviço.

3.4.3. Deverá ser de responsabilidade da CONTRATADA dimensionar o número de profissionais adequado para entrega de tal serviço, sem que haja impacto no acordo de nível de serviço estabelecido.

3.4.4. Com o objetivo de garantir que os profissionais envolvidos têm conhecimento e habilidade, para executar o processo de gestão de vulnerabilidades da CONTRATANTE, a CONTRATADA obrigatoriamente deverá compor o GRUPO DE DE GESTÃO DE VULNERABILIDADES com ao menos 1 (um) perfil de cada que segue descrito abaixo. O profissional deverá possuir ao menos uma das certificações indicadas no respectivo perfil, ou certificação equivalente.

Perfis	Certificações
Analista de Segurança 1	• CompTIA Security+ ou equivalente
Analista de Segurança 2	• CompTIA Cybersecurity Analyst (CySA+), GIAC GSEC, SC-200 ou equivalente
Analista de Segurança Linux	• Linux LPIC-2, RHCSA, RHCE ou equivalente
Analista de Segurança Windows	• SC-200, Windows Server Hybrid Administrator Associate ou equivalente

TABELA 03 – CERTIFICAÇÕES GRUPO DE GESTÃO DE VULNERABILIDADES

3.4.5. Durante a execução do contrato, a CONTRATADA se obriga a manter todos os profissionais com os requisitos abaixo:

3.4.5.1. Diploma, devidamente registrado, de curso de nível superior de graduação na área de Tecnologia da Informação ou de graduação em qualquer curso superior, acrescido de certificado de curso de pós-graduação em área de Tecnologia da Informação de, no mínimo, 360 (trezentos e sessenta) horas, fornecido por instituição reconhecida pelo Ministério da Educação (MEC);

3.4.5.2. Conhecimento em segurança da informação, com experiência comprovada de no mínimo 06 (meses) em gestão de vulnerabilidades;



Poder Judiciário

Conselho Nacional de Justiça

3.4.6. Não existe restrição ou limite para acúmulo de perfis em um mesmo profissional, uma vez que é de responsabilidade da CONTRATADA definir o quantitativo de profissionais envolvidos no GRUPO DE GESTÃO DE VULNERABILIDADES, porém conforme já fora mencionado no presente termo de referência, este(s) deve(m) compor único e exclusivamente o time denominado GRUPO DE GESTÃO DE VULNERABILIDADES.

3.4.7. Será exigido da CONTRATADA as seguintes documentações do(s) profissionais que participarão do GRUPO DE GESTÃO DE VULNERABILIDADES, os quais devem comprovar as exigências e obrigações descritas no presente termo de referência: carteira de trabalho devidamente assinada pela CONTRATADA, curriculum vitae para comprovação de habilidades, e as devidas certificações técnicas para comprovação do conhecimento.

3.5. Das entregas

3.5.1. Para acompanhamento e avaliação do serviço a ser ofertado pela CONTRATADA, a CONTRATANTE definiu os seguintes indicadores chave de desempenho, que reunidos vão compor um único relatório a ser entregue de forma online e em tempo de execução, através do portal segurança da CONTRATADA, a saber:

DENOMINAÇÃO	FORMA DE CÁLCULO	FILTRO	AGRUPADOR	DESCRIÇÃO
Quantitativo de vulnerabilidades	Soma de vulnerabilidades	Vulnerabilidades	Vulnerabilidades	Número total de vulnerabilidades
Quantitativo de vulnerabilidades críticas por área responsável	Soma de vulnerabilidades críticas por área responsável	Vulnerabilidades críticas	Vulnerabilidades	Número total de vulnerabilidades de críticas por área responsável
Quantitativo de vulnerabilidades corrigidas	Soma de vulnerabilidades corrigidas	Vulnerabilidades corrigidas	Vulnerabilidades	Número total de vulnerabilidades corrigidas
Quantitativo de vulnerabilidades em Aplicações WEB	Soma de vulnerabilidades em Aplicações WEB	Vulnerabilidades em Aplicações WEB	Vulnerabilidades	Número total de vulnerabilidades em Aplicações WEB
Quantitativo de vulnerabilidades corrigidas em Aplicações WEB	Soma de vulnerabilidades corrigidas em Aplicações WEB	Vulnerabilidades corrigidas em Aplicações WEB	Vulnerabilidades	Número total de vulnerabilidades corrigidas em Aplicações WEB



Poder Judiciário

Conselho Nacional de Justiça

Quantitativo de vulnerabilidades em ativos	Soma de vulnerabilidades em ativos	Vulnerabilidades em ativos	Vulnerabilidades	Número total de vulnerabilidades em ativos
Quantitativo de vulnerabilidades corrigidas em ativos	Soma de vulnerabilidades corrigidas em ativos	Vulnerabilidades corrigidas em ativos	Vulnerabilidades	Número total de vulnerabilidades corrigidas em ativos
Quantidade de vulnerabilidades em códigos de aplicações	Soma de vulnerabilidades em códigos de aplicações	Vulnerabilidades em códigos de aplicações	Vulnerabilidades	Número total de vulnerabilidades em códigos de aplicações
Quantitativo de certificados digitais expirados	Soma de certificados digitais expirados	Certificados digitais expirados	Certificados digitais	Número total de certificados digitais expirados
Quantitativo de certificados digitais a expirar em 3 meses	Soma de certificados digitais a expirar em 3 meses	Certificados digitais a expirar em 3 meses	Certificados digitais	Número total de certificados digitais a expirar em 3 meses
TOP 10 – Ativos mais vulneráveis	Soma de vulnerabilidades por ativo	Vulnerabilidades por ativo	Vulnerabilidades	TOP 10 do número de vulnerabilidades por ativo
TOP 10 – Aplicações WEB mais vulneráveis	Soma de vulnerabilidades em Aplicações WEB	Vulnerabilidades em Aplicações WEB	Vulnerabilidades	TOP 10 do número total de vulnerabilidades em Aplicações WEB
TOP 10 – Aplicações WEB mais vulneráveis em comparação com OWASP	Soma de vulnerabilidades em Aplicações WEB em comparação com OWASP	Vulnerabilidades em Aplicações WEB	Vulnerabilidades	TOP 10 do número total de vulnerabilidades em Aplicações WEB em comparação com OWASP
Quantitativo de ataque simulados	Soma de ataques executados	Número de ataques	BAS	Número total de ataque simulados
Quantitativo de ataques bem-sucedidos	Soma de ataques bem-sucedidos	Ataques efetivos	BAS	Número total de ataques que obtiveram êxito
Quantitativo de falhas exploráveis	Soma de falhas exploráveis	Vulnerabilidades exploráveis	BAS	Número total de falhas exploráveis identificadas
Quantitativo de controles validados	Soma de validações de controles	Controles de segurança	BAS	Número total de validações realizadas em controles de segurança



Poder Judiciário

Conselho Nacional de Justiça

TABELA 04 - INDICADORES ESTRATÉGICOS GESTÃO DE VULNERABILIDADE

3.5.2. Tais relatórios e indicadores devem ser apresentados e discutidos em reunião mensal, com presença de profissional que conheça todos os serviços. Nesse contexto, o profissional deve apresentá-lo de forma presencial nas dependências da CONTRATANTE em Brasília-DF ou de forma virtual, por meio de solução de videoconferência.

4. GRUPO 01 – Item 03: SERVIÇO DE GESTÃO DE INCIDENTES DE SEGURANÇA (CSIRT - BLUE TEAM)

4.1. Condições Gerais

4.1.1. Tem por objetivo analisar, documentar e indicar como conter e remediar os eventos de segurança da informação que foram transformados em um incidente de segurança da informação. Tal serviço deverá ser executado obedecendo aos frameworks NIST e SANS de resposta a incidente de segurança da informação e boas práticas de mercado.

4.1.2. Um incidente de segurança é definido como qualquer evento adverso, confirmado ou sob suspeita, relacionado à segurança de sistemas de informação da CONTRATANTE, levando a perda de um ou mais princípios básicos de Segurança da Informação: Confidencialidade, Integridade, Disponibilidade e Privacidade.

4.1.3. Apresentamos a seguir uma definição detalhada e escalonada das naturezas de “Incidentes” que serão escopo dos serviços prestados pela CONTRATADA:

Evento	Algo que ocorreu nos sistemas de informação, infraestrutura ou dados mas não necessariamente malicioso ou que requer uma ação.
Alerta	Algo potencialmente acionável. Uma indicação de um evento acionável.
Incidente	Qualquer evento com a violação da confidencialidade, integridade, disponibilidade e privacidade, mas sem impacto à missão ou ao negócio.
Incidente grave	Qualquer evento com a violação da confidencialidade, integridade, disponibilidade e privacidade, com impacto à missão ou ao negócio.



Poder Judiciário

Conselho Nacional de Justiça

Invasão e/ou Vazamento	Perda ou comprometimento de sistemas, dados regulados, propriedade empresarial que dispara uma ação ou resposta legal que vai além dos serviços de monitoramento e respostas a incidentes.
------------------------	--

TABELA 05 – DEFINIÇÃO DOS INCIDENTES

- 4.1.4.O serviço de resposta a incidentes será responsável por monitorar equipamentos e softwares componentes das soluções de segurança da CONTRATANTE, envolvendo identificação, classificação e análise de eventos que possam comprometer a disponibilidade, integridade, confidencialidade dos serviços e requerimentos legais de privacidade dos serviços.
- 4.1.5.A CONTRATADA deverá prover serviços de resposta aos incidentes de segurança da informação diante os eventos registrados no monitoramento.
- 4.1.6.Os serviços de monitoramento e resposta a incidentes de segurança poderão ser prestados REMOTAMENTE por meio de Centro de Operações de Segurança da Informação, sem prejuízo aos níveis de serviços solicitados nesse documento.
- 4.1.7.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).
- 4.1.8.A CONTRATADA deverá ser responsável por:
- 4.1.8.1. Prestar o serviço gestão de incidentes de segurança, envolvendo, no mínimo:
 - 4.1.8.1.1. Identificação da causa;
 - 4.1.8.1.2. Tratamento da causa;
 - 4.1.8.1.3. Aplicação/Orientação da correção;
 - 4.1.8.1.4. Validação do contorno do incidente;
 - 4.1.8.1.5. Encerramento do registro do incidente.
 - 4.1.8.2. Criar, em colaboração com a CONTRATANTE, casos de uso (regras) que devem ser implementados nas ferramentas disponíveis no serviço de Monitoramento e Visibilidade de Ataques, fornecendo, no mínimo:
 - 4.1.8.2.1. Lista de casos de uso candidatos;
 - 4.1.8.2.2. Categorização dos casos de uso em: orientados a ameaças, orientados a controles e orientado a ativos críticos do CNJ;
 - 4.1.8.2.3. Lista de casos de uso não operacionalizáveis;



Poder Judiciário

Conselho Nacional de Justiça

- 4.1.8.2.4. Lista de casos de uso implementados;
- 4.1.8.2.5. Lista de casos de uso removidos.
- 4.1.8.3. Revisar periodicamente os casos de uso, realizando as adaptações e evoluções necessárias;
- 4.1.8.4. Produzir e entregar informação de inteligência acionável, na forma de procedimentos para triagem de alertas e procedimentos para resposta a incidentes, correspondentes aos casos de uso.
- 4.1.8.5. Documentar e manter atualizado o processo de gestão de incidentes contendo, no mínimo, as fases de alerta, triagem, análise, tratamento, recuperação e lições aprendidas.
- 4.1.9. Os casos de grave incidente de segurança devem ser liderados por um Gerente de Crise, que deve possuir certificação CISSP (*Certified Information Systems Security Professional*) ou comprovada experiência no tratamento de incidentes de segurança de grande impacto técnico e institucional.
- 4.1.10. Durante os horários de prestação dos serviços de Gestão de Incidentes de Segurança não serão permitidas ações como “*SLA HOLD*” ou qualquer recurso similar que possa vir mascarar ou paralisar o real tempo de atendimento destas requisições.
- 4.1.11. O Serviço de Gestão de Incidentes de Segurança será responsável por monitorar e reagir a eventos e incidentes de SI em equipamentos, softwares e demais componentes do ambiente computacional do CONTRATANTE, envolvendo, mas não se limitando em: identificar, classificar, analisar e solucionar incidentes que possam comprometer os requisitos de segurança da informação definidos pelo CNJ.
- 4.1.12. Os canais de comunicação para tratamento dos incidentes devem ser as ferramentas de suporte definidas pelo CONTRATANTE, tais quais, telefone, ferramenta ITSM e e-mail, não se limitando a estas.

4.2. Processo de resposta a incidente de segurança da informação

- 4.2.1. O início do processo de resposta a incidente de segurança se dará, sempre que um evento adverso for submetido pelo SERVIÇO DE MONITORAMENTO E VISIBILIDADE DE ATAQUES CIBERNÉTICOS descrito no presente termo de referência, ou quando a ETIR-CNJ for notificada acerca de incidente de segurança por meio do endereço abuse@cnj.jus.br, sem prejuízo de outras formas de detecção ou comunicação. Poderá o corpo técnico de segurança do



Poder Judiciário

Conselho Nacional de Justiça

CONTRATANTE a qualquer tempo, abrir um incidente de segurança, seguindo as diretrizes descritas em 4.4.2 - Solicitações por meio da central de serviços:.

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

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

4.2.4. Como próximo passo o grupo de resposta a incidente de segurança (Blue Team) da CONTRATADA, deverá comunicar ao time de segurança da informação do CONTRATANTE, de acordo com os SLAs informados nesse documento, as informações iniciais sobre o incidente de segurança gerado, e quais serão as linhas de atuação para solução do incidente. Dados e Informações iniciais esperados da CONTRADADA:

Prioridade	Representação/número de prioridade ou severidade do incidente, em uma escala de 1 a 4 sendo 1 a maior prioridade.
Categoria/Classificação	Palavra única que classifica o tipo do incidente, como malware, phishing, misconfiguration entre outros.
Entidades fontes	Se aplicável, os detalhes dos nomes dos dispositivos, endereço de e-mails, endereços IPs, detalhes da vulnerabilidade ou outros fatores de identificação que apontam para a fonte do incidente.
Entidades de destino	Os detalhes de nomes dos dispositivos, endereços de e-mail, endereços IPs ou outros fatores de identificação que apontam para os ativos afetados.
Ações recomendadas	Instruções inteligentes e simples a serem seguidas que detalhem as ações de remediação já tomadas pela CONTRATADA e ações que a CONTRATANTE precisa tomar.



Poder Judiciário

Conselho Nacional de Justiça

Fontes da Detecção	Detalhes das fontes dos logs ou os dispositivos de segurança que identificaram (ou colaboraram) na descoberta do incidente. Essa informação será útil para análise de causa raiz ou remediação direcionada.
---------------------------	---

TABELA 06 – INFORMAÇÕES INICIAIS DOS INCIDENTES

- 4.2.5. Juntamente com o CONTRATANTE o grupo de resposta a incidente de segurança (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 encontra no tópico dos níveis mínimos de serviços.
- 4.2.6. Após análises iniciais do incidente, caberá ao grupo de resposta a incidente de segurança (Blue Team), realizar uma análise mais profunda do incidente baseando-se no comportamento do ataque e/ou artefato (malware).
- 4.2.7. Todo o processo de análise e os 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.
- 4.2.8. Uma vez identificado comportamento e os principais vetores de ataque, o grupo de resposta a incidente de segurança (Blue Team) da CONTRATADA, deverá definir 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, deverá antes ser autorizada tal alteração pelo corpo técnico de segurança do CONTRATANTE.
- 4.2.9. Mitigado o incidente de segurança, o próximo passo exigido é que a CONTRATADA, através do grupo de resposta a incidente de segurança (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.
- 4.2.10. Inicia-se então o processo de restauração dos serviços e soluções afetadas, ou seja, a RESPOSTA AO INCIDENTE. Todo esse processo é de responsabilidade da CONTRATADA, sendo realizado pelo Grupo de resposta a incidente de segurança (Blue Team).



Poder Judiciário

Conselho Nacional de Justiça

- 4.2.11. Entende-se como RESPOSTA AO INCIDENTE o restabelecimento do serviço impactado deixando-o operacional para utilização de maneira definitiva ou através de solução de contorno (workaround), sendo que esta sempre deverá ser autorizada pelo CONTRATANTE;
- 4.2.12. 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 (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. Somente após esta análise o incidente deve ser FECHADO.
- 4.2.13. Caso seja necessário, a reconstrução do ataque deve ser realizada pela CONTRATADA em ambiente controlado, usando-se por exemplo ambiente 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.
- 4.2.14. O grupo de resposta a incidente de segurança (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.
- 4.2.15. Caso a resposta ao incidente não seja efetiva (restabelecimento do serviço) o chamado deve ser reaberto com um nível de criticidade imediatamente superior ao do incidente original.
- 4.2.16. As ações técnicas adotadas em incidentes de criticidade EMERGENCIAL e ALTA deverão ser revalidadas pelo grupo de resposta a incidente de segurança (Blue Team) em até 18 (dezoito) horas após a RESPOSTA AO INCIDENTE, tal ação caberá a um analista diferente ao que implementou as ações inicialmente. Somente após isso os incidentes destas categorias poderão ser FECHADOS.
- 4.2.17. No caso da recorrência de um mesmo incidente de criticidade PROBLEMA, deverá ser aberto chamado pelo grupo de resposta a incidente de segurança (Blue Team) para que seja feita a devida investigação de sua causa raiz e demais tratativas necessárias à solução definitiva. Neste caso,



Poder Judiciário

Conselho Nacional de Justiça

sua criticidade\SLA será definido como imediatamente superior a dos incidentes que o originaram.

4.2.18. Quando solicitada, a CONTRATADA deverá realizar processos de auditoria e investigação forense, inspecionando logs e informações contidas no SERVIÇO DE MONITORAMENTO E VISIBILIDADE DE ATAQUES CIBERNÉTICOS com vistas a rastrear e identificar ações não autorizadas e/ou demais análises que se façam necessárias.

4.2.19. Espera-se que a linha de base dos eventos de segurança monitorados seja revista de forma mensal, contudo não se limitando a este tempo, pois todos os dias novos ataques são projetados, e se espera que a CONTRATADA tome ciência destes ataques e, por sua vez, atualize a linha de base para que em um cenário onde estes novos ataques sejam direcionados ao CONTRATANTE sejam detectados através dos serviços em questão.

4.2.20. O processo descrito é o mínimo esperado a ser seguido e executado pela CONTRATADA, todavia como o objeto do presente termo de referência se trata de um serviço continuado, logo se espera da CONTRATADA a apresentação da melhoria contínua deste, a qual pode ser alterado desde que aprovado pela CONTRATANTE.

4.3. Ferramentas

4.3.1. O Serviço de Gestão de Incidente de Segurança deverá ser prestado pela CONTRATADA com o apoio de ferramenta de ITSM para permitir a criação e acompanhamento de Incidentes de Segurança e gerir todo o ciclo de vida de um incidente de segurança.

4.3.2. A CONTRATADA deverá realizar a integração da ferramenta de SIEM descrita no GRUPO 01 – Item 04: SERVIÇO DE MONITORAMENTO E VISIBILIDADE DE ATAQUES CIBERNÉTICOS, para permitir o recebimento de alertas e abertura automática de incidentes na ferramenta de ITSM da CONTRATANTE e/ou CONTRATADA.

4.3.3. A CONTRATADA deverá utilizar ferramenta ou mecanismos de orquestração e automação do processo de resposta à incidentes, próprios ou integrados à solução já existente no ambiente da CONTRATANTE, visando a diminuição de erros operacionais e consistência de atendimento.



Poder Judiciário

Conselho Nacional de Justiça

4.3.4. Alinhado a uma gestão eficiente do processo de resposta a incidentes, a CONTRATADA deve possuir ou ser capaz de integrar-se a uma solução de orquestração e automação de resposta a incidentes com o intuito de simplificar processos complexos, acelerar fluxos, reduzir a carga de trabalho e tornar a operação de Segurança Cibernética mais eficiente.

4.3.5. O SOAR deve ajudar a transformar tarefas manuais do time de segurança cibernética em um processo automatizado e eficiente otimizando várias etapas no fluxo de tratamento e respostas. Através de processos bem elaborados, enriquecimento de contexto e outros recursos de investigação, o SOAR deve ser capaz de ajudar as equipes de resposta a incidentes a qualificar, colaborar e gerenciar incidentes mais rapidamente.

4.4. Grupo de respostas a incidentes de segurança (Blue Team)

4.4.1. Este grupo deverá ser exclusivo para trabalhar com respostas a incidentes, não podem os profissionais pertencentes a este grupo serem compartilhados e/ou atuarem, com os demais serviços descritos no objeto do presente termo de referência.

4.4.2. Todos os profissionais que integram o GRUPO DE RESPOSTA A INCIDENTE DE SEGURANÇAS (Blue Team), devem obrigatoriamente compor o quadro de colaboradores da CONTRATADA em regime de trabalho CLT (Consolidação das Leis do Trabalho), não havendo possibilidade a terceirização ou subcontratação de tal serviço.

4.4.3. Deverá ser de responsabilidade da CONTRATADA dimensionar o número de profissionais adequado para entrega de tal serviço, sem que haja impacto no acordo de nível de serviço, ou em custos para a CONTRATANTE.

4.4.4. A fim de garantir que os profissionais envolvidos têm conhecimento e habilidade para executar o processo de resposta a incidente de segurança da CONTRATANTE, a CONTRATADA obrigatoriamente deverá compor o GRUPO DE RESPOSTA A INCIDENTE DE SEGURANÇA (Blue Team), com ao menos 1 (um) perfil de cada que segue descrito abaixo. O profissional deverá possuir, no mínimo, 01 (uma) certificação dentre as indicadas para o respectivo perfil, admitidas certificações equivalentes reconhecidas pelo mercado e compatíveis com as atribuições descritas:

Perfis	Certificações	Atribuições técnicas
Analista de Segurança 1	<ul style="list-style-type: none">• CompTIA Security+• Blue Team Level 1 (BTL1)	<ul style="list-style-type: none">• Detecção e resposta a incidentes



Poder Judiciário

Conselho Nacional de Justiça

	<ul style="list-style-type: none">• (ISC)² SSCP• Certificação equivalente de fundamentos em segurança da informação	<ul style="list-style-type: none">• Monitoramento e análise de eventos• Triagem de incidentes• Procedimentos operacionais (IR)
Analista de Segurança 2	<ul style="list-style-type: none">• CompTIA Cybersecurity Analyst (CySA+)• Blue Team Level 2 (BTL2)• GIAC GCIH – Incident Handler• Microsoft SC-200 – Security Operations Analyst• AWS Certified Security – Specialty• Microsoft AZ-500 – Azure Security Engineer• (ISC)² CCSP.	<ul style="list-style-type: none">• Tratamento de incidentes• Análise de logs• Contenção e erradicação• Recuperação• Gestão de crise• Lições aprendidas
Analista de Segurança 3	<ul style="list-style-type: none">• GCFE – GIAC Certified Forensic Examiner• GCFA – GIAC Certified Forensic Analyst• Certificação equivalente em forense digital com conteúdo programático compatível.	<ul style="list-style-type: none">• Análise pós-incidente• Preservação de evidências

TABELA 07 – CERTIFICAÇÕES GRUPO DE RESPOSTA A INCIDENTE DE SEGURANÇA

4.4.5. Durante a execução do contrato, a CONTRATADA se obriga a manter todos os profissionais com os requisitos abaixo:

4.4.5.1. Diploma, devidamente registrado, de curso de nível superior de graduação na área de Tecnologia da Informação ou de graduação em qualquer curso superior, acrescido de certificado de curso de pós-graduação em área de Tecnologia da Informação de, no mínimo, 360 (trezentos e sessenta) horas, fornecido por instituição reconhecida pelo Ministério da Educação (MEC);

4.4.5.2. Conhecimento avançado em segurança da informação, com experiência comprovada de no mínimo 06 (meses) em resposta a incidente de segurança de informação.

4.4.6. Não existe restrição ou limite para acúmulo de perfis em um mesmo profissional, uma vez que é de responsabilidade da CONTRATADA definir o quantitativo de profissionais envolvidos no GRUPO DE RESPOSTA A



Poder Judiciário

Conselho Nacional de Justiça

INCIDENTE DE SEGURANÇA, porém conforme já fora mencionado, este(s) deve(m) compor única e exclusivamente o time denominado GRUPO DE RESPOSTA A INCIDENTE DE SEGURANÇA (Blue Team).

4.4.7. Será exigido da CONTRATADA, as seguintes documentações do(s) profissionais que participarão do GRUPO DE RESPOSTA A INCIDENTE DE SEGURANÇA (Blue Team), os quais devem comprovar as exigências e obrigações: carteira de trabalho devidamente assinada pela CONTRATADA, curriculum vitae para comprovação de habilidades, e as devidas certificações técnicas para comprovação do conhecimento.

4.5. Das Entregas

4.5.1. Para acompanhamento e avaliação do serviço a ser ofertado pela CONTRATADA, a CONTRATANTE definiu os seguintes indicadores chave de desempenho, que reunidos vão compor um único relatório a ser entregue de forma online e em tempo de execução, através do portal segurança da CONTRATADA, a saber:

DENOMINAÇÃO	FORMA DE CÁLCULO	FILTRO	AGRUPADOR	DESCRIÇÃO
Quantitativo de incidentes abertos	Soma de incidentes abertos	Incidentes abertos	Incidentes	Número total de incidentes abertos
Incidentes por tipo	Total de incidentes categorizado por tipo	Categoria do incidente	Incidentes	Total de incidentes categorizado por tipo: malware, vaz. de info., acesso não aut., etc.
Incidentes por severidade	Total de incidentes categorizado por severidade	Categoria do incidente	Incidentes	Total de incidentes categorizado por severidade: emerg., alta, média e baixa.
Ativos comprometidos	Total de ativos comprometidos categorizado por tipo: servidores, estações, disp. móveis, etc.	Incidentes abertos	Tipo de ativo	Total de ativos comprometidos categorizado por tipo: servidores, estações, disp. móveis, etc.
Investigações forenses	Total de investigações abertas e concluídas	Investigações abertas	Status da investigação	Total de investigações forenses em andamento e concluídas
Quantitativo de incidentes que resultaram em	Soma de incidentes abertos que resultaram em	Incidentes com comprometimento	Incidentes com comprometimento	Número total de incidentes com comprometimento



Poder Judiciário

Conselho Nacional de Justiça

comprometimento da segurança	comprometimento da segurança			
TOP 10 – IP de destino de incidentes de segurança	Soma do número de incidentes por IP de destino	Incidentes abertos/tratados por IP de destino	IP de destino	TOP do número de incidentes por IP de destino
TOP 10 – Incidentes de segurança por origem	Soma do número de incidentes por origem	Incidentes abertos/tratados por origem	Origem	TOP do número de incidentes por origem interna ou externa
TOP 10 – Tipos de Incidentes	Soma do número de incidentes por tipo	Incidentes abertos/tratados por tipo	Tipo	TOP 10 por tipo de incidente

TABELA 08 - INDICADORES ESTRATÉGICOS DE GESTÃO DE INCIDENTES DE SEGURANÇA

4.5.2. Tais relatórios e indicadores devem ser apresentados e discutidos em reunião mensal, com presença de profissional que conheça todos os serviços. Nesse contexto, o profissional deve apresentá-lo de forma presencial nas dependências da CONTRATANTE em Brasília-DF ou de forma virtual, por meio de solução de videoconferência.

5. GRUPO 01 – Item 04: SERVIÇO DE MONITORAMENTO E VISIBILIDADE DE ATAQUES CIBERNÉTICOS

5.1. Condições gerais

5.1.1. Visa o monitoramento contínuo e ininterrupto de ataques cibernéticos direcionados ao CNJ, através de correlacionamento de logs, pacotes de redes, e/ou comportamento anômalo de aplicações, serviços, usuários e infraestrutura, sejam locais (on-premises) e nuvem, 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.

5.1.2. Além do monitoramento da solução de SIEM, a CONTRATADA deverá realizar o monitoramento de log e eventos de segurança das soluções de UTM, WAF (Web Application Firewall), endpoint EDR, CNAPP e proteção de gateway de e-mail constantes no ANEXO B – PLATAFORMA DE SEGURANÇA e outras soluções que vierem a integrar o ambiente de segurança da CONTRATANTE.



Poder Judiciário

Conselho Nacional de Justiça

- 5.1.3. Para execução do serviço, a CONTRATADA será responsável pela integração, por meio da coleta de logs/eventos, da solução de SIEM com as demais soluções de segurança instaladas no ambiente da CONTRATANTE.
- 5.1.4. A CONTRATADA deve prever capacidade técnica e operacional para análise de dados em volumes de até 10 Gigabits por segundo e 50 milhões de eventos (logs e flows) por hora.
- 5.1.5. Principais atividades a serem executadas de forma contínua pela CONTRATADA:
- 5.1.5.1. Monitorar os eventos recebidos pelo sistema de correlação de eventos de segurança da informação;
 - 5.1.5.2. Investigar os eventos recebidos para determinar se eles geraram incidentes de segurança da informação;
 - 5.1.5.3. Classificar e tratar os incidentes identificados de acordo com os roteiros de operação;
 - 5.1.5.4. Analisar as causas e os impactos dos incidentes tratados e propor controles para evitar novos incidentes similares;
 - 5.1.5.5. Ser responsável pela gestão e documentação dos casos de uso configurados na ferramenta de monitoração e detecção;
 - 5.1.5.6. Criar casos de uso configurando regras, limiares e alertas de acordo com as especificações fornecidas pelo CNJ;
 - 5.1.5.7. Criar casos de uso configurando regras, limiares e alertas de acordo com as especificações desenvolvidas por equipe especializada da CONTRATADA com base em ameaças identificadas em outros clientes;
 - 5.1.5.8. Aperfeiçoar as regras, limiares e alertas do sistema de correlação de eventos de segurança da informação, visando reduzir o número de falsos positivos e falsos negativos;
 - 5.1.5.9. Apoiar a construção e melhoria de roteiros para tratamento de incidentes similares para formar uma base de conhecimento do CNJ;
 - 5.1.5.10. Operação, administração, configuração e documentação das ferramentas fornecidas, inclusive suas integrações;
 - 5.1.5.11. Apoio na manutenção preventiva, corretiva e atualizações das ferramentas fornecidas.



Poder Judiciário

Conselho Nacional de Justiça

5.2. Ferramentas

5.2.1. Solução de SIEM

- 5.2.1.1. Para execução deste serviço a CONTRATADA deverá utilizar e ser capaz de operar, sustentar e suportar a solução Microsoft Sentinel com função de SIEM (*Security Information and Event Management*) e recursos de SOAR (Orquestração, Automação e Resposta de Segurança).
- 5.2.1.2. Apesar de tal solução ser de propriedade do CNJ, e não pertencer a este termo de referência a aquisição e/ou renovação de tal solução, será de responsabilidade da CONTRATADA operar, sustentar, suportar e apresentar melhorias contínuas de tal ferramenta durante todo o período de vigência do contrato.
- 5.2.1.3. Ressalta-se que apesar de estar definido a utilização da ferramenta Microsoft Sentinel para execução e entrega de tal serviço, a CONTRATADA deverá complementar, se for necessário para garantir o cumprimento dos acordos de níveis de serviços estabelecidos no ANEXO C – NÍVEIS MÍNIMOS DE SERVIÇO, com ferramentas de sua propriedade sem incorrer em custos adicionais para a CONTRATANTE, as quais para serem habilitadas e/ou utilizadas, precisam de avaliação e autorização previa da equipe técnica do CNJ.
- 5.2.1.4. Ressalta-se ainda que sobre nenhuma hipótese, a ferramenta Microsoft Sentinel poderá ser substituída pela CONTRATADA, apenas poderá ser complementada seguindo os processos de homologação e aprovação estabelecidos neste parágrafo.

5.2.2. Monitoramento em Deep e Dark Web

- 5.2.2.1. A CONTRATADA deverá fornecer, operar e suportar solução de segurança para buscas na Superfície, Deep e Dark Web com dados fornecidos pela CONTRATANTE, com as seguintes características:
 - 5.2.2.1.1. Possuir interface web (HTTPS) intuitiva.
 - 5.2.2.1.2. Possuir tecnologia baseada em natural language processing (NLP) e machine-learning para otimizar as pesquisas;



Poder Judiciário

Conselho Nacional de Justiça

- 5.2.2.1.3. Deve gerar alertas em tempo real de dados de domínios da CONTRATANTE;
- 5.2.2.1.4. Deve permitir buscas em sites da rede Tor, em fóruns restritos, em grupos de Telegram, em redes sociais abertas e em sites de vazamentos (paste sites, ex.: Pastebin, Reddit);
- 5.2.2.1.5. Deve permitir a criação e geração de alertas sobre possíveis vazamentos de dados da CONTRATANTE em Deep, Dark e Surface Web. Isso inclui vazamentos em mídias sociais, sites de compra e venda de dados vazados, fóruns criminosos, grupos de Telegram, etc.
- 5.2.2.1.6. Deve possibilitar a descoberta de novos exploits e códigos maliciosos relevantes referentes às tecnologias implementadas no ambiente da CONTRATANTE;
- 5.2.2.1.7. Deve permitir consultas com palavras-chave relacionadas à CONTRATANTE;
- 5.2.2.1.8. Deve prever a monitoração de reputação do CNJ como um todo, considerando todos seus ativos e usuários internos.
- 5.2.2.1.9. A solução deve realizar o monitoramento contínuo de fontes externas nacionais e internacionais, como Fóruns, Redes Sociais, Mídias Sociais, Nuvens Públicas e Grupos Hackers para identificação de motivações, intenções e atividades de possíveis adversários que possam causar impactos à CONTRATANTE, seja na INTERNET profunda (Deep Web), escura (Dark Web) ou de superfície (Surface Web).
- 5.2.2.1.10. Diretamente a partir de um incidente aberto pela ferramenta deve ser possível solicitar o serviço de remoção de conteúdo infrator (TAKEDOWN).

5.2.3. Monitoramento e Detecção de Incidentes de Rede (NDR)

- 5.2.3.1. A CONTRATADA deverá fornecer, operar e suportar solução de monitoramento e detecção de incidentes de rede (NDR), com capacidade de ampliar a visibilidade sobre o ambiente do CONTRATANTE, apoiar o



Poder Judiciário

Conselho Nacional de Justiça

correlacionamento com a solução de SIEM existente e fortalecer o processo de resposta a incidentes.

- 5.2.3.2. A solução deverá detectar automaticamente ameaças ativas em tempo real, inclusive aquelas que tenham burlado controles tradicionais de segurança.
- 5.2.3.3. A solução deverá permitir análise retrospectiva contínua mediante aplicação de novos Indicadores de Comprometimento (IoCs) sobre dados históricos armazenados.
- 5.2.3.4. A solução deverá realizar correlação avançada de metadados de rede utilizando técnicas de análise comportamental, aprendizado de máquina e inteligência artificial.
- 5.2.3.5. A solução deverá classificar os comprometimentos detectados por tipo (ex.: malware, comando e controle – C2, phishing, exploração, entre outros).
- 5.2.3.6. A solução deverá identificar o primeiro ativo impactado em cada incidente detectado, quando tecnicamente possível.
- 5.2.3.7. A solução deverá armazenar metadados e registros históricos de rede por período mínimo de 24 (vinte e quatro) meses, sem necessidade de contratação adicional de módulos essenciais, mantendo capacidade plena de consulta e aplicação de novos IoCs durante todo o período de retenção.
- 5.2.3.8. A solução deverá coletar continuamente metadados de rede de forma agnóstica a fabricante, incluindo, no mínimo:
 - 5.2.3.8.1. DNS
 - 5.2.3.8.2. Firewall
 - 5.2.3.8.3. Proxy
 - 5.2.3.8.4. VPN
 - 5.2.3.8.5. NetFlow ou equivalente
- 5.2.3.9. A coleta deverá ser baseada exclusivamente em metadados, sem necessidade obrigatória de captura integral de pacotes (PCAP).
- 5.2.3.10. A solução deverá permitir coleta por meio de:



Poder Judiciário

Conselho Nacional de Justiça

- 5.2.3.10.1. Integrações via API
- 5.2.3.10.2. Coletor passivo
- 5.2.3.10.3. Agentes, quando necessário
- 5.2.3.11. A solução deverá permitir ingestão de metadados provenientes de ambientes locais (on-premises), remotos e em nuvem pública, privada ou híbrida.
- 5.2.3.12. A solução deverá operar sob o conceito de Avaliação Contínua de Comprometimento, mantendo visão abrangente de toda a rede.
- 5.2.3.13. A solução deverá analisar em tempo real o estado de comprometimento dos ativos de TI.
- 5.2.3.14. A solução deverá integrar inteligência de ameaças proveniente de múltiplas fontes públicas, privadas ou proprietárias.
- 5.2.3.15. A solução deverá permitir a inclusão de fontes adicionais de inteligência (modelo Bring Your Own Threat Intelligence – BYOTI).
- 5.2.3.16. A solução deverá disponibilizar os IoCs relacionados aos incidentes detectados, incluindo domínios, URLs, hashes e endereços IP.
- 5.2.3.17. A solução deverá permitir exportação de informações de ameaças em formato aberto e interoperável (ex.: STIX ou equivalente).
- 5.2.3.18. A solução deverá permitir o gerenciamento completo do ciclo de vida do incidente dentro da própria plataforma.
- 5.2.3.19. A solução deverá permitir envio de notificações configuráveis por e-mail ou outro meio eletrônico.
- 5.2.3.20. A solução deverá permitir configuração da periodicidade de alertas e relatórios.
- 5.2.3.21. A solução deverá permitir integração com ferramentas de SIEM, SOAR e demais soluções de segurança, por meio de APIs abertas, documentadas e oficialmente suportadas pelo fabricante.
- 5.2.3.22. A solução deverá permitir automação de respostas e bloqueios por meio da infraestrutura de segurança já existente.



Poder Judiciário

Conselho Nacional de Justiça

- 5.2.3.23. A solução deverá prover visibilidade da superfície externa de ataque, identificando ativos expostos à internet.
- 5.2.3.24. A solução deverá identificar ativos externos não catalogados.
- 5.2.3.25. A solução deverá identificar exposição de credenciais e possíveis vazamentos associados à organização.
- 5.2.3.26. A solução deverá disponibilizar portal web seguro para acesso administrativo e operacional.
- 5.2.3.27. O portal deverá permitir visualização de estatísticas, filtros por período e exportação de dados.
- 5.2.3.28. A solução deverá permitir a criação de perfis de acesso com níveis distintos de permissão.
- 5.2.3.29. A solução deverá disponibilizar relatórios periódicos configuráveis.
- 5.2.3.30. A solução deverá permitir supervisão dos coletores implantados, incluindo status operacional e volume de dados coletados.
- 5.2.3.31. A solução deverá permitir monitoramento dos agentes implantados, incluindo informações de versão e sistema operacional.

5.3. Processo de monitoramento e visibilidade de ataques cibernéticos

- 5.3.1. A CONTRATADA fica responsável pela solução Microsoft Sentinel já adquirida pela CONTRATANTE, incluindo:
 - 5.3.1.1. Operação, administração, sustentação e apresentação de melhoria contínua de tal ferramenta durante todo o período de vigência do contrato;
 - 5.3.1.2. Criação de regras específicas para identificação de ataques na rede;
 - 5.3.1.3. Criação de parsers para comunicação entre ferramentas;
 - 5.3.1.4. Criação de dashboards para geração de relatórios customizados;
 - 5.3.1.5. Abertura de chamados junto ao fabricante/fornecedor da solução.
- 5.3.2. A CONTRATADA também ficará responsável pela operação, sustentação e suporte da ferramenta fornecida pela CONTRATADA de monitoramento em



Poder Judiciário

Conselho Nacional de Justiça

Deep e Dark Web e de Monitoramento e Detecção de Incidentes de Rede (NDR).

- 5.3.3. É sabido que para o sucesso de um monitoramento de ataques cibernéticos, a primeira definição se deve a que tipo de ocorrência de eventos de segurança, se deseja detectar e tomar algum tipo de ação, logo será de responsabilidade da CONTRATADA como primeiro passo deste processo, a definição de linha de base de eventos monitorados.
- 5.3.4. Tal definição de linha de base de eventos de segurança monitorados não deve ser tomada de forma unilateral pela CONTRATADA, a CONTRATANTE deverá participar ativamente no processo de construção de forma consultiva, porém, se ratifica que é de responsabilidade da CONTRATADA a definição e colocar em operação tal linha de base.
- 5.3.5. Espera-se que a linha de base de eventos de segurança monitorados, seja revista de forma mensal, contudo não se limitando a este tempo, pois todos os dias novos ataques são projetados no mundo, e se espera que a CONTRATADA tome ciência destes ataques e, por sua vez, atualize a linha de base, para que em um cenário onde estes novos ataques sejam direcionados à CONTRATADA, sejam detectados através dos serviços em questão.
- 5.3.6. O produto de um evento é a correlação dos insumos: logs e pacotes de rede, gerados pelos itens de configurações do parque da CONTRATANTE. Uma vez definida a linha de base de eventos, será também de responsabilidade da CONTRATADA avaliar se todos os insumos para a correta geração do evento, estão sendo enviados corretamente para a ferramenta da CONTRATANTE.
- 5.3.7. Caso a CONTRATADA identifique a ausência dos insumos (logs e pacotes de rede) a ser gerado por um item de configuração, será de responsabilidade da CONTRATADA a correção e/ou habilitação de tal insumo dos itens de configuração. Caso o item de configuração não pertença ao objeto contratado, porém necessário para a correta geração do evento, deverá a CONTRATADA solicitar à CONTRATANTE a correção e/ou habilitação de tal insumo no item de configuração em questão.
- 5.3.8. Dar-se-á então o passo de classificação do evento, também de responsabilidade da CONTRATADA. O grupo de monitoramento de ataques da CONTRATADA deve focar as ações nos eventos que são significativos, logo tal grupo deve analisar todos os eventos apresentados, classificando-os nos seguintes grupos, a saber:



Poder Judiciário

Conselho Nacional de Justiça

5.3.8.1. **Eventos de Informação:** Estes eventos não requerem qualquer ação. São usados para fazer verificação de funcionalidade dos itens de configuração de segurança. Ou seja, tem por objetivo puro e simples, identificar se as ferramentas e soluções, estão funcionando dentro do esperado. Estes eventos são também úteis para gerar estatísticas como por exemplo, porcentagem de hosts com a última vacina de antivírus do dia.

5.3.8.2. **Eventos de Aviso:** Este grupo de eventos deve ser utilizado, quando existe algum comportamento anômalo se comparado a linha de base de operação padrão do ambiente (serviço, tráfego e/ou solução), porém ainda não gerou algum tipo de impacto ao ambiente (serviço, tráfego e/ou solução) da CONTRATANTE, como por exemplo fictício: É esperado que exista 1000 (mil) ataques do tipo *port scan* bloqueados pelo firewall, porém na última hora este número passou para 10000 (dez mil) ataques, todavia o firewall ainda continua bloqueando sem que haja degradação da performance do ambiente (serviço, tráfego e/ou solução).

5.3.8.3. **Eventos de Exceção:** Estes eventos são aqueles que sugere que os pilares de segurança da informação (confidencialidade, integridade, disponibilidade e requerimentos legais de privacidade) foram impactados, como por exemplo: Uma infecção gerada por um malware do tipo *ransomware*, onde a mesma não tenha sido bloqueada pela solução de antivírus da CONTRATANTE. Este é o único tipo de evento que pode iniciar o processo de resposta a incidente de segurança descrito no tópico **PROCESSO DE RESPOSTA A INCIDENTE DE SEGURANÇA DA INFORMAÇÃO** do presente termo de referência.

5.3.9. Uma vez classificado o evento se inicia o passo de resposta ao mesmo, que também é de responsabilidade da CONTRATADA. As respostas são baseadas nos grupos de classificação de eventos, a saber:

5.3.9.1. Para eventos do tipo Informação, não é requerido qualquer tipo de ação, porém como já mencionado no presente termo de referência, tais eventos são utilizados para verificação do perfeito funcionamento das soluções de segurança, portanto se espera que a CONTRATADA os utilize para tal.

5.3.9.2. Para eventos do tipo Aviso, deve existir a garantia por parte da CONTRATADA, que uma interface humana, ou seja, uma analista que pertence ao grupo de monitoramento de ataques, esteja validando se tal evento pode se transformar em um evento do tipo exceção, e obviamente



Poder Judiciário

Conselho Nacional de Justiça

tomando as ações cabíveis para identificar a causar raiz da mudança de comportamento do ambiente.

5.3.9.3. Para eventos do tipo Exceção, deverá a CONTRATADA transformar tal evento em um incidente de segurança, realizando, portanto, a abertura do mesmo na ferramenta de incidente de segurança da informação da CONTRATANTE, definida no **PROCESSO DE RESPOSTA A INCIDENTE DE SEGURANÇA DA INFORMAÇÃO**. Após a abertura do incidente de segurança obedecendo os critérios estabelecidos para tal, se encerra a participação do grupo de monitoramento de ataques.

5.3.10. Como último passo do processo, a CONTRATADA deve encerrar os eventos após as devidas ações tomadas, conforme definido no parágrafo acima. Eventos podem ter apenas dois tipos de status “aberto” ou “encerrado”, ou seja, após o correto tratamento o evento deverá ter seu status alterado na ferramenta de “aberto” para “encerrado”.

5.3.11. Importante ressaltar que todo processo de tratamento do evento, independente de qual fase e/ou status, deve ser registrado no módulo de tratamento de eventos da ferramenta da CONTRATADA. Também é responsabilidade da CONTRATADA a segurança dos eventos e fica expressamente proibida a remoção de qualquer evento, independentemente de sua classificação e fase de tratamento.

5.3.12. O processo descrito é o mínimo esperado a ser seguido e executado pela CONTRATADA, todavia como o objeto do presente termo de referência se trata de um serviço continuado, logo se espera da CONTRATADA a apresentação da melhoria contínua deste, a qual pode ser alterado desde que aprovado pela CONTRATANTE.

5.4. Grupo de monitoramento de ataques cibernéticos

5.4.1. Todos os profissionais que integram GRUPO DE MONITORAMENTO DE ATAQUES, devem obrigatoriamente compor o quadro de colaboradores da CONTRATADA em regime de trabalho CLT (Consolidação das Leis do Trabalho), não havendo possibilidade a terceirização ou subcontratação de tal serviço.

5.4.2. Deverá ser de responsabilidade da CONTRATADA dimensionar o número de profissionais adequado para entrega de tal serviço, sem que haja impacto no acordo de nível de serviço estabelecido.



Poder Judiciário

Conselho Nacional de Justiça

5.4.3.A fim de garantir que os profissionais envolvidos têm conhecimento e habilidade, para executar o processo monitoramento de ataques cibernéticos da CONTRATANTE, a CONTRATADA obrigatoriamente deverá compor o GRUPO DE MONITORAMENTO DE ATAQUES, com ao menos 1 (um) perfil de cada que segue descrito abaixo. O profissional deverá possuir, no mínimo, 01 (uma) certificação dentre as indicadas para o respectivo perfil, admitidas certificações equivalentes reconhecidas pelo mercado e compatíveis com as atribuições descritas

. Perfis	Certificações	Atribuições técnicas
Analista de Segurança N1	<ul style="list-style-type: none">• CompTIA Security+• Blue Team Level 1 (BTL1)• Certificação equivalente de fundamentos em Segurança da Informação	<ul style="list-style-type: none">• Gestão das plataformas de monitoramento• Classificação de severidade• Escalonamento para N2• Execução de playbooks operacionais
Analista de Segurança N2	<ul style="list-style-type: none">• CompTIA Cybersecurity Analyst (CySA+)• Blue Team Level 2 (BTL2)• SC- 200 – Microsoft Certified: Security Operations Analyst Associate• AZ-500 – Azure Security Engineer• Certificação equivalente em análise e resposta a incidentes	<ul style="list-style-type: none">• Investigação aprofundada de alertas• Correlação avançada de logs• Ajuste e criação de regras no SIEM• Hardening e tuning de detecções• Ações de contenção técnica• Apoio à resposta a incidentes

TABELA 09 – CERTIFICAÇÕES GRUPO DE MONITORAMENTO DE ATAQUES

5.4.4. Para a adequada operação, administração e evolução da solução de SIEM Microsoft Sentinel, ao menos 1 (um) dos profissionais do grupo deverá possuir certificação específica na plataforma Microsoft Sentinel ou experiência comprovada mínima de 2 (dois) anos na sua operação.

5.4.5. Durante a execução do contrato, a CONTRATADA se obriga a manter todos os profissionais com os requisitos abaixo:

5.4.5.1. Diploma, devidamente registrado, de curso de nível superior de graduação na área de Tecnologia da Informação ou de graduação em qualquer curso superior, acrescido de certificado de curso de pós-graduação em área de Tecnologia da Informação de, no mínimo, 360 (trezentos e sessenta) horas, fornecido por instituição reconhecida pelo Ministério da Educação (MEC);



Poder Judiciário

Conselho Nacional de Justiça

5.4.5.2. Conhecimento avançado em segurança da informação, com experiência comprovada de no mínimo 06 (meses) em monitoramento de ataques cibernéticos utilizando ferramentas e soluções de SIEM e ATD (Advanced Threat Detection).

5.4.6. Não existe restrição ou limite para acúmulo de perfis em um mesmo profissional, uma vez que é de responsabilidade da CONTRATADA definir o quantitativo de profissionais envolvidos no GRUPO DE MONITORAMENTO DE ATAQUES, porém conforme já fora mencionado no presente termo de referência, este(s) deve(m) compor único e exclusivamente o time denominado GRUPO DE MONITORAMENTO DE ATAQUES.

5.4.7. Será exigido da CONTRATADA, as seguintes documentações do(s) profissionais que participarão do GRUPO DE MONITORAMENTO DE ATAQUES, os quais devem comprovar as exigências e obrigações descritas aqui descritas: carteira de trabalho devidamente assinada pela CONTRATADA, curriculum vitae para comprovação de habilidades, e as devidas certificações técnicas para comprovação do conhecimento.

5.5. Das entregas acerca de monitoramento e visibilidade de ataques cibernéticos

5.5.1. Para acompanhamento e avaliação do serviço a ser ofertado pela CONTRATADA, a CONTRATANTE definiu os seguintes indicadores chave de desempenho, que reunidos vão compor um único relatório a ser entregue de forma online e em tempo de execução, através do portal de segurança da CONTRATADA, a saber:

DENOMINAÇÃO	FORMA DE CÁLCULO	FILTRO	AGRUPADOR	DESCRIÇÃO
Quantitativo de eventos correlacionados	Soma de eventos correlacionados	Eventos correlacionados	Eventos correlacionados	Número total de eventos correlacionados
Quantitativo de pacotes correlacionados	Soma de pacotes correlacionados	pacotes correlacionados	pacotes correlacionados	Número total de pacotes correlacionados
Relação de alertas	Total de eventos dividido pelos alertas	Tipo de evento: malware, acesso não autorizado, etc.	Alertas	Relação entre o número de eventos analisados e alertas



Poder Judiciário

Conselho Nacional de Justiça

Falso positivo	Total de alertas dividido pelo total de falso positivos	Alertas	Alertas	Percentual de alertas que são falsos positivos
Quantitativo de incidentes abertos	Soma de incidentes abertos	Incidentes abertos	Incidentes abertos	Número total de incidentes abertos
Quantitativo de regras de correlacionamento	Soma do número de regras de correlacionamento	Regras de correlacionamento	Regras de correlacionamento	Número total de regras de correlacionamento
TOP 10 – Regras de correlacionamento	Soma do número de eventos/pacotes correlacionados por regra de correlacionamento	Eventos e pacotes correlacionados	Regra de correlacionamento	TOP 10 do número de eventos correlacionados por regra de correlacionamento
TOP 10 – IP de destino de regras de correlacionamento	Soma do número de eventos correlacionados por IP de destino	Eventos e pacotes correlacionados por IP de destino	IP de destino	TOP do número de eventos correlacionados por IP de destino
TOP 10 – Regras de correlacionamento por país de origem	Soma do número de eventos correlacionados por país de origem	Eventos e pacotes correlacionados por país de origem	País de origem	TOP do número de eventos correlacionados por país de origem
TOP 10 – Tipos de ataques	Soma do número de ataques correlacionados por tipo de ataque	Eventos e pacotes correlacionados por ataque	Ataques	TOP 10 por tipo de ataque
Quantitativo de takedown realizados	Soma de takedown realizados	Takedown solicitado	Takedown	Número total de Takedown realizados

Tabela 10 – INDICADORES ESTRATÉGICOS DE MONITORAMENTO DE ATAQUES CIBERNÉTICOS

5.5.2. Tais relatórios e indicadores devem ser apresentados e discutidos em reunião mensal, com presença de profissional que conheça todos os serviços. Nesse contexto, o profissional deve apresentá-lo de forma presencial nas dependências da CONTRATANTE em Brasília-DF ou de forma virtual, por meio de solução de videoconferência.

6. GRUPO 01 – Item 05: SERVIÇO DE CONSCIENTIZAÇÃO EM SEGURANÇA DA INFORMAÇÃO

6.1. Condições Gerais

6.1.1. Tem por objetivo promover, manter e evoluir continuamente a cultura de segurança da informação no âmbito da organização, por meio da realização de



Poder Judiciário

Conselho Nacional de Justiça

ações educativas voltadas às boas práticas de proteção de dados, uso seguro de sistemas e prevenção de incidentes cibernéticos.

- 6.1.2. O serviço contempla a identificação proativa de usuários com maior exposição a riscos ou potencial para atuarem como vetores de ataques, bem como o desenvolvimento, a aplicação e o acompanhamento de campanhas, palestras, treinamentos e materiais informativos, com foco na mitigação de riscos humanos e no fortalecimento do comportamento seguro, em conformidade com as políticas internas, normas técnicas e a legislação vigente.
- 6.1.3. O serviço será prestado de forma gerenciada, contínua e sistemática, com planejamento anual e revisões periódicas, considerando o perfil dos usuários, os riscos identificados e o nível de maturidade em segurança da informação da organização.
- 6.1.4. O serviço deverá contemplar todos os perfis de usuários da organização, incluindo magistrados, servidores, colaboradores, estagiários, terceirizados e demais públicos que utilizem ou tenham acesso a ativos de informação.
- 6.1.5. Para execução das campanhas de simulação de phishing e ações de conscientização, deverá ser considerado o quantitativo estimado de até 1500 (mil e quinhentas) contas de correio eletrônico corporativo ativas e elegíveis para participação nas campanhas e treinamentos.
- 6.1.6. O serviço dar-se-á em 3 (três) ciclos anuais, e tem como principais objetivos:
 - 6.1.6.1. Criar, planejar e formalizar institucionalmente o Programa de Conscientização de Segurança da Informação do CNJ;
 - 6.1.6.2. Identificar o nível de maturidade atual do processo de conscientização em segurança da informação dos usuários da organização;
 - 6.1.6.3. Definir o nível de maturidade desejado ao final do primeiro ciclo;
 - 6.1.6.4. Definir a estratégia para se alcançar o nível de maturidade ao final do primeiro ciclo;
 - 6.1.6.5. Definir governança e métricas para monitorar a efetividade do programa e suas ações de conscientização;
 - 6.1.6.6. Executar ações previstas de conscientização em cada ciclo;
 - 6.1.6.7. Criar proposta de ações de conscientização que serão executadas.
- 6.1.7. A tabela a seguir elenca os principais serviços a serem prestados pela CONTRATADA, sempre com a participação das áreas da CONTRATANTE que



Poder Judiciário

Conselho Nacional de Justiça

sejam necessárias para o alinhamento e definição dos detalhamentos necessários para sua execução:

Serviços	Quantidade	Frequência
Desenho de programa de conscientização de segurança	01	Anual
Simulação de phishing geral para descobrir a estatística de propensão de cliques	03	Anual
Personalização e envio de ataques simulados	02	Mensal
Rastreamento de resposta de Phishing Simulado	01	Contínuo
Análise e emissão de relatório com os indicadores dos ataques simulados	01	Mensal
Análise dos usuários com maior risco humano e direcionamento dos devidos treinamentos	01	Mensal
Personalização de campanhas de treinamento	01	Mensal
Definição e manutenção dos grupos inteligentes	01	Mensal
Simulação de ataques USB	01	Mensal
Emissão de relatórios avançados	01	Mensal
Avaliação da evolução	01	Contínuo

6.2. Processos de Conscientização em Segurança da Informação

6.2.1.O Serviço Gerenciado de Conscientização em Segurança da Informação deverá ser executado de forma estruturada, contínua e cíclica, observando, no mínimo, as etapas descritas a seguir, de modo a assegurar a eficácia das ações educativas e a evolução contínua da cultura organizacional de segurança da informação.

6.2.2.Diagnóstico e Planejamento:

- 6.2.2.1. Realização de levantamento detalhado do cenário atual de conscientização, incluindo a análise do nível de maturidade em segurança da informação, práticas adotadas pelos usuários, histórico de incidentes relacionados a falhas humanas e aderência às políticas internas.
- 6.2.2.2. Identificação e análise de riscos associados ao fator humano, incluindo comportamentos inseguros, fragilidades recorrentes e definição de perfis de usuários mais suscetíveis a ataques cibernéticos, tais como phishing, engenharia social e vazamento de informações.
- 6.2.2.3. Definição de público-alvo, priorização dos temas a serem abordados e elaboração de cronograma anual de ações de conscientização,



Poder Judiciário

Conselho Nacional de Justiça

considerando criticidade dos riscos, perfis de acesso à informação e necessidades institucionais.

- 6.2.2.4. Elaboração e formalização do Plano de Conscientização em Segurança da Informação, contemplando objetivos, escopo, metodologias, responsabilidades, indicadores de desempenho e critérios de avaliação.

6.2.3. Desenvolvimento das Ações Educativas:

- 6.2.3.1. Criação de campanhas de conscientização temáticas baseadas em riscos reais e boas práticas de segurança da informação, abrangendo, entre outros temas: phishing, engenharia social, proteção de dados pessoais, gestão de senhas, uso seguro do correio eletrônico, internet e dispositivos corporativos. (ex.: phishing, engenharia social, proteção de dados pessoais, senhas, uso seguro do e-mail e da internet).
- 6.2.3.2. Elaboração de materiais educativos digitais, tais como cartilhas, infográficos, comunicados, quizzes e conteúdos interativos, adequados à linguagem e ao perfil dos públicos-alvo.

6.2.4. Execução das Ações

- 6.2.4.1. Aplicação de campanhas educativas contínuas, garantindo a periodicidade, o alcance dos públicos definidos e a atualização dos conteúdos conforme o contexto de ameaças.
- 6.2.4.2. Realização de palestras, workshops e treinamentos e ações de sensibilização periódicos, com registro de participação e avaliação de eficácia.
- 6.2.4.3. Execução de simulações controladas (ex.: campanhas de phishing simulado), quando aplicável e previamente autorizado, com o objetivo de avaliar o comportamento dos usuários e reforçar o aprendizado.
- 6.2.4.4. Divulgação de comunicados, alertas e orientações educativas, especialmente em situações de aumento de risco ou ocorrência de incidentes relevantes e alertas educativos.

6.2.5. Monitoramento e Avaliação

- 6.2.5.1. Acompanhamento contínuo da participação dos usuários nas ações de conscientização, considerando taxas de adesão, conclusão e engajamento.
- 6.2.5.2. Avaliação do nível de assimilação dos conteúdos, da efetividade das ações e da evolução do comportamento dos usuários, por meio de testes, métricas e indicadores definidos.



Poder Judiciário

Conselho Nacional de Justiça

6.2.5.3. Identificação de usuários, áreas ou grupos que apresentem maior exposição a riscos ou desempenho insatisfatório, demandando ações corretivas, reforço educativo ou campanhas direcionadas.

6.2.5.4. Monitoramento e análise de indicadores de risco humano, com correlação, sempre que possível, com eventos e incidentes de segurança da informação.

6.2.6. Melhoria Contínua

6.2.6.1. Análise dos resultados obtidos, considerando métricas, indicadores e feedback dos usuários.

6.2.6.2. Ajustes nas estratégias, conteúdos e metodologias adotadas, com foco no aumento da eficácia das ações.

6.2.6.3. Atualização contínua Plano de Conscientização em Segurança da Informação, incorporando novos riscos, ameaças emergentes, lições aprendidas, alterações normativas e mudanças no ambiente organizacional.

6.3. Ferramentas

6.3.1. A CONTRATADA deverá suportar o serviço de conscientização de usuários com plataformas de simulação de phishing, envio de pesquisas de maturidade, divulgação de conteúdo e treinamento a distância.

6.3.2. As ferramentas deverão ser providas em formato SaaS ou similar, onde toda a responsabilidade de configuração e gestão ficará por conta da CONTRATADA.

6.3.3. O serviço deverá ter módulo específico para envio de simulações de ataques de phishing.

6.3.4. A CONTRATANTE deverá ter acesso, através de portal integrado, onde deverá ser possível acompanhar a eficiência e abrangência do programa.

6.3.5. A CONTRATANTE poderá sugerir alterações no portal, de forma a representar as necessidades do CNJ.

6.3.6. Não serão aceitos qualquer software livre, OpenSource ou outros que não sejam do fabricante.

6.3.7. A Plataforma deve suportar no mínimo os seguintes idiomas inglês, português Brasil e espanhol sendo que o conteúdo dos treinamentos deve ser provido também, nas mesmas línguas já citadas.



Poder Judiciário

Conselho Nacional de Justiça

6.3.8. Deve suportar integração com Azure Active Directory e LDAP Active Directory;

6.3.9. A solução deve ser provida 100% em nuvem e não deve exigir nenhum servidor adicional, IP dedicado para disparos de e-mail, tão pouco registro de domínios para a sua plena execução.

6.3.10. Deve prover os seguintes módulos/funcionalidades através da console:

- 6.3.10.1. Customização e Simulação de Phishing via e-mail;
- 6.3.10.2. Customização e Simulação de Phishing via USB;
- 6.3.10.3. Treinamentos;
- 6.3.10.4. Exames e Testes;
- 6.3.10.5. Relatórios e Indicadores;
- 6.3.10.6. Materiais Adicionais como cartilhas, papel de paredes, vídeos etc.

6.3.11. Treinamentos devem obrigatoriamente ser:

- 6.3.11.1. Vídeos, Gaming (jogos) e módulos Interativos;
- 6.3.11.2. Entre 5 min a 20 min cada treinamento;
- 6.3.11.3. Ser providos em inglês, português e espanhol;
- 6.3.11.4. Deve ser possível substituir logo da plataforma para logo corporativo da empresa;
- 6.3.11.5. Caso não haja integração SAML, deve ser possível implementar políticas de senhas complexas;
- 6.3.11.6. A plataforma deve possuir a característica de repositório de imagens customizadas para serem utilizadas em simulações de phishing e treinamentos customizados.

6.3.12. A customização de novos templates de e-mail phishing deve possuir as seguintes características:

- 6.3.12.1. Lista de domínios próprios providos pelo fabricante da solução que podem ser utilizados nas simulações, sem qualquer ônus adicional para a sua utilização;
- 6.3.12.2. Devem possuir domínios para serem utilizados no conceito de "impersonation";
- 6.3.12.3. Deve possuir domínios parecidos com grandes marcas no mínimo, nos seguintes segmentos de negócios:



Poder Judiciário

Conselho Nacional de Justiça

- 6.3.12.3.1. Financeiro, no mínimo domínios parecidos com a Paypal;
 - 6.3.12.3.2. Corporativo, no mínimo domínios parecidos com Onedrive, Sharepoint,
 - 6.3.12.3.3. Outlook e HP;
 - 6.3.12.3.4. Tecnologia, no mínimo domínios parecidos com Microsoft;
 - 6.3.12.3.5. Redes Sociais, no mínimo domínios parecidos com LinkedIn;
 - 6.3.12.3.6. Comercial, no mínimo domínios parecidos com Adobe;
 - 6.3.12.3.7. Serviços de Cloud, no mínimo domínios parecidos com Dropbox;
 - 6.3.12.3.8. Consumo final, no mínimo domínios parecidos com Gmail;
- 6.3.13. A CONTRATADA deverá ter a possibilidade de personalização do portal, com alteração de identidade visual de maneira a condizer com as cores e marcas da CONTRATANTE.
- 6.3.14. O portal deverá apresentar uma visão geral do programa fornecendo visibilidade dos participantes das ações, sua área e cargo.
- 6.3.15. O portal deverá permitir a visualização dos resultados das campanhas considerando:
- 6.3.15.1. Número de e-mails de phishing enviados;
 - 6.3.15.2. Taxa de envio de phishing;
 - 6.3.15.3. Número de e-mails de phishing abertos;
 - 6.3.15.4. Taxa de abertura de phishing;
 - 6.3.15.5. Número de e-mails de phishing clicados por usuários;
 - 6.3.15.6. Taxa de cliques em e-mails phishing;
 - 6.3.15.7. Número de usuários que submeteram dados;
 - 6.3.15.8. Taxa de submissão de dados.
- 6.3.16. O portal deverá apresentar minimamente os seguintes indicadores de público de risco:



Poder Judiciário

Conselho Nacional de Justiça

- 6.3.16.1. Número total da Amostragem;
 - 6.3.16.2. Percentual de Usuários com alto grau de risco;
 - 6.3.16.3. Quantidade total de usuários com alto grau de risco;
 - 6.3.16.4. Percentual de usuários com reincidência em campanhas de phishing;
 - 6.3.16.5. Quantidade total de usuários com reincidência em campanhas de phishing;
 - 6.3.16.6. Indicadores de total de participantes da campanha por áreas;
 - 6.3.16.7. Indicadores de total de participantes da campanha por cargo;
 - 6.3.16.8. Indicadores que permitam compreender as estratégias educativas de ataques adotadas;
 - 6.3.16.9. Sumário de acompanhamento da efetividade das ações com relacionando o usuário com a estratégia adotada e o status ações realizadas (submissão de dados ou link clicado).
- 6.3.17. O portal deve permitir a criação de filtros por estratégia adotada, por área e por cargo.
- 6.3.18. O serviço deverá apresentar, em portal web, uma análise cruzada, das informações de credenciais vazadas, frente aos usuários de maior risco identificados no programa de conscientização e frente aos usuários de maior risco identificado pelo serviço de monitoração de segurança.
- 6.3.19. A solução deve possuir no mínimo 80 campanhas prontas, destinadas ao público brasileiro, que despertem o interesse dos usuários com os temas iguais ou similares a:
- 6.3.19.1. Amazon Prime, Netflix ou similares;
 - 6.3.19.2. Armazenamento em serviços de nuvem;
 - 6.3.19.3. Ferramentas de comunicação;
 - 6.3.19.4. Redes sociais;
 - 6.3.19.5. Comunicações sobre serviços de rede;
 - 6.3.19.6. Serviços financeiros;
 - 6.3.19.7. Serviços Apple;
 - 6.3.19.8. Comunicados de apelo social.



Poder Judiciário

Conselho Nacional de Justiça

6.3.20.A solução deve possuir a capacidade de criação de campanhas personalizadas de e-mails de phishing.

6.4. Grupo de Conscientização em Segurança da Informação

6.4.1.Este grupo deverá ser exclusivo para trabalhar no serviço de Conscientização em Segurança da Informação e não podem os profissionais pertencentes a este grupo serem compartilhados e/ou atuarem, com os demais serviços descritos no objeto do presente termo de referência.

6.4.2.Todos os profissionais que integram O GRUPO DE CONSCIENTIZAÇÃO EM SEGURANÇA DA INFORMAÇÃO devem obrigatoriamente compor o quadro de colaboradores da CONTRATADA em regime de trabalho CLT (Consolidação das Leis do Trabalho), não havendo possibilidade a terceirização ou subcontratação de tal serviço.

6.4.3.Deverá ser de responsabilidade da CONTRATADA dimensionar o número de profissionais adequado para entrega de tal serviço, sem que haja impacto no acordo de nível de serviço estabelecido.

6.4.4.Com o objetivo de garantir que os profissionais envolvidos têm conhecimento e habilidade, para executar o processo de conscientização em segurança da informação da CONTRATANTE, a CONTRATADA obrigatoriamente deverá compor o GRUPO DE CONSCIENTIZAÇÃO EM SEGURANÇA DA INFORMAÇÃO com ao menos 1 (um) perfil que segue descrito abaixo. O profissional deverá possuir ao menos uma das certificações indicadas no respectivo perfil, ou equivalentes.

Perfis	Certificações
Analista de Segurança 1	<ul style="list-style-type: none">• CompTIA Security+;• CompTIA CySA+;• CEH - Certified Ethical Hacker;• ISO/IEC 27001 Foundation;• ISO/IEC 27002 Foundation;• Certificação ou curso formal em <i>Security Awareness</i> ou <i>Information Security Awareness</i> emitido por entidade reconhecida;• ISO/IEC 27001 Lead Implementer ou Lead Auditor;• COBIT (Foundation ou superior);



Poder Judiciário

Conselho Nacional de Justiça

	• ITIL (Foundation ou superior).
--	----------------------------------

TABELA 11 – CERTIFICAÇÕES GRUPO DE CONSCIENTIZAÇÃO EM SEGURANÇA DA INFORMAÇÃO

6.4.5. Durante a execução do contrato, a CONTRATADA se obriga a manter todos os profissionais com os requisitos abaixo:

6.4.5.1. Diploma, devidamente registrado, de curso de nível superior de graduação na área de Tecnologia da Informação ou de graduação em qualquer curso superior, acrescido de certificado de curso de pós-graduação em área de Tecnologia da Informação de, no mínimo, 360 (trezentos e sessenta) horas, fornecido por instituição reconhecida pelo Ministério da Educação (MEC);

6.4.5.2. Conhecimento avançado em segurança da informação, com experiência comprovada de no mínimo 06 (meses) em Conscientização em Segurança da Informação;

6.4.6. Não existe restrição ou limite para acúmulo de perfis em um mesmo profissional, uma vez que é de responsabilidade da CONTRATADA definir o quantitativo de profissionais envolvidos no GRUPO DE CONSCIENTIZAÇÃO EM SEGURANÇA DA INFORMAÇÃO, porém conforme já fora mencionado no presente termo de referência, este(s) deve(m) compor único e exclusivamente o time denominado GRUPO DE CONSCIENTIZAÇÃO EM SEGURANÇA DA INFORMAÇÃO.

6.4.7. Será exigido da CONTRATADA as seguintes documentações do(s) profissionais que participarão do CONSCIENTIZAÇÃO EM SEGURANÇA DA INFORMAÇÃO, os quais devem comprovar as exigências e obrigações descritas no presente termo de referência: carteira de trabalho devidamente assinada pela CONTRATADA, curriculum vitae para comprovação de habilidades, e as devidas certificações técnicas para comprovação do conhecimento.

6.5. Das entregas

6.5.1. Para acompanhamento e avaliação do serviço a ser ofertado pela CONTRATADA, a CONTRATANTE definiu os seguintes indicadores chave de desempenho, que reunidos vão compor um único relatório a ser entregue de forma online e em tempo de execução, através do portal segurança da CONTRATADA, a saber: 6.5.2.



Poder Judiciário

Conselho Nacional de Justiça

DENOMINAÇÃO	FORMA DE CÁLCULO	FILTRO	AGRUPADOR	DESCRIÇÃO
Quantitativo de ações de conscientização	Soma das ações executadas no período	Ações executadas	Ações	Número total de ações efetivamente realizadas no mês
Quantitativo de usuários convocados	Soma dos usuários convocados para ações	Usuários convocados	Usuários	Número total de usuários convocados para participar das ações de conscientização
Quantitativo de usuários participantes	Soma dos usuários que participaram	Usuários participantes	Usuários	Número total de usuários que participaram efetivamente das ações de conscientização
Quantitativo de treinamentos concluídos	Soma dos treinamentos concluídos	Treinamentos concluídos	Treinamentos	Número total de treinamentos finalizados no período
Quantitativo de campanhas educativas realizadas	Soma das campanhas realizadas	Campanhas realizadas	Campanhas	Número total de campanhas de conscientização executadas no mês
Quantitativo de simulações de phishing realizadas	Soma das simulações executadas	Simulações de phishing	Simulações	Número total de campanhas de phishing simulado realizadas
Taxa de cliques em phishing simulado	$(\text{Cliques em phishing} / \text{Usuários testados}) \times 100$	Phishing simulado	Percentual	Percentual de usuários que interagiram com mensagens de phishing simulado
Quantitativo de usuários classificados como alto risco	Soma dos usuários de alto risco	Usuários alto risco	Usuários	Número total de usuários classificados com alto nível de risco humano
TOP 10 – Temas mais recorrentes	Soma das ações por tema	Ações por tema	Tema	Ranking dos temas mais abordados nas ações de conscientização
TOP 10 – Áreas com maior exposição ao risco	Soma de usuários de alto risco por área	Vulnerabilidades em Aplicações WEB Usuários por área	Área	Ranking das áreas organizacionais com maior concentração de risco humano
10 – Usuários com maior reincidência (quando aplicável)	Soma de reincidências por usuário	Reincidência de comportamento	Usuário	Ranking de usuários com maior reincidência de comportamentos inseguros
Índice de assimilação de conteúdo	Média dos resultados em avaliações	Avaliações aplicadas	Percentual	Média de aproveitamento dos usuários nos testes pós-treinamento



Poder Judiciário

Conselho Nacional de Justiça

Quantitativo de materiais educativos produzidos	Soma dos materiais produzidos	Materiais produzidos	Materiais	Número total de materiais educativos desenvolvidos no período
Quantitativo de comunicados e alertas divulgados	Soma de comunicados divulgados	Comunicados divulgados	Comunicados	Número total de comunicados e alertas educativos emitidos

TABELA 12 - INDICADORES ESTRATÉGICOS GESTÃO DE CONSCIENTIZAÇÃO DE SEGURANÇA

6.5.3. Tais relatórios e indicadores devem ser apresentados e discutidos em reunião mensal, com presença de profissional que conheça todos os serviços. Nesse contexto, o profissional deve apresentá-lo de forma presencial nas dependências da CONTRATANTE em Brasília-DF ou de forma virtual, por meio de solução de videoconferência.

7. ITEM 06 - SERVIÇO DE TESTES DE INVASÃO (Red Team)

7.1. Condições Gerais

7.1.1. 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.

7.1.2. 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.

7.1.3. 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:

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

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



Poder Judiciário

Conselho Nacional de Justiça

- 7.1.3.3. NIST Special Publication 800115 (Technical Guide to Information Security Testing and Assessment);
- 7.1.3.4. NIST Special Publication 80042;
- 7.1.3.5. Guideline on Network Security Testing;
- 7.1.3.6. OWASP TESTING GUIDE 3.0 The Open Web Application Security Project.
- 7.1.4. Neste documento os termos “pentest”, teste de penetração, teste de intrusão e testes de invasão, são considerados sinônimos;
- 7.1.5. 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);
- 7.1.6. A Contratada deverá observar que os testes de invasão serão executados internamente (qualquer ponto da rede corporativa do CONTRATANTE) E externamente (através da Internet) ;
- 7.1.7. Todas as fases dos “Testes de Invasão” serão acompanhadas e supervisionadas a critério do CONTRATANTE;
- 7.1.8. 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;
- 7.1.9. O teste de invasão deverá obedecer às seguintes fases:
 - 7.1.9.1. Planejamento;
 - 7.1.9.2. Descoberta;
 - 7.1.9.3. Ataque;
 - 7.1.9.4. Relatório Teste de Invasão;
 - 7.1.9.5. Reunião para apresentação do relatório de recomendações e descrição das atividades executada durante o teste;
 - 7.1.9.6. Reavaliação, novo teste pós remediação;
 - 7.1.9.7. Relatório Final do Teste de Invasão.



Poder Judiciário

Conselho Nacional de Justiça

7.2. Planejamento

- 7.2.1. Todas as premissas, processos, atividades descritas e aprovadas na OS, inclusive os cronogramas serão detalhados e apresentados na fase de planejamento;
- 7.2.2. Informações sobre o ambiente corporativo, utilizando-se das seguintes técnicas (podendo ser utilizadas ambas, conforme definição do escopo):
 - 7.2.2.1. Técnica da caixa-preta (pouco ou nenhum conhecimento sobre o ambiente a ser avaliado. O ambiente deverá ser descoberto pelo especialista) ;
 - 7.2.2.2. Técnica da caixa branca (o avaliador tem acesso irrestrito a qualquer informação que possa ser relevante ao teste) ;
 - 7.2.2.3. Técnica da caixa cinza ou híbrida (conhecimento limitado sobre o alvo).

7.3. Descoberta

- 7.3.1. 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 deverão ser apresentadas para ciência e aprovação antes de sua efetiva utilização, assim como a metodologia para análise manual de vulnerabilidades;
- 7.3.2. Na fase da DESCOBERTA deverão ser atendidos os seguintes quesitos e apresentado juntamente no “RELATÓRIO TESTE DE INVASÃO” (quando necessário):
 - 7.3.2.1. Coleta passiva, onde deverá ser utilizada, no mínimo, as seguintes técnicas:
 - 7.3.2.1.1. Whois e nslookup (consultas DNS) ;
 - 7.3.2.1.2. Sites de busca;
 - 7.3.2.1.3. Listas de discussão;
 - 7.3.2.1.4. Blogs de colaboradores;
 - 7.3.2.1.5. Dumpster diving ou trashing;



Poder Judiciário

Conselho Nacional de Justiça

7.3.2.1.6. Informações livres;

7.3.2.1.7. Packet sniffing “passive eavesdropping”;

7.3.2.1.8. Captura de banner.

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

7.3.2.2.1. Port scanning (Mapeamento de rede) ;

7.3.2.2.2. Varredura de vulnerabilidade.

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

7.3.2.3.1. Hosts ativos na rede;

7.3.2.3.2. Portas e serviços em execução;

7.3.2.3.3. Serviços ativos e vulneráveis nos hosts;

7.3.2.3.4. Sistemas operacionais;

7.3.2.3.5. Vulnerabilidades associadas com sistemas operacionais e aplicações descobertas;

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

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

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

7.3.2.3.9. Vulnerabilidades Detectadas (CVE);

7.3.2.3.10. Vulnerabilidades de Alto Risco;

7.3.2.3.11. Vulnerabilidades de Médio Risco;

7.3.2.3.12. Vulnerabilidades de Baixo Risco;

7.3.2.3.13. Informações a serem aplicadas na fase de ataques.

7.3.2.4. Dos serviços e aplicações web:



Poder Judiciário

Conselho Nacional de Justiça

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

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

7.3.2.4.3. Tratamento indevido de entrada;

7.3.2.4.4. Problemas relacionados à má configuração dos serviços;

7.3.2.4.5. Gerenciamento inseguro de sessões web.

7.4. Ataque (exploração)

7.4.1. 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;

7.4.2. 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;

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

7.4.3.1. Violações do protocolo HTTP;

7.4.3.2. SQL Injection;

7.4.3.3. LDAP Injection;

7.4.3.4. Cookie Tampering;

7.4.3.5. CrossSite

7.4.3.6. Scripting (XSS);

7.4.3.7. Directory Transversal;

7.4.3.8. Buffer Overflow;

7.4.3.9. OS Command Execution;

7.4.3.10. Command Injection;nRemote Code Inclusion;



Poder Judiciário

Conselho Nacional de Justiça

7.4.3.11. Server Side Includes (SSI) Injection;

7.4.3.12. File disclosure;

7.4.3.13. Information Leak;

7.4.3.14. Zero day attacks;

7.4.3.15. DDos (Distributed Denial of Service) ;

7.4.3.16. Dos (Denial of Service) ;

7.4.3.17. Contra protocolo TCP;

7.4.3.18. Ataques contra a aplicação.

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

7.4.4.1. Bugs em serviços, aplicativos e sistemas operacionais;

7.4.4.2. SYN flooding;

7.4.4.3. Fragmentação de pacotes de IP;

7.4.4.3.1. Smurf e fraggle;

7.4.4.3.2. Teardrop, nuke e land.

7.4.4.4. Para ataques contra o protocolo TCP:

7.4.4.4.1. Sequestro de conexões;

7.4.4.4.2. Prognóstico de número de sequência do protocolo TCP.

7.4.4.4.2.1. Ataque de Mitnick;

7.4.4.4.2.2. Source routing.

7.4.5. Para ataques em nível da aplicação:

7.4.5.1. Buffer Overflow;

7.4.5.2. Problemas com o SNMP;



Poder Judiciário

Conselho Nacional de Justiça

7.4.5.3. Vírus, worms e cavalos de Tróia.

7.4.6. Injeção de Código:

7.4.6.1. Ataques XSS (Crosssite Script) ;

7.4.6.2. Comprometimento do acesso remoto;

7.4.6.3. Manutenção de acesso;

7.4.6.4. Encobrimento de rastros da invasão.

7.4.7. 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):

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

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

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

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

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

7.4.7.6. Para testes de negócio lógico, aplicar padrão: OWASPBL001;

7.4.7.7. 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;



Poder Judiciário

Conselho Nacional de Justiça

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

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

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

7.4.8.1. Referência-base (Whitepaper);

7.4.8.2. Ameaças encontradas;

7.4.8.3. Riscos levantados ao ambiente computacional;

7.4.8.4. Contramedidas para mitigar as ameaças encontradas.

7.5. Relatório de Teste de Invasão

7.5.1. 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:

7.5.1.1. 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.

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

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

7.5.2.2. Equipamentos e recursos demandados para este teste;

7.5.2.3. Tipos de ataque;



Poder Judiciário

Conselho Nacional de Justiça

- 7.5.2.4. Prazos (janelas de tempo para execução dos testes) ;
- 7.5.2.5. Pontos de contato da contratada (responsáveis para tratamento de questões abordadas nos testes) ;
- 7.5.2.6. Tipos de testes realizados pelos especialistas em segurança da informação;
- 7.5.2.7. Confirmação ou refutação de a existência de vulnerabilidades;
- 7.5.2.8. Documentação sobre o caminho utilizado para exploração, avaliação do impacto e prova da existência da vulnerabilidade;
- 7.5.2.9. Obtenção de acesso e possível escalada de privilégios;
- 7.5.2.10. Detalhamento da metodologia do ataque;
- 7.5.2.11. Recomendações para sanar riscos e vulnerabilidades.

7.6. Reunião para apresentação do relatório de recomendações e descrição das atividades executada durante o teste:

- 7.6.1. 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.

7.7. Relatório Final do Teste de Invasão

- 7.7.1. 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.
- 7.7.2. 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.

7.8. Atividades de Apoio:

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



Poder Judiciário

Conselho Nacional de Justiça

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

7.9. Periodicidade de execução:

- 7.9.1.A CONTRATADA deverá realizar os Testes de Invasão conforme a quantidade definida em Ordem de Serviço (OS);
- 7.9.2.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:
 - 7.9.2.1. Atividades do Pentest;
 - 7.9.2.2. Entrega do relatório “Teste de Invasão”;
 - 7.9.2.3. Ações corretivas das vulnerabilidades apontadas pela CONTRATADA e aplicadas pelo CONTRATANTE;
 - 7.9.2.4. Reavaliação Pentest, caso necessário;
 - 7.9.2.5. Entrega do relatório “Relatório Final do Teste de Invasão”.
- 7.9.3.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”.

7.10. Grupo Técnico de Teste de Invasão (Red Team)

- 7.10.1.O grupo responsável pela execução do serviço de teste de invasão será o GRUPO TÉCNICO DE TESTE DE INVASÃO (Red Team).
- 7.10.2.Com o objetivo de garantir que os profissionais envolvidos têm conhecimento e habilidade, para executar o serviço de teste de invasão, a CONTRATADA



Poder Judiciário

Conselho Nacional de Justiça

obrigatoriamente deverá compor o GRUPO DE TESTE DE INVASÃO com ao menos 1 (um) perfil que segue descrito abaixo:

Perfis	Certificações
Analista de Segurança	<ul style="list-style-type: none">• Certified Ethical Hacker (CEH) Practical ou• 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 ITILv4 Foundation ou superior.

TABELA 13 – CERTIFICAÇÕES GRUPO DE TESTE DE INVASÃO (RED TEAM)



Poder Judiciário

Conselho Nacional de Justiça

ANEXO B – PLATAFORMA DE SEGURANÇA

Borda	Firewall/ NGFW UTM	02
	IPS/Web Filter/Application Control	02
Segurança de Rede	WAF	02
	Anti DDoS	03
	AntiSpam	02
Endpoint	Proteção Endpoints (Servidores, estações e mobile)	01
	Solução de Endpoint Detection and Response (EDR)	01
	Gerenciamento e Políticas de Segurança para Dispositivos e Aplicações	01
SIEM	Gerenciamento de Informações e Eventos de Segurança	01
Nuvem	Ambiente Multi Nuvem	02
	Workloads Cloud	02
	Ativos do ambiente nuvem	3000
	CNAPP - Solução de Proteção de Aplicações Nativas em Nuvem	01
E-mail	Caixas de E-mail	4000
	Caixa Corporativa	600
	Antispam, antimalware e Advanced Threat Protection	02
Identidade	Proteção avançada contra ameaças para Active Directory	01
	Proteção de identidade, políticas de acesso condicional e análise de risco	01
	Inspeção SSL do tráfego web	01
Ferramentas de Gerência	Gerenciamento Centralizado de Logs de NGFW	01



Poder Judiciário

Conselho Nacional de Justiça

ANEXO C – NÍVEIS MÍNIMOS DE SERVIÇO

Para efeito desta contratação, estabelecem-se os seguintes níveis mínimos de serviço. 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 acordo com a Unidade e Periodicidade/Frequência do serviço conforme ([Tabela 1 – Objeto detalhado](#)), de modo a alcançar as respectivas metas exigidas, conforme tabela adiante.

Para os casos de haver mais de uma ocorrência, as glosas por inadimplemento (pontos) serão cumulativas.

De maneira a uniformizar o entendimento quanto a classificação para incidentes e requisições de serviço de segurança da Informação define-se os níveis de criticidade como:

Emergencial	<ul style="list-style-type: none">• Algum tipo de ataque que gerou indisponibilidade em servidores e sistemas críticos, afetando um ou mais usuários;• Infecção ou paralisação generalizada devido a <i>ransomware</i> ou algum outro tipo de malware;• Roubo ou vazamento de dados devido a falha humana ou técnica;• Algum tipo de impacto ou risco grave a empresa ou a equipe de Segurança da Informação;• Quando o problema\incidente é definido com o nível de criticidade “EMERGENCIAL”.
Alta	<ul style="list-style-type: none">• Servidor de produção ou sistema crítico está apresentando instabilidade, degradação ou sofrendo ataques recorrentes que podem acarretar uma exploração ou vazamento de dados;• Alarmes de nível ALTA identificados por ferramentas de SIEM ou ferramenta de segurança que podem ser um falso positivo e necessitam de uma análise para validação;• Ocorrências\incidentes\requisições relacionados a usuários definidos como VIP pelo CONTRATANTE;• Quando o problema\incidente é definido com o nível de criticidade “ALTA”.
Média	<ul style="list-style-type: none">• Nenhum serviço crítico está envolvido e não existe risco de perda de dados;• Alarmes de nível MÉDIO identificados por ferramentas de SIEM ou ferramenta de segurança que podem ser um falso positivo e necessitam de uma análise para validação;• Quando o problema\incidente é definido com o nível de criticidade “MÉDIA”.
Baixa	<ul style="list-style-type: none">• Dúvidas ou apoio à implementação;• Mudanças planejadas;• Novas implementações;• Sugestões de novos recursos ou aprimoramento do Software;



Poder Judiciário

Conselho Nacional de Justiça

	<ul style="list-style-type: none">• Alarmes de nível BAIXA identificados por ferramentas de SIEM ou ferramenta de segurança que podem ser um falso positivo e necessitam de uma análise para validação;• Evidências de um bloqueio ou tratativa automatizada; e• Quando o problema/incidente é definido com o nível de criticidade “BAIXA”.
--	---

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

Grupo 1	1	Tempo máximo para correção de incidente nos serviços de segurança do CNJ, em caso de indisponibilidade	Tempo = Hora do restabelecimento – Hora do início da indisponibilidade	<= 60 minutos	30 pontos (+5 pontos a cada 15 minutos excedentes)
	2	Tempo máximo para requisição de mudança para aplicação de patches e hotfixes de segurança ou indicação de solução de contorno para tratamento de grave 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 dia excedente)
	3	Tempo máximo para abertura de chamados de suporte com terceiros	Tempo = Hora de abertura do chamado – hora da triagem	<= 30 minutos	5 pontos (+2 pontos a cada 10 minutos excedente)
	4	Tempo máximo para resolução de requisições de serviços relacionadas aos Produtos de UTM e WAF	Tempo = Hora da resolução da solicitação – hora de início da solicitação	<= 120 minutos	10 pontos (+3 pontos a cada 30 minutos excedentes)
	5	Tempo máximo para resolução de requisições de serviços relacionadas aos produtos do Anexo B – Plataforma de Segurança	Tempo = Hora da resolução da solicitação – hora da solicitação	<= 24 horas	10 pontos (+3 pontos a cada hora excedente)



Poder Judiciário

Conselho Nacional de Justiça

	6	Tempo máximo para resolução das demais requisições de serviços	Tempo = Hora da resolução da solicitação – hora da solicitação	<= 72 horas	10 pontos (+3 pontos a cada dia excedente)
Item 3 - Grupo 1	7	Tempo máximo para triagem de incidentes de segurança	Tempo = Hora da triagem – Hora de entrada do evento de segurança	<= 30 minutos	3 pontos (+1 ponto a cada 10 minutos excedentes)
	8	Tempo máximo para resposta de incidentes de segurança de criticidade emergencial	Tempo = Hora do início da resposta – hora da triagem	<= 30 minutos	10 pontos (+3 pontos a cada 5 minutos excedentes)
	10	Tempo máximo para resposta de incidentes de segurança de criticidade alta	Tempo = Hora do início da resposta – hora da triagem	<= 60 minutos	10 pontos (+3 pontos a cada 10 minutos excedentes)
	11	Tempo máximo para resposta de incidentes de segurança de criticidade média	Tempo = Hora do início da resposta – hora da triagem	<= 180 minutos	5 pontos (+3 pontos a cada 15 minutos excedentes)
	12	Tempo máximo para resposta de incidentes de segurança de criticidade baixa	Tempo = Hora do início da resposta – hora da triagem	<= 240 minutos	3 pontos (+2 pontos a cada 30 minutos excedente)
	13	Tempo máximo para comunicação de incidentes a Central de serviços da CONTRATADA e aos gestores de TI	Tempo = Hora da comunicação – hora da triagem	<= 30 minutos	5 pontos (+2 pontos a cada 10 minutos excedentes)
Item 6 – Não Agrupado	14	Índice de cumprimento dos prazos acordados para a execução das Ordens de Serviço Exclusivas	Prazo Real – (Prazo Acordado + 25%)	<= 0	20 pontos



Poder Judiciário

Conselho Nacional de Justiça

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

Todos	12	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
	13	Causar qualquer indisponibilidade dos serviços da contratante por motivo de imperícia ou imprudência na execução das atividades contratuais	Por ocorrência	10
	14	Suspender, colocar como pendente, pausar ou interromper, salvo por motivo de força maior ou caso fortuito, os serviços solicitados.	Por ocorrência	05
	15	Realizar mudanças de configuração nas soluções de segurança sem autorização da unidade responsável	Por regra incluída, alterada ou excluída	10
	16	Fraudar, manipular ou descaracterizar indicadores, metas de níveis de serviço e de desempenho por quaisquer subterfúgios	Por ocorrência	100
	17	Causar qualquer indisponibilidade dos serviços do CONTRATANTE por motivo de imperícia ou imprudência na execução das atividades contratuais.	Por ocorrência	50
	18	Deixar de cumprir qualquer outra obrigação estabelecida no edital e não prevista nesta tabela, de forma reincidente, após formalmente notificada pelo CONTRATANTE.	Por ocorrência	10
	19	Perder dados ou informações corporativas por erros na operação devidamente comprovados.	Por ocorrência	200
	20	Causar qualquer dano aos equipamentos do contratante por motivo de imperícia na execução das atividades contratuais.	Por ocorrência	50
	21	Recusar-se a executar serviço relacionado ao objeto do contrato, determinado pela fiscalização, por serviço.	Por ocorrência	10
	22	Utilizar indevidamente os recursos de TI (acessos indevidos, utilização para fins particulares, etc.) ou utilizar equipamento particular, salvo em situação excepcional e devidamente autorizado pelo CONTRATANTE.	Por ocorrência	10



Poder Judiciário

Conselho Nacional de Justiça

	23	Incluir, excluir ou alterar regras nos dispositivos de segurança sem autorização do gestor de TI, ou contrariando as políticas de segurança do CONTRATANTE.	Por ocorrência	30
	24	Não respeitar o cronograma apresentado em uma proposta de execução de atividades quando se tratar de uma Requisição Planejada.	Por ocorrência	10
	25	Interromper unilateralmente a prestação de serviços sem que haja evento de força maior que o justifique	Por ocorrência	30
	26	Deixar de apresentar relatórios, levantamentos ou inventários no prazo determinado em comum acordo.	Por ocorrência	10
Grupo 1	27	Deixar de produzir ou de manter atualizadas as rotinas e scripts da Base de Dados de Conhecimentos.	Por ocorrência	05
	28	Deixar de comunicar o contratante da substituição de profissionais responsáveis pela execução das atividades	Por ocorrência	10
	29	Deixar de atuar tempestivamente no caso de incidentes graves	Por ocorrência	15
	30	Deixar de documentar os ICs – Itens de Configuração e de manter completa e atualizada a Base de Dados de Configuração, inclusive no que diz respeito aos diagramas e desenhos, imediatamente após sua inclusão ou exclusão do ambiente.	Por ocorrência	02

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

Todos	31	Cumprir ou implementar as rotinas em conformidade com a Política de Segurança ou determinações da equipe de fiscalização do contrato	Por ocorrência	10 pontos
	32	Cumprir quaisquer obrigações estabelecidas no contrato e anexos, não previstas nesta tabela, após reincidência formalmente notificada pelo CNJ	Por ocorrência	15 pontos
	33	Cumprir ou implementar as rotinas em conformidade com os processos de trabalho do CNJ e da Diretoria de Tecnologia da Informação	Por ocorrência	10 pontos



Poder Judiciário

Conselho Nacional de Justiça

	34	Elaborar auditorias de dados, consultas às bases de logs de transações ou relatórios diversos	Por ocorrência	15 pontos
Grupo 1	35	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
	36	Apresentar relatórios, levantamentos ou inventários conforme demanda em até 3 dias úteis	Por ocorrência	05 pontos
	37	Apresentar mensalmente proposta de melhorias no ambiente	Por ocorrência	05 pontos
	38	Notificar sobre ocorrências recorrentes	Por ocorrência	05 pontos
Item 1 Grupo 1	39	Manter o Configuration Management Database (CMDB) atualizado	Por ocorrência	10 pontos
	40	Manter a documentação e os desenhos das topologias atualizados e completos	Por ocorrência	05 pontos
	41	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
	42	Analisar a viabilidade e o impacto da instalação de novas soluções ou correções	Por ocorrência	05 pontos
	43	Deixar de notificar incidentes repetitivos**, quer tenham sido conhecidos através do monitoramento ou por notificações de usuários, para a equipe segurança da CONTRATANTE.	Por ocorrência	05 pontos

****Entende-se por “incidentes repetitivos” aqueles abertos por um mesmo usuário a respeito de uma mesma solicitação por mais de duas vezes em um período de 7 dias consecutivos**



Poder Judiciário

Conselho Nacional de Justiça

ANEXO D - MODELO ORDEM DE SERVIÇO



Poder Judiciário

Conselho Nacional de Justiça

ORDEM DE SERVIÇO N. X DE XX DE <MÊS> DE 2026

Área demandante	DISI/SEGS
Nome da Contratada	<nome da contratada>
Nº Contrato	<número do contrato>
Descrição da OS	Prestação de SERVIÇOS GERENCIADOS DE SEGURANÇA DA INFORMAÇÃO
Data de Início	Dia/mês/ano
Classificação da OS	Rotineira ou exclusiva
Detalhamento dos Serviços	Serviços Gerenciados de Segurança da Informação, observados o Edital, o Termo de Referência e seus Anexos e a proposta da CONTRATADA , incluindo: Item 1 - Serviço de administração, operação e manutenção e atendimento a requisições. Item 2 - Serviço de gestão de vulnerabilidades Item 3 - Serviço de gestão de incidentes de segurança (CSIRT - Blue Team Item 4 - Serviço de monitoramento e visibilidade de ataques cibernéticos Item 5 - Serviço de conscientização em segurança da informação Item 6 - Serviço de teste de invasão (Pentest)
Níveis mínimos de serviço	Conforme ANEXO "C" DO CONTRATO N. XX/XXXX, CELEBRADO ENTRE A UNIÃO, POR INTERMÉDIO DO CONSELHO NACIONAL DE JUSTIÇA, E A EMPRESA <CONTRATADA>, PARA CONTRATAÇÃO DE SERVIÇOS GERENCIADOS DE SEGURANÇA DA INFORMAÇÃO
Responsáveis pela fiscalização e autorização no CONTRATANTE	Gestores do Contrato XX/XXXX
Responsável pelo aceite na CONTRATADA	Nome responsável pela CONTRATADA



Poder Judiciário

Conselho Nacional de Justiça

ANEXO E - MODELO DE TERMO DE RECEBIMENTO DEFINITIVO DO SERVIÇO

OS Nº	Data da Emissão	Hora da Emissão	Nº do Contrato
INFORMAÇÕES DA CONTRATADA			
Razão Social:			
Endereço:			
CNPJ/MF:			
Telefone: ()		Contato:	
INFORMAÇÕES DA CONTRATANTE			
Contratante: CONSELHO NACIONAL DE JUSTIÇA			
Endereço: SAF SUL Quadra 2 Lotes 5/6 CEP: 70070-600 (edifício sede)			
CNPJ n.º 07.421.906/0001-29			
ESPECIFICAÇÃO DO SERVIÇO			
Objeto: Prestação de serviços técnicos Serviços Gerenciados de Segurança da Informação para atendimento às necessidades do Conselho Nacional de Justiça - CNJ, conforme especificações e condições definidas em CONTRATO.			
PRAZO DE EXECUÇÃO:			
LOCAL DE EXECUÇÃO:			
RECEBIMENTO DEFINITIVO			
<p>O CONSELHO NACIONAL DE JUSTIÇA – CNJ recebe definitivamente os serviços prestados através da OS supracitada, autorizando, após análise da adequação aos parâmetros mínimos de serviço e desempenho, a emissão da correspondente Nota Fiscal de Serviços no valor abaixo.</p> <p>Valor dos Serviços: R\$_____ Valor dos serviços, considerados os ajustes em função do descumprimento dos níveis mínimos de serviço e desempenho.</p> <p>Brasília, _____ de _____ de _____.</p>			
Assinatura Gestor do Contrato Matricula:XXXXXXXXXX		Assinatura Fiscal Requisitante do Contrato Matricula:XXXXXXXXXX	



Poder Judiciário

Conselho Nacional de Justiça

ANEXO F – DECLARAÇÃO DE VISTORIA

DECLARAÇÃO DE VISTORIA TÉCNICA

Ao Conselho Nacional de Justiça

A _____ (nome da empresa, CNPJ),
localizada _____ (endereço completo),
representada por _____, declara, para fins de
participação em processo licitatório, que vistoriou o local dos serviços, tem conhecimento do
objeto licitado no Pregão Eletrônico nº...../2026, inclusive quanto às características físicas,
das quantidades e especificidades dos serviços objeto desta licitação e não fará qualquer
reclamação posterior de desconhecimento de detalhes técnicos e operacionais não
detectados na vistoria.

Brasília - DF, ____ de _____ de 2026.

RESPONSÁVEL TÉCNICO DA EMPRESA

SERVIDOR RESPONSÁVEL



Poder Judiciário

Conselho Nacional de Justiça

ANEXO G – TERMO DE CIÊNCIA INDIVIDUAL

Termo de Ciência Individual do Compromisso de Sigilo e Segurança da Informação	
IDENTIFICAÇÃO DO CONTRATO	
Nº do Contrato	
Empresa Contratada	
CNPJ	
Objeto Resumido	
Vigência Contratual	
TERMOS	
<p>O(s) funcionário(s) abaixo qualificado(s) declara(m) ter pleno conhecimento de sua(s) responsabilidade(s) no que concerne ao sigilo que deve ser mantido sobre as atividades desenvolvidas ou as ações realizadas no âmbito do Contrato Administrativo nº / , bem como sobre todas as informações que eventualmente ou por força de sua(s) função(ões) venha(m) a tomar conhecimento, comprometendo-se a guardar o sigilo necessário nos termos da legislação vigente e a prestar total obediência às normas de segurança da informação vigentes no ambiente do CONTRATANTE ou que venham a ser implantadas a qualquer tempo por este; em conformidade com o TERMO DE COMPROMISSO DE SEGURANÇA DA INFORMAÇÃO firmado entre as partes.</p>	
OBSERVAÇÕES	
(registrar, caso haja)	
DE ACORDO	
<p>E, por assim estarem justas e estabelecidas as condições, o presente TERMO DE CIÊNCIA é assinado pela(s) parte(s) declarante(s) em 02 (duas) vias de igual teor e um só efeito</p>	
Brasília (DF), / / .	
IDENTIFICAÇÃO E ASSINATURA DO(S) DECLARANTE(S)	
Nome: Identidade: CPF: Função:	Assinatura
Observação: Este termo deve ser impresso em papel timbrado da CONTRATADA	



Poder Judiciário

Conselho Nacional de Justiça

ANEXO H - MODELO DE TERMO DE COMPROMISSO DE MANUTENÇÃO DE SIGILO

O Conselho Nacional de Justiça, sediado em SAF SUL Quadra 2 Lotes 5/6 CEP: 70070-600 (edifício sede), em Brasília – Distrito Federal, CNPJ n.º 07.421.906/0001-29 doravante denominado CONTRATANTE, e, de outro lado, a <NOME DA EMPRESA>, sediada em <ENDEREÇO>, CNPJ n.º <CNPJ>, doravante denominada CONTRATADA;

CONSIDERANDO que, em razão do CONTRATO N.º XX/20XX doravante denominado CONTRATO PRINCIPAL, a CONTRATADA poderá ter acesso a informações sigilosas do CONTRATANTE;

CONSIDERANDO a necessidade de ajustar as condições de revelação destas informações sigilosas, bem como definir as regras para o seu uso e proteção;

CONSIDERANDO o disposto na Política de Segurança da Informação do CONTRATANTE;

Resolvem celebrar o presente TERMO DE COMPROMISSO DE MANUTENÇÃO DE SIGILO, doravante TERMO, vinculado ao CONTRATO PRINCIPAL, mediante as seguintes cláusulas e condições

Cláusula Primeira – DO OBJETO

Constitui objeto deste TERMO o estabelecimento de condições específicas para regulamentar as obrigações a serem observadas pela CONTRATADA, no que diz respeito ao trato de informações sensíveis e sigilosas, disponibilizadas pelo CONTRATANTE, por força dos procedimentos necessários para a execução do objeto do CONTRATO PRINCIPAL celebrado entre as partes e em acordo com o que dispõe o Decreto n. 7.845/2012- Salvaguarda de dados, informações, documentos e materiais sigilosos de interesse da segurança da sociedade e do Estado.

Cláusula Segunda – DOS CONCEITOS E DEFINIÇÕES

Para os efeitos deste TERMO, são estabelecidos os seguintes conceitos e definições:

Informação: é o conjunto de dados organizados de acordo com procedimentos executados por meios eletrônicos ou não, que possibilitam a realização de atividades específicas e/ou tomada de decisão.

Informação Pública ou Ostensiva: são aquelas cujo acesso é irrestrito, obtida por divulgação pública ou por meio de canais autorizados pelo CONTRATANTE.

Informações Sensíveis: são todos os conhecimentos estratégicos que, em função de seu potencial no aproveitamento de oportunidades ou desenvolvimento nos ramos econômicos, político, científico, tecnológico, militar e social, possam beneficiar a Sociedade e o Estado brasileiros.



Poder Judiciário

Conselho Nacional de Justiça

Informações Sigilosas: são aquelas cujo conhecimento irrestrito ou divulgações possam acarretar qualquer risco à segurança da sociedade e do Estado, bem como aquelas necessárias ao resguardo da inviolabilidade da intimidade, da vida privada, da honra e da imagem das pessoas.

Cláusula Terceira – DAS INFORMAÇÕES SIGILOSAS

Serão consideradas como informação sigilosa, toda e qualquer informação escrita ou oral, revelada a outra parte, contendo ou não a expressão confidencial e/ou reservada. O TERMO informação abrangerá toda informação escrita, verbal, ou em linguagem computacional em qualquer nível, ou de qualquer outro modo apresentada, tangível ou intangível, podendo incluir, mas não se limitando a: know-how, técnicas, especificações, relatórios, compilações, código fonte de programas de computador na íntegra ou em partes, fórmulas, desenhos, cópias, modelos, amostras de ideias, aspectos financeiros e econômicos, definições, informações sobre as atividades do CONTRATANTE e/ou quaisquer informações técnicas/comerciais relacionadas/resultantes ou não ao CONTRATO PRINCIPAL, doravante denominados INFORMAÇÕES, a que diretamente ou pelos seus empregados, a CONTRATADA venha a ter acesso, conhecimento ou que venha a lhe ser confiada durante e em razão das atuações de execução do CONTRATO PRINCIPAL celebrado entre as partes.

Parágrafo Primeiro – Comprometem-se, as partes, 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 Segundo – As partes deverão cuidar para que as informações sigilosas fiquem restritas ao conhecimento das pessoas que estejam diretamente envolvidas nas atividades relacionadas à execução do objeto do CONTRATO PRINCIPAL.

Parágrafo Terceiro – As obrigações constantes deste TERMO não serão aplicadas às INFORMAÇÕES que:

I – Sejam comprovadamente de domínio público no momento da revelação;

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 Quarta – DOS DIREITOS E OBRIGAÇÕES



Poder Judiciário

Conselho Nacional de Justiça

As partes se comprometem e se obrigam a utilizar a informação sigilosa revelada pela outra parte exclusivamente para os propósitos da execução do CONTRATO PRINCIPAL, em conformidade com o disposto neste TERMO.

Parágrafo Primeiro – A CONTRATADA se compromete a não efetuar qualquer tipo de cópia da informação sigilosa sem o consentimento expresso e prévio do CONTRATANTE.

Parágrafo Segundo – A CONTRATADA compromete-se a dar ciência e obter o aceite formal da direção e empregados que atuarão direta ou indiretamente na execução do CONTRATO PRINCIPAL sobre a existência deste TERMO bem como da natureza sigilosa das informações.

I – A CONTRATADA deverá firmar acordos por escrito com seus empregados visando garantir o cumprimento de todas as disposições do presente TERMO e dará ciência ao CONTRATANTE dos documentos comprobatórios.

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

Parágrafo Quarto – Cada parte permanecerá como fiel depositária das informações reveladas à outra parte em função deste TERMO.

I – Quando requeridas, as informações deverão retornar imediatamente ao proprietário, bem como todas e quaisquer cópias eventualmente existentes.

Parágrafo Quinto – A CONTRATADA obriga-se por si, sua controladora, suas controladas, coligadas, representantes, procuradores, sócios, acionistas e cotistas, por terceiros eventualmente consultados, seus empregados, 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 Proprietárias por seus agentes, representantes ou por terceiros;



Poder Judiciário

Conselho Nacional de Justiça

III – Comunicar ao CONTRATANTE, de imediato, de forma expressa e antes de qualquer divulgação, caso tenha que revelar qualquer uma das informações, por determinação judicial ou ordem de atendimento obrigatório determinado por órgão competente; e

IV – Identificar as pessoas que, em nome da CONTRATADA, terão acesso às informações sigilosas.

Cláusula Quinta – 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 Sexta – DAS PENALIDADES

A quebra do sigilo e/ou da confidencialidade das informações, devidamente comprovada, possibilitará a imediata aplicação de penalidades previstas conforme disposições contratuais e legislações em vigor que tratam desse assunto, podendo até culminar na rescisão do CONTRATO PRINCIPAL firmado entre as PARTES. Neste caso, a CONTRATADA, estará sujeita, por ação ou omissão, ao pagamento ou recomposição de todas as perdas e danos sofridos pelo CONTRATANTE, inclusive as de ordem moral, bem como as de responsabilidades civil e criminal, as quais serão apuradas em regular processo administrativo ou judicial, sem prejuízo das demais sanções legais cabíveis, conforme Art. 87 da Lei nº. 8.666/93.

Cláusula Sétima – DISPOSIÇÕES GERAIS

Este TERMO 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 deles decorrentes, ou se constatando 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 – O CONTRATANTE terá o direito de, a qualquer tempo e sob qualquer motivo, auditar e monitorar as atividades da CONTRATADA;

II – A CONTRATADA deverá disponibilizar, sempre que solicitadas formalmente pelo CONTRATANTE, todas as informações requeridas pertinentes ao CONTRATO PRINCIPAL.



Poder Judiciário

Conselho Nacional de Justiça

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 regulamentações brasileiras pertinentes;

V – O presente TERMO somente poderá ser alterado mediante TERMO aditivo firmado pelas partes;

VI – Alterações do número, natureza e quantidade das informações disponibilizadas para a CONTRATADA não descaracterizarão ou reduzirão o compromisso e as obrigações pactuadas neste TERMO, que permanecerá válido e com todos seus efeitos legais em qualquer uma das situações tipificadas neste instrumento;

VII – O acréscimo, complementação, substituição ou esclarecimento de qualquer uma das informações disponibilizadas para a CONTRATADA, serão incorporados a este TERMO, passando a fazer dele parte integrante, para todos os fins e efeitos, recebendo também a mesma proteção descrita para as informações iniciais disponibilizadas, sendo necessário a formalização de TERMO aditivo ao CONTRATO PRINCIPAL;

VIII – Este TERMO não deve ser interpretado como criação ou envolvimento das Partes, ou suas filiadas, nem em obrigação de divulgar Informações Sigilosas para a outra Parte, nem como obrigação de celebrarem qualquer outro acordo entre si.

Cláusula Oitava – DO FORO

O CONTRATANTE elege o foro da <CIDADE DO CONTRATANTE>, onde está localizada a sede do CONTRATANTE, para dirimir quaisquer dúvidas originadas do presente TERMO, com renúncia expressa a qualquer outro, por mais privilegiado que seja.

E, por assim estarem justas e estabelecidas as condições, o presente TERMO DE COMPROMISSO DE MANUTENÇÃO DE SIGILO é assinado pelas partes na forma eletrônica, nos termos da Lei n. 11.419/2006 e da Instrução Normativa CNJ n. 67/2015..

_____, _____ de _____ de 20____

<ASSINATURA DO CONTRATANTE> - Nome/Matricula

<ASSINATURA DO CONTRATADA> - nome/identificação



Poder Judiciário

Conselho Nacional de Justiça

ANEXO I – DECLARAÇÃO DE NÃO-NEPOTISMO

1. O modelo a seguir corresponde à declaração a ser assinada por cada profissional designado em qualquer serviço objeto deste edital.

DECLARAÇÃO DE RELAÇÃO FAMILIAR OU DE PARENTESCO

(Resolução 7/2005 – CNJ e suas alterações)

IDENTIFICAÇÃO DA EMPRESA CONTRATADA:

XXXXXXXXXXXXXXXXXXXXXXXXXXXX

CNPJ/MF: xxxxxxxx

Endereço: XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX

Telefone/fax (NN) NNNNNN

Contrato n. NNNNNN

IDENTIFICAÇÃO DO(A) EMPREGADO(A)

NOME:.....

RG:..... ÓRGÃO EMISSOR:..... CPF:



Poder Judiciário

Conselho Nacional de Justiça

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 CNJ?

NÃO ()

SIM () pormenorizar em folha anexa.

DECLARO, sob as penas da Lei, que as informações prestadas são verdadeiras.

Local: _____

Data/...../.....

Assinatura do (a) empregado (a):

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 e suas alterações:

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. O modelo a seguir corresponde à declaração a ser assinada pelo representante da empresa na assinatura do contrato e em cada renovação.



Poder Judiciário

Conselho Nacional de Justiça

DECLARAÇÃO DE NÃO OCORRÊNCIA DE NEPOTISMO

Eu, _____, brasileiro, casado, RG n. _____ Órgão
Emissor:....., 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 Nacional de Justiça

ANEXO J – PLANILHA DE ATENDIMENTO AOS REQUISITOS TÉCNICOS

Grupo 01 – Item 02: Gestão de vulnerabilidades – Item 3.3.6, Breach and Attack Simulation (BAS) – Item 3.3.7 e Gerenciamento de Correções (Patch Management) – Item 3.3.8 do Anexo A do Termo de Referência			
Nome da Solução ou Produto ofertado:			
Descrição:			
Fabricante:			
Item	Documento	Página	Localização

Grupo 01 – Item 04: Monitoramento em Deep e Dark Web – Item 5.2.2 e Monitoramento e Detecção de Incidentes de Rede (NDR) – Item 5.2.3 do Anexo A do Termo de Referência			
Nome da Solução ou Produto ofertado:			
Descrição:			
Fabricante:			
Item	Documento	Página	Localização

Grupo 01 – Item 05: Plataforma de Conscientização em Segurança da Informação – Item 6.3 do Anexo A do Termo de Referência			
Nome da Solução ou Produto ofertado:			
Descrição:			
Fabricante:			
Item	Documento	Página	Localização



Poder Judiciário

Conselho Nacional de Justiça

ANEXO K - TERMO DE RESPONSABILIDADE E COMPROMISSO COM O CÓDIGO DE CONDUTA PARA FORNECEDORES DE BENS E SERVIÇOS DO CONSELHO NACIONAL DE JUSTIÇA

Eu, _____, inscrito(a) no CPF sob nº _____, neste ato representando o(a) _____, inscrito(a) no CNPJ nº _____, declaro: Ter recebido cópia do "Código de Conduta para Fornecedores de Bens e de Serviços do Conselho Nacional de Justiça"; Ter conhecimento do inteiro teor do referido Código e estar de pleno acordo com o seu conteúdo, que li e entendi, comprometendo-me a cumpri-lo fielmente durante toda a vigência de meu contrato e, após, no que for cabível; Ter conhecimento de que para fornecer serviços, bens e produtos ou estabelecer qualquer tipo de parceria com o Conselho Nacional de Justiça é necessário respeitar fielmente o presente Código, cujas avaliações quanto ao cumprimento serão objeto de cláusula(s) contratual(ais). Ter conhecimento de que as infrações a este Código, às políticas e normas do Conselho Nacional de Justiça serão analisadas, mediante a apresentação de relatórios, documentos, disponibilização de acesso a sistemas informatizados, vistorias, na forma que forem estabelecidas nas cláusulas contratuais, estando sujeitas à não prorrogação dos contratos administrativos e às ações aplicáveis, sem prejuízo de encaminhamento aos órgãos responsáveis pela apuração dos fatos e aplicação das penalidades cabíveis.

_____, _____ de _____ de _____



Poder Judiciário

Conselho Nacional de Justiça

ANEXO L – CATÁLOGO DE SERVIÇO

Este catálogo de serviços de apoio ao planejamento tem por finalidade estabelecer, descrever e caracterizar grande parte dos serviços que compõem o objeto da contratação. A estrutura deste catálogo é organizada em conformidade com os itens do objeto contratual, correspondendo diretamente aos serviços descritos nos itens 1 a 5 do instrumento convocatório, conforme segue:

1. Serviço de Administração, Operação e Manutenção e Atendimento a requisições
2. Serviço de Gestão de Vulnerabilidades
3. Serviço de Gestão de incidentes de segurança
4. Serviço de Monitoramento e Visibilidade de Ataques Cibernéticos
5. Serviço de Conscientização em Segurança da Informação

Essa organização visa assegurar aderência integral ao objeto da contratação, facilitar a rastreabilidade entre escopo, execução e fiscalização contratual, bem como promover clareza na definição das obrigações e entregas associadas a cada serviço.

Grupo de Serviço	ID	Serviço
01	1	Configuração de políticas e regras de Firewall
	2	Configuração de políticas IDS/IPS
	3	Configuração de políticas de WAF
	4	Configuração de políticas de AntiDDoS
	5	Configuração de políticas de AntiSpam
	6	Configuração de políticas de segurança (L4/L7)
	7	Configuração de políticas por identidade e grupo
	8	Gestão centralizada de proteção de endpoint
	9	Configuração de políticas de integridade do host
	10	Configuração de políticas de controle de aplicações e dispositivos
	11	Instalação e atualização de clientes via console
	12	Aplicação de política de Threat Prevention (antivírus, anti-spyware/bot ou IPS)
	13	Aplicação de políticas de QoS



Poder Judiciário

Conselho Nacional de Justiça

	14	Configuração de políticas de autenticação e controle de acesso
	15	Ajuste de MFA/SSO e perfis administrativos
	16	Aplicação de categoria de URL filtering baseada em usuário/grupo
	17	Análise/criação e tratamento de IOC (Indicator of Compromise)
	18	Atualizações de SO e firmwares dos dispositivos
	19	Configuração de inspeção SSL/TLS
	20	Gestão e controle de acesso VPN
	21	Configuração de políticas de categorização e bloqueio por URL
	22	Parametrização, updates e suporte de ferramentas de segurança
	23	Criação de relatórios gerenciais e técnicos de situação do parque
	24	Aplicar controle de uso de aplicação por usuário/grupo de usuário
	25	Aplicação de hardening em sistemas, servidores e dispositivos de segurança
	26	Verificações periódicas de saúde e performance
	27	Auditorias técnicas, relatórios e recomendações
	28	Gestão de certificados digitais e chaves criptográficas (quando aplicável às ferramentas)
	29	Gestão de integrações com Active Directory/LDAP/SSO
	30	Atendimento de requisições técnicas e operacionais da CONTRATANTE
	31	Operação contínua das soluções de segurança
Serviço de Gestão de Vulnerabilidades		
Grupo de Serviço	ID	Serviço
02	1	Fornecimento de ferramenta de Gestão de Vulnerabilidades
	2	Fornecimento de ferramenta de BAS (Breach and Attack Simulation)
	3	Implantação e configuração da ferramenta de Gestão de Vulnerabilidades
	4	Implantação e configuração da ferramenta BAS
	5	Descoberta de ativos e inventário contínuo do ambiente monitorado
	6	Parametrização do escopo de varredura de infraestrutura e aplicações Web/APIs



Poder Judiciário

Conselho Nacional de Justiça

7	Configuração de credenciais para varreduras autenticadas (quando aplicável)
8	Checagem (scan) e varredura recorrentes e sob demanda em ativos de rede
9	Checagem (scan) e varredura recorrentes e sob demanda em aplicações Web e APIs
10	Análise de falso positivo em ativos de rede e aplicações Web/APIs
11	Informativo sobre vulnerabilidades em ativos de rede e aplicações Web/APIs
12	Priorização de vulnerabilidades com base em criticidade (CVSS, contexto e impacto)
13	Monitoramento contínuo de vulnerabilidades críticas e exploração ativa (quando aplicável)
14	Apoio técnico ao processo de correção de vulnerabilidades pelas equipes internas
15	Revalidação periódica de vulnerabilidades tratadas e encerramento de achados
16	Gestão de exceções, aceites de risco e justificativas técnicas
17	Execução de simulações controladas via BAS para validação de controles existentes
18	Execução de campanhas BAS com base em MITRE ATT&CK
19	Apresentação de abordagem dinâmica para priorizar correções
20	Emissão de relatórios técnicos e gerenciais periódicos
21	Geração de indicadores (KPIs) e métricas de maturidade de vulnerabilidades
22	Fornecimento da ferramenta de gerenciamento de correções (patch management)
23	Identificação, correlação e priorização de patches associados às vulnerabilidades identificadas
24	Execução de aplicação de patches e atualizações de segurança
25	Agendamento, orquestração e controle de tarefas de aplicação de patches
26	Acompanhamento da aplicação de patches e validação de conformidade dos ativos
27	Monitoramento de ativos desatualizados, vulneráveis ou sem cobertura de políticas de atualização
28	Revalidação de vulnerabilidades após aplicação de patches ou ações de remediação
29	Geração de relatórios e indicadores sobre conformidade, cobertura e efetividade do processo de patch management
30	Apoio técnico às equipes da CONTRATANTE na análise de impacto, planejamento e tratamento de correções críticas



Poder Judiciário

Conselho Nacional de Justiça

	31	Acompanhamento de falhas de aplicação de patches, inconsistências e necessidade de rollback (quando aplicável)
Serviço de Gestão de Incidentes		
Grupo de Serviço	ID	Serviço
03	1	Recebimento e triagem de alertas provenientes do SOC e ferramentas de segurança
	2	Classificação de eventos de segurança e categorização de incidentes
	3	Investigação técnica de incidentes de segurança da informação
	4	Coleta, análise e preservação de evidências digitais (logs, endpoints, tráfego e artefatos)
	5	Execução de contenção de incidentes (bloqueios, isolamento e mitigação imediata)
	6	Erradicação de ameaças e remoção de artefatos maliciosos
	7	Validação do contorno do incidente
	8	Apoio à recomposição e restauração segura de serviços afetados
	9	Apoio à resposta a incidentes
	10	Playbooks e resposta coordenada
	11	Elaboração de plano de resposta e recomendações técnicas de mitigação
	12	Análise de causa raiz e documentação
	13	Emissão de relatório técnico completo do incidente
	14	Emissão de relatório executivo com impacto e recomendações estratégicas
	15	Registro e documentação do incidente em sistema de tickets e/ou ferramenta definida
	16	Formalização e comunicação de encerramento
	17	Apoio à comunicação interna e à gestão de crise
	18	Apoio à melhoria de processos e controles após incidentes (revisões e lições aprendidas)
	19	Documentação e melhorias de processo
Serviços de Monitoramento e visibilidade de ataques cibernéticos		
Grupo de Serviço	ID	Serviço
	1	Fornecimento de Inteligência de Ameaças e Proteção de Risco Digital (DRP/CTI)



Poder Judiciário

Conselho Nacional de Justiça

04	2	Monitoramento contínuo 24x7 dos ativos e eventos
	3	Coleta e ingestão de logs de infraestrutura, sistemas e aplicações
	4	Coleta e ingestão de logs de firewalls, proxies, WAF, EDR/XDR, AD e serviços críticos
	5	Normalização, correlação e análise de eventos de segurança em SIEM
	6	Identificação de indicadores de comprometimento (IOC) e comportamento suspeito
	7	Análise de alertas e redução de falsos positivos
	8	Criação, ajuste e otimização de regras de correlação e detecção
	9	Classificação de severidade e priorização de alertas
	10	Escalonamento de eventos para CSIRT/Blue Team quando configurado incidente
	11	Emissão de relatórios de monitoramento e indicadores periódicos
	12	Manutenção de dashboards e painéis gerenciais de visibilidade
	13	Análise de campanhas maliciosas e tentativas de exploração direcionadas
	14	Revisão e melhoria contínua da capacidade de detecção (casos de uso)
Serviço de Conscientização em Segurança da Informação		
Grupo de Serviço	ID	Serviço
05	1	Planejamento programa de conscientização em segurança da informação
	2	Execução de campanhas educativas recorrentes
	3	Criação e distribuição de materiais informativos (cartilhas, guias, e-mails e folders)
	4	Realização de palestras e workshops presenciais e/ou remotos
	5	Aplicação de treinamentos periódicos sobre boas práticas de segurança
	6	Realização de campanhas de phishing simulado controlado
	7	Identificação de usuários com maior exposição ao risco
	8	Execução de ações corretivas e educativas direcionadas a públicos específicos
	9	Aplicação de avaliações e testes de assimilação de conteúdo
	10	Produção de relatórios de desempenho e engajamento das campanhas



Poder Judiciário

Conselho Nacional de Justiça

11	Geração de indicadores de maturidade do fator humano (human risk score)
12	Realização de campanhas temáticas
13	Divulgação de alertas e comunicados preventivos sobre ameaças atuais
14	Apoio na elaboração de conteúdos alinhados às políticas internas do CNJ
15	Emissão de relatórios gerenciais periódicos com recomendações de melhoria



Poder Judiciário

Conselho Nacional de Justiça

PREGÃO ELETRÔNICO N. 90012/2026

ANEXO II DO EDITAL

A) ESTIMATIVA DE PREÇOS

GRUPO 1					
ITEM	DESCRIÇÃO	UN.	QUANTIDADE	VALOR UNITÁRIO (R\$)	VALOR TOTAL (R\$)
1	Serviço de administração, operação e manutenção e atendimento a requisições	Mês	60	R\$ 110.921,23	R\$ 6.655.273,80
2	Serviço de gestão de vulnerabilidades	Mês	60	R\$ 64.665,54	R\$ 3.879.932,40
3	Serviço de gestão de incidentes de segurança (CSIRT - <i>Blue Team</i>)	Mês	60	R\$ 32.514,83	R\$ 1.950.889,80
4	Serviço de monitoramento e visibilidade de ataques cibernéticos	Mês	60	R\$ 47.713,06	R\$ 2.862.783,60
5	Serviço de Conscientização em Segurança da Informação	Mês	60	R\$ 18.962,57	R\$ 1.137.754,20
VALOR TOTAL ESTIMADO GRUPO 1				R\$ 16.486.633,80	



Poder Judiciário

Conselho Nacional de Justiça

ITEM	DESCRIÇÃO	UN.	QUANTIDADE	VALOR UNITÁRIO (R\$)	VALOR TOTAL (R\$)
6	Serviço de testes de invasão (Red Team)	Sistemas	80	R\$ 7.884,23	R\$ 630.738,40

VALOR TOTAL ESTIMADO	R\$ 17.117.372,20 (dezesete milhões, cento e dezesete mil, trezentos e setenta e dois reais e vinte centavos)
-----------------------------	--

B) PROPOSTA PREÇOS (MODELO)

ITE M	DESCRIÇÃO	UN.	QTD.	VALOR UNITÁRIO (R\$)	VALOR TOTAL (R\$)
(...)	(...)	(...)	(...)	(algarismo s)	(algarismos)



Poder Judiciário

Conselho Nacional de Justiça

PREGÃO ELETRÔNICO N. 90012/2026

ANEXO III DO EDITAL – MINUTA DO CONTRATO

CONTRATO ADMINISTRATIVO
CELEBRADO ENTRE A UNIÃO, POR
INTERMÉDIO DO CONSELHO NACIONAL
DE JUSTIÇA, E A EMPRESA
_____, **PARA OS FINS**
QUE ESPECIFICA (pregão eletrônico n.
90012/2026 - Processo
Administrativo/CNJ n. 04520/2025).

A **UNIÃO**, por intermédio do **CONSELHO NACIONAL DE JUSTIÇA (CNJ)**, sediado no Edifício Sede do CNJ, SAF SUL Quadra 2, CEP 70070-600, Brasília/DF, CNPJ n. 07.421.906/0001-29, doravante denominado **CONTRATANTE**, neste ato representado pelo Diretor-Geral, Bruno César de Oliveira Lopes, RG n. 5****5 COMAER/SP e CPF n. ***.5**.*7-**, no uso das atribuições conferidas pela Portaria n. 290, de 11 de outubro de 2022, e pelo art. 3º, inciso XI, alíneas “al”, da Portaria n. 112, de 4 de junho de 2010, e a empresa _____, com sede _____, CEP _____, telefone (____) _____, inscrita no CNPJ sob o n. _____, doravante denominada **CONTRATADA**, neste ato representada por seu _____, _____, RG n. _____ e CPF n. _____, considerando o julgamento do pregão Eletrônico CNJ N. 90012/2026, publicado no Diário Oficial da União do dia ____ de _____ de **2026**, e a respectiva homologação, conforme Despacho _____ do Processo n. 08126/2023, celebram o presente termo de contrato, observando-se as normas da Lei n. 14.133/2021, demais legislação aplicável e as cláusulas a seguir.



Poder Judiciário

Conselho Nacional de Justiça

DO OBJETO

CLÁUSULA PRIMEIRA – Constitui objeto do presente contrato a contratação de Serviços Gerenciados de Segurança da Informação, observados o edital da licitação, o Termo de Referência, a proposta da **CONTRATADA**, e eventuais anexos dos documentos supracitados, os quais, independentemente de transcrição, são parte integrante deste instrumento e serão observados naquilo que não o contrarie.

Parágrafo único – Objeto da contratação:

ITEM	ESPECIFICAÇÃO	CATSER	UNIDADE DE MEDIDA	QUANT IDADE	VALOR UNITÁRIO	VALOR TOTAL
1						
2						
...						

DA VIGÊNCIA

CLÁUSULA SEGUNDA - O prazo de vigência da contratação é de 60 (sessenta) meses contados da data do início da prestação dos serviços, prorrogável por até 10 anos, na forma dos arts. 106 e 107 da Lei n. 14.133/2021.

Parágrafo único - A prorrogação de que trata este item é condicionada ao ateste, pela autoridade competente, de que as condições e os preços permanecem vantajosos para a Administração, permitida a negociação com o contratado.



Poder Judiciário

Conselho Nacional de Justiça

DO REGIME DE EXECUÇÃO E GESTÃO CONTRATUAL

CLÁUSULA TERCEIRA – O regime de execução será por empreitada por preço unitário.

Parágrafo único - O modelo de gestão do objeto, compreendidos os prazos, as condições de entrega, recebimento e demais informações relativas à gestão, constam no Termo de Referência, parte integrante deste contrato.

DA SUBCONTRATAÇÃO

CLÁUSULA QUARTA - Não será admitida a subcontratação do objeto contratual.

DAS OBRIGAÇÕES DO CONTRATANTE

CLÁUSULA QUINTA – Constituem obrigações do **CONTRATANTE**:

- a) Exigir o cumprimento de todas as obrigações assumidas pela **CONTRATADA**, de acordo com o contrato e seus anexos;
- b) Receber o objeto no prazo e condições estabelecidas no Termo de Referência;
- c) Notificar a **CONTRATADA**, por escrito, sobre vícios, defeitos ou incorreções verificadas no objeto fornecido, para que seja por ele substituído, reparado ou corrigido, no total ou em parte, às suas expensas;
- d) Acompanhar e fiscalizar a execução do contrato e o cumprimento das obrigações pela **CONTRATADA**;
- e) Comunicar a empresa para emissão de nota fiscal no que pertinente à parcela incontroversa da execução do objeto, para efeito de liquidação e pagamento, quando houver controvérsia sobre a execução do objeto, quanto à dimensão, qualidade e quantidade, conforme o art. 143 da Lei n. 14.133/2021;
- f) Efetuar o pagamento à **CONTRATADA** do valor correspondente ao fornecimento do objeto, no prazo, forma e condições estabelecidas neste contrato;



Poder Judiciário

Conselho Nacional de Justiça

- g) Aplicar à **CONTRATADA** as sanções previstas na lei e neste contrato;
- h) Explicitamente emitir decisão sobre todas as solicitações e reclamações relacionadas à execução deste contrato, ressalvados requerimentos manifestamente impertinentes, meramente protelatórios ou de nenhum interesse para a boa execução do ajuste;
- i) Responder eventuais pedidos de reestabelecimento do equilíbrio econômico-financeiro feitos pela **CONTRATADA** no prazo máximo de 30 (trinta) dias.
- j) Não responder por quaisquer compromissos assumidos pela **CONTRATADA** com terceiros, ainda que vinculados à execução do contrato, bem como por qualquer dano causado a terceiros em decorrência de ato da **CONTRATADA**, de seus empregados, prepostos ou subordinados.
- k) Notificar os emitentes das garantias quanto ao início de processo administrativo para apuração de descumprimento de cláusulas contratuais.

DAS OBRIGAÇÕES DA CONTRATADA

CLÁUSULA SEXTA – Constituem obrigações da CONTRATADA:

- a) Cumprir todas as obrigações constantes deste contrato e em seus anexos, assumindo como exclusivamente seus os riscos e as despesas decorrentes da boa e perfeita execução do objeto;
- b) Responsabilizar-se pelos vícios e danos decorrentes do objeto, de acordo com o Código de Defesa do Consumidor (Lei n. 8.078/ 1990);
- c) Comunicar ao **CONTRATANTE**, no prazo máximo de 24 (vinte e quatro) horas que antecede a data da entrega do objeto, os motivos que impossibilitem o cumprimento do prazo previsto, com a devida comprovação;
- d) Atender às determinações regulares emitidas pelo fiscal ou gestor do contrato ou autoridade superior (art. 137, II, da Lei n. 14.133/2021) e prestar todo esclarecimento ou informação por eles solicitados;
- e) Reparar, corrigir, remover, reconstruir ou substituir, às suas expensas, no total ou em parte, no prazo fixado pelo fiscal do contrato, os bens nos quais se



Poder Judiciário

Conselho Nacional de Justiça

verificarem vícios, defeitos ou incorreções resultantes da execução ou dos materiais empregados;

- f) Responsabilizar-se pelos vícios e danos decorrentes da execução do objeto, bem como por todo e qualquer dano causado à Administração ou terceiros, não reduzindo essa responsabilidade a fiscalização ou o acompanhamento da execução contratual pelo contratante, que ficará autorizado a descontar dos pagamentos devidos ou da garantia, caso exigida, o valor correspondente aos danos sofridos;
- g) Responsabilizar-se pelo cumprimento de todas as obrigações trabalhistas, previdenciárias, fiscais, comerciais e as demais previstas em legislação específica, cuja inadimplência não transfere a responsabilidade ao contratante e não poderá onerar o objeto do contrato;
- h) Comunicar ao fiscal do contrato, no prazo de 24 (vinte e quatro) horas, qualquer ocorrência anormal ou acidente que interfira a execução do objeto;
- i) Paralisar, por determinação do **CONTRATANTE**, qualquer atividade que não esteja sendo executada de acordo com a boa técnica ou que ponha em risco a segurança de pessoas ou bens de terceiros.
- j) Manter durante toda a vigência do contrato, em compatibilidade com as obrigações assumidas, todas as condições exigidas para habilitação na licitação;
- k) Arcar com o ônus decorrente de eventual equívoco no dimensionamento dos quantitativos da proposta, inclusive quanto aos custos variáveis decorrentes de fatores futuros e incertos, devendo complementá-los, caso o previsto inicialmente na proposta não seja satisfatório para o atendimento do objeto, salvo em caso de evento arrolado no art. 124, II, d, da Lei n. 14.133/2021.
- l) Cumprir, além dos postulados legais vigentes de âmbito federal as normas de segurança do **CONTRATANTE**;
- m) Observar o Código de Conduta de Fornecedores de Bens e Serviços;



Poder Judiciário

Conselho Nacional de Justiça

- n) Observar a Resolução CNJ n. 400/2021 que dispõe sobre a política de sustentabilidade no Poder Judiciário;
- o) Assinar o Termo de Responsabilidade com o Código De Conduta De Fornecedores de Bens e Serviços do **CONTRATANTE**, conforme Portaria n. 18/2020, constante do modelo ANEXO B - Modelo de termo de responsabilidade e compromisso com o código de conduta para fornecedores de bens e serviços do Conselho Nacional De Justiça deste contrato;
- p) Assinar o Termo de Compromisso de Manutenção de Sigilo do **CONTRATANTE**, constante do modelo ANEXO C - Modelo de Termo de Compromisso de Manutenção de Sigilo;
- q) Demais obrigações previstas no Termo de Referência.

Parágrafo único - Quando não for possível a verificar a regularidade no SICAF, a **CONTRATADA** deverá entregar ao setor responsável pela fiscalização do contrato, junto à nota fiscal para fins de pagamento, os seguintes documentos: 1) prova de regularidade relativa à Seguridade Social; 2) certidão conjunta relativa aos tributos federais e à Dívida Ativa da União; 3) certidões que comprovem a regularidade junto à Fazenda Estadual ou Distrital do domicílio ou sede do contratado; 4) Certidão de Regularidade do FGTS (CRF); e 5) Certidão Negativa de Débitos Trabalhistas (CNDT);

DO VALOR

CLÁUSULA SÉTIMA – O valor total do presente contrato é de R\$ _____ (_____), conforme discriminado no Anexo A deste contrato.

Parágrafo primeiro – 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, taxa de administração, frete, seguro e outros necessários ao integral cumprimento.



Poder Judiciário

Conselho Nacional de Justiça

Parágrafo segundo - O valor acima é meramente estimativo, de forma que os pagamentos devidos a CONTRATADA dependerão dos quantitativos efetivamente fornecidos.

DO PAGAMENTO

CLÁUSULA OITAVA – O prazo para pagamento à **CONTRATADA** e demais condições a ele referentes encontram-se definidos no Termo de Referência, quando mantidas as condições iniciais de habilitação, e cumpridos os seguintes requisitos:

- a) Apresentação de nota fiscal de acordo com a legislação vigente à época da emissão (nota fiscal eletrônica, se for o caso), acompanhada de: prova de regularidade ante às Fazendas federal, estadual e municipal do domicílio ou sede da contratada, prova de regularidade ante à Seguridade Social CRF e CNDT; e
- b) Inexistência de fato impeditivo para o qual tenha concorrido a **CONTRATADA**.

Parágrafo primeiro. A nota fiscal apresentada em desacordo com o disposto neste edital, ou com qualquer circunstância que desaconselhe o pagamento, será devolvida à **CONTRATADA** e, nesse caso, o prazo será interrompido e reiniciado a partir da respectiva regularização;

Parágrafo segundo. Nenhum pagamento será efetuado à **CONTRATADA** enquanto pendente de liquidação qualquer obrigação. Esse fato não será gerador de direito a reajustamento de preços ou a atualização monetária;

Parágrafo terceiro. Os documentos de cobrança deverão ser entregues pela **CONTRATADA** no Protocolo Eletrônico do CNJ (<https://www.cnj.jus.br/formularios/protocolo-eletronico/>).

DO REAJUSTE

CLÁUSULA NONA – Após o interregno de um ano da data do orçamento estimado, e independentemente de pedido da **CONTRATADA**, os preços iniciais serão



Poder Judiciário

Conselho Nacional de Justiça

reajustados, mediante a aplicação, pelo **CONTRATANTE**, do Índice de Custos de Tecnologia da Informação (ICTI), exclusivamente para as obrigações iniciadas e concluídas após a ocorrência da anualidade.

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

Parágrafo segundo - 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.

Parágrafo terceiro - Nas aferições finais, o índice utilizado para reajuste será, obrigatoriamente, o definitivo.

Parágrafo quarto - 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.

Parágrafo quinto - 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.

Parágrafo sexto - O reajuste será realizado por apostilamento.

DO RECEBIMENTO

CLÁUSULA DÉCIMA – O objeto do presente contrato será recebido conforme especificações do Termo de Referência.

DA ATUALIZAÇÃO MONETÁRIA

CLÁUSULA ONZE – Ocorrendo atraso no pagamento para o qual não tenha concorrido a **CONTRATADA**, incidirá atualização monetária sobre o valor devido,



Poder Judiciário

Conselho Nacional de Justiça

pela variação acumulada do ICTI entre a data prevista para o pagamento e a data da efetiva realização.

DA DOTAÇÃO ORÇAMENTÁRIA

CLÁUSULA DOZE – A despesa decorrente deste contrato correrá à conta de recursos do Orçamento Geral da União, Programa de Trabalho 02.032.0033.21BH.5664 - "Controle da atuação administrativa e financeira do Poder Judiciário, do cumprimento dos deveres funcionais dos juízes e Gestão de Políticas Judiciárias", Natureza da Despesa: 3.3.90.40.11, tendo sido emitida a Nota de Empenho n. _____, datada de ____ de ____ de ____.

DA GARANTIA CONTRATUAL

CLÁUSULA TREZE - A **CONTRATADA** deverá apresentar garantia de até 5% (cinco por cento) do valor anual do contrato em uma das seguintes modalidades:

a) caução em dinheiro ou em títulos da dívida pública emitidos sob a forma escritural, mediante registro em sistema centralizado de liquidação e de custódia autorizado pelo Banco Central do Brasil (BCB), e avaliados por seus valores econômicos, conforme definido pelo Ministério da Economia;

b) seguro-garantia;

c) fiança bancária emitida por banco ou instituição financeira devidamente autorizada a operar no país pelo BCB;

d) título de capitalização custeado por pagamento único, com resgate pelo valor total.

Parágrafo primeiro - O prazo para apresentação da garantia pela contratada nas modalidades caução ou fiança bancária será de **até 10 (dez) dias úteis** contados da publicação do extrato do contrato na Imprensa Oficial, prorrogáveis por igual período, a critério da Administração.



Poder Judiciário

Conselho Nacional de Justiça

Parágrafo segundo - O prazo para apresentação na modalidade seguro-garantia será de um mês contado da data de homologação da licitação e anterior à assinatura do contrato.

Parágrafo terceiro - Após a homologação da licitação, o licitante terá o prazo de 30 (trinta) dias corridos, prorrogável por igual período, a critério da Administração, para encaminhar a comprovação do seguro-garantia e assinatura do contrato.

Parágrafo quarto - Quando a garantia for apresentada em dinheiro, ela será atualizada monetariamente conforme os critérios estabelecidos pela instituição bancária em que for realizado o depósito.

Parágrafo quinto - Quando a garantia for apresentada na modalidade seguro-garantia, a apólice deverá:

- a) ser expedida exclusivamente por qualquer das entidades controladas e fiscalizadas pela Superintendência de Seguros Privados (SUSEP);
- b) conter o número com que a apólice ou o endosso tenha sido registrado na SUSEP;
- c) não estar integrada por cláusula compromissória nem por previsão de instauração de júízo arbitral; e
- d) não poderá estabelecer franquias, participações obrigatórias do segurado (CNJ) e/ou prazo de carência.

Parágrafo sexto - Quando a garantia for apresentada na modalidade fiança bancária, o instrumento respectivo deverá ser expedido exclusivamente por entidade controlada e fiscalizada pelo BCB.

Parágrafo sétimo – Quando a garantia for apresentada na modalidade fiança bancária, a instituição financeira fiadora deverá ser domiciliada ou possuir agência no Distrito Federal e demonstrar possuir bens suficientes à garantia integral da fiança prestada, conforme art. 825 da Lei n. 10.406/2002. A carta de fiança deverá conter cláusula expressa de renúncia do fiador ao benefício de ordem previsto no art. 827



Poder Judiciário

Conselho Nacional de Justiça

da Lei n. 10.406/2002, conforme facultado pelo inciso I do art. 828 do mesmo diploma, e ser registrada no Registro de Títulos e Documentos, conforme previsto nos arts. 128, 129 e 130 da Lei n. 6.015/1973.

Parágrafo oitavo - A garantia, em qualquer modalidade, assegurará o pagamento de:

a) prejuízos advindos do não cumprimento do objeto contratado e do não adimplemento das demais obrigações nele previstas;

b) prejuízos causados ao contratante, decorrentes de culpa ou dolo durante a execução do contrato;

c) multas moratórias e punitivas aplicadas pelo contratante à contratada;

d) obrigações trabalhistas e previdenciárias de qualquer natureza, não adimplidas pela contratada, quando couber.

Parágrafo nono - Alterado o valor do contrato, fica a contratada obrigada a apresentar garantia complementar ou substituí-la, no mesmo percentual e modalidades constantes desta seção, em **até 10 (dez) dias úteis** contados da data de publicação do termo de aditamento na Imprensa Oficial ou da assinatura da apostila de repactuação.

Parágrafo dez - Prorrogado o prazo de vigência do contrato, fica a contratada obrigada a renovar a garantia, no mesmo percentual e modalidades constantes desta seção, em **até 10 (dez) dias úteis** contados da data de publicação do termo aditivo na Imprensa Oficial.

Parágrafo onze - A garantia apresentada em desacordo com os requisitos e coberturas previstas no contrato será devolvida à contratada, que disporá do prazo improrrogável de **10 (dez) dias úteis** para a regularização da pendência.



Poder Judiciário

Conselho Nacional de Justiça

DAS SANÇÕES

CLÁUSULA QUATORZE – Nos termos da Instrução Normativa CNJ n. 94/2023 e dos arts. 155, 156 e 162 da Lei n. 14.133/2021, comete infração administrativa a **CONTRATADA** que:

- a) der causa à inexecução parcial do contrato;
- b) der causa à inexecução parcial do contrato que cause grave dano à Administração ou ao funcionamento dos serviços públicos ou ao interesse coletivo;
- c) der causa à inexecução total do contrato;
- d) ensejar o retardamento da execução ou da entrega do objeto da contratação sem motivo justificado;
- e) apresentar documentação falsa ou prestar declaração falsa durante a execução do contrato;
- f) praticar ato fraudulento na execução do contrato;
- g) comportar-se de modo inidôneo ou cometer fraude de qualquer natureza;
- h) praticar ato lesivo previsto no art. 5º da Lei n. 12.846/2013.

Parágrafo primeiro – Serão aplicadas à **CONTRATADA** que incorrer nas infrações acima descritas as seguintes sanções:

- a) advertência, quando o contratado der causa à inexecução parcial do contrato, sempre que não se justificar a imposição de penalidade mais grave;
- b) **multa, nas condições e percentuais estabelecidos no Termo de Referência;**
- c) impedimento de licitar e contratar com a União e descredenciamento do SICAF, pelo prazo de até 3 (três) anos quando praticadas as condutas descritas nas alíneas “b”, “c” e “d” da cláusula quatorze deste contrato, sempre que não se justificar a imposição de penalidade mais grave;
- d) declaração de inidoneidade para licitar ou contratar, quando praticadas as condutas descritas nas alíneas “e”, “f”, “g” e “h” da cláusula quatorze deste



Poder Judiciário

Conselho Nacional de Justiça

contrato, bem como nas alíneas “b”, “c” e “d”, que justifiquem a imposição de penalidade mais grave.

Parágrafo segundo – O valor da multa, aplicada após o regular processo administrativo, será descontado de pagamentos eventualmente devidos pelo **CONTRATANTE** à **CONTRATADA** ou cobrado judicialmente.

Parágrafo terceiro – A aplicação das sanções previstas neste contrato não exclui, em hipótese alguma, a obrigação de reparação integral do dano causado ao **CONTRATANTE**.

Parágrafo quarto – Todas as sanções previstas neste contrato poderão ser aplicadas cumulativamente com a multa.

Parágrafo quinto – Se a multa aplicada e as indenizações cabíveis forem superiores ao valor do pagamento eventualmente devido pelo **CONTRATANTE** à **CONTRATADA**, além da perda desse valor, a diferença será descontada da garantia prestada ou cobrada judicialmente.

Parágrafo sexto - A aplicação das sanções realizar-se-á em processo administrativo que assegure o contraditório e a ampla defesa ao contratado, observando-se o procedimento previsto no **caput** e parágrafos do [art. 158 da Lei n. 14.133/2021](#), para as penalidades de impedimento de licitar e contratar e de declaração de inidoneidade para licitar ou contratar.

Parágrafo sétimo - Na aplicação das sanções serão considerados:

- a) a natureza e a gravidade da infração cometida;
- b) as peculiaridades do caso concreto;
- c) as circunstâncias agravantes ou atenuantes;
- d) os danos que dela provierem para o contratante;
- e) a implantação ou o aperfeiçoamento de programa de integridade, conforme normas e orientações dos órgãos de controle.



Poder Judiciário

Conselho Nacional de Justiça

Parágrafo oitavo - A personalidade jurídica do contratado poderá ser desconsiderada sempre que utilizada com abuso do direito para facilitar, encobrir ou dissimular a prática dos atos ilícitos previstos neste contrato ou para provocar confusão patrimonial, e, nesse caso, todos os efeitos das sanções aplicadas à pessoa jurídica serão estendidos aos seus administradores e sócios com poderes de administração, à pessoa jurídica sucessora ou à empresa do mesmo ramo com relação de coligação ou controle, de fato ou de direito, com o **CONTRATADO**, observados, em todos os casos, o contraditório, a ampla defesa e a obrigatoriedade de análise jurídica prévia.

Parágrafo nono - o **CONTRATANTE** deverá, no prazo máximo 15 (quinze) dias úteis, contado da data de aplicação da sanção, informar e manter atualizados os dados relativos às sanções por ela aplicadas, para fins de publicidade no Cadastro Nacional de Empresas Inidôneas e Suspensas (CEIS) e no Cadastro Nacional de Empresas Punidas (CNEP), instituídos no âmbito do Poder Executivo Federal.

Parágrafo dez - Excepcionalmente, desde que devidamente justificado no processo administrativo, o **CONTRATANTE** poderá efetuar a retenção do valor presumido da multa, e, concomitantemente, instaurar regular processo administrativo oportunizando à **CONTRATADA** o exercício do contraditório e da ampla defesa.

Parágrafo onze – Os instrumentos de requerimentos, de defesas prévias e de recursos eventualmente interpostos pela **CONTRATADA** deverão ser instruídos com os documentos hábeis à prova das alegações neles contidas. Referidos documentos probatórios deverão ser apresentados nas versões originais, podendo ser digitalizados, e/ou em versões reconhecidas por servidores da Administração Pública, sob pena de, a critério exclusivo do **CONTRATANTE**, não serem avaliados.

DA EXTINÇÃO DO CONTRATO

CLÁUSULA QUINZE – O inadimplemento de cláusula estabelecida neste contrato, por parte da **CONTRATADA**, assegurará ao **CONTRATANTE** o direito de rescindi-lo, mediante notificação, com prova de recebimento.



Poder Judiciário

Conselho Nacional de Justiça

CLÁUSULA DEZESSEIS – Além de outras hipóteses expressamente previstas no art. 137 da Lei n. 14.133/2021, constituem motivos para a extinção deste contrato:

- a) não cumprimento ou cumprimento irregular de normas editalícias ou de cláusulas contratuais, de especificações, de projetos ou de prazos;
- b) desatendimento das determinações regulares emitidas pela autoridade designada para acompanhar e fiscalizar sua execução ou por autoridade;
- c) alteração social ou modificação da finalidade ou da estrutura da **CONTRATADA** que restrinja sua capacidade de concluir o contrato; e
- d) decretação de falência ou de insolvência civil, dissolução da sociedade ou falecimento do contratado.

Parágrafo único – Caso a **CONTRATADA** venha a sofrer processos de fusão, cisão ou incorporação, será admitida a continuação deste contrato, desde que sua execução não seja afetada e que a **CONTRATADA** mantenha o fiel cumprimento dos termos contratuais e as condições de habilitação.

CLÁUSULA DEZESSETE – Ao **CONTRATANTE** é reconhecido o direito de extinção do contrato, nos termos do art. 137, § 2º, da Lei n. 14.133/2021, aplicando-se, no que couber, as disposições dos arts. 138 e 139 da referida lei.

Parágrafo primeiro - A extinção do contrato poderá ser consensual, por acordo entre as partes, por conciliação, por mediação ou por comitê de resolução de disputas, desde que haja interesse da Administração.

Parágrafo segundo - O contrato poderá ser rescindido antes do término final acordado, mediante notificação prévia à **CONTRATADA** com antecedência mínima de 30 (trinta) dias, em face da conclusão de procedimento licitatório contemplando o mesmo objeto do contrato.

Parágrafo terceiro - A extinção poderá ser determinada por decisão arbitral, em decorrência de cláusula compromissória ou compromisso arbitral, ou por decisão judicial.



Poder Judiciário

Conselho Nacional de Justiça

Parágrafo quarto - Os casos de extinção contratual serão formalmente motivados nos autos do processo, assegurado o contraditório e a ampla defesa.

CLÁUSULA DEZOITO – A **CONTRATANTE** poderá extinguir o contrato, sem ônus, quando não dispuser de créditos orçamentários para sua continuidade ou quando entender que o contrato não mais lhe oferece vantagem, conforme prerrogativa constante no inciso III, do art. 106, da Lei 14.133/2021.

DO ACOMPANHAMENTO E DA FISCALIZAÇÃO

CLÁUSULA DEZENOVE – O **CONTRATANTE** nomeará um gestor titular e um substituto para executar a fiscalização do contrato. As ocorrências serão registradas em relatório, cuja cópia será encaminhada à **CONTRATADA**, objetivando a imediata correção das irregularidades apontadas.

Parágrafo único – 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.

DOS CASOS OMISSOS

CLÁUSULA VINTE – Casos omissos ou situações não explicitadas nas cláusulas deste contrato serão decididos pelas partes, no que couber, segundo dispõem a Lei n. 14.133/2021, demais regulamentos e normas administrativas federais.

DAS ALTERAÇÕES

CLÁUSULA VINTE E UM- Eventuais alterações contratuais reger-se-ão pela disciplina dos arts. 124 e seguintes da Lei n. 14.133/2021.

Parágrafo primeiro - A **CONTRATADA** é obrigada a aceitar, nas mesmas condições contratuais, acréscimos ou supressões que se fizerem necessários, até o limite de 25% (vinte e cinco por cento) do valor inicial atualizado do contrato.



Poder Judiciário

Conselho Nacional de Justiça

Parágrafo segundo - Registros que não caracterizam alteração do contrato podem ser realizados por simples apostila, dispensada a celebração de termo aditivo, na forma do art. 136 da Lei n. 14.133/2021.

DA PUBLICIDADE

CLÁUSULA VINTE E DOIS - O extrato do presente contrato será divulgado no Portal Nacional de Contratações Públicas (PNCP), na forma do art. 94 da Lei n. 14.133/2021, e no sítio oficial do **CONTRATANTE**, em atenção ao art. 8º, §2º, da Lei n. 12.527/ 2011, c/c art. 7º, §3º, inciso V, do Decreto n. 7.724/2012.

DO FORO

CLÁUSULA VINTE E TRÊS – Para dirimir eventuais conflitos oriundos deste contrato que não puderem ser compostos pela conciliação, é eleito o foro da Justiça Federal – Seção Judiciária do Distrito Federal, conforme o art. 92, §1º, da Lei n. 14.133/2021.

Justas e contratadas, as partes assinam o presente instrumento na forma eletrônica, nos termos da Lei n. 14.133/2021 e da Instrução Normativa CNJ n. 67/2015.

Pelo **CONTRATANTE**

Bruno César de Oliveira Lopes

Diretor-Geral

Portaria n. 329/2025

Pela **CONTRATADA**



Poder Judiciário

Conselho Nacional de Justiça

ANEXO A DO CONTRATO N. ____/2026, CELEBRADO ENTRE A UNIÃO, POR INTERMÉDIO DO CONSELHO NACIONAL DE JUSTIÇA, E A EMPRESA _____, PARA OS FINS QUE ESPECIFICA (Pregão Eletrônico n. 90012/2026 – Processo Administrativo/CNJ n. 04520/2025).

VALOR DISCRIMINADO DO CONTRATO

Item	Descrição	Un.	Qtd.	Valor Unitário (R\$)	Valor Total (R\$)
...



Poder Judiciário

Conselho Nacional de Justiça

**ANEXO B DO CONTRATO N. ____/2026,
CELEBRADO ENTRE A UNIÃO, POR
INTERMÉDIO DO CONSELHO NACIONAL
DE JUSTIÇA, E A EMPRESA
_____, PARA OS FINS QUE
ESPECIFICA (Pregão Eletrônico n.
90012/2026 - Processo Administrativo/CNJ
n. 04520/2025).**

**TERMO DE RESPONSABILIDADE E COMPROMISSO COM O CÓDIGO DE
CONDUTA PARA FORNECEDORES DE BENS E SERVIÇOS DO CONSELHO
NACIONAL DE JUSTIÇA**

Eu, _____, inscrito(a) no CPF sob n. _____, neste ato representando o(a) _____, inscrito(a) no CNPJ n. _____, declaro: Ter recebido cópia do Código de Conduta para Fornecedores de Bens e de Serviços do Conselho Nacional de Justiça; ter conhecimento do inteiro teor do referido Código e estar de pleno acordo com o seu conteúdo, que li e entendi, comprometendo-me a cumpri-lo fielmente durante toda a vigência de meu contrato e, após, no que for cabível; ter conhecimento de que, para fornecer serviços, bens e produtos ou estabelecer qualquer tipo de parceria com o Conselho Nacional de Justiça, é necessário respeitar fielmente o presente Código, cujas avaliações quanto ao cumprimento serão objeto de cláusula(s) contratual(ais); ter conhecimento de que as infrações a este Código, às políticas e normas do Conselho Nacional de Justiça serão analisadas, mediante a apresentação de relatórios, documentos, disponibilização de acesso a sistemas informatizados, vistorias, na forma que forem estabelecidas nas cláusulas contratuais, estando sujeitas à não prorrogação dos contratos administrativos e às ações aplicáveis, sem



Poder Judiciário

Conselho Nacional de Justiça

prejuízo de encaminhamento aos órgãos responsáveis pela apuração dos fatos e aplicação das penalidades cabíveis.

_____, _____ de _____ de _____



Poder Judiciário

Conselho Nacional de Justiça

**ANEXO C DO CONTRATO N. ____/2026,
CELEBRADO ENTRE A UNIÃO, POR
INTERMÉDIO DO CONSELHO NACIONAL
DE JUSTIÇA, E A EMPRESA
_____, PARA OS FINS QUE
ESPECIFICA (Pregão Eletrônico n.
90012/2026 - Processo Administrativo/CNJ
n. 04520/2025).**

TERMO DE COMPROMISSO DE SIGILO E NORMAS DE SEGURANÇA

O <<ÓRGÃO>>, sediado na XXXXXX, CEP: XXXXXXXX, CNPJ n. XXXX/XXXX-XX doravante denominado CONTRATANTE, e, de outro lado, a <NOME DA EMPRESA>, sediada em <ENDEREÇO>, CNPJ n. <CNPJ>, doravante denominada CONTRATADA;

CONSIDERANDO que, em razão do CONTRATO N. XX/20XX doravante denominado CONTRATO PRINCIPAL, a CONTRATADA poderá ter acesso a informações sigilosas do CONTRATANTE;

CONSIDERANDO a necessidade de ajustar as condições de revelação destas informações sigilosas, bem como definir as regras para o seu uso e proteção;

CONSIDERANDO o disposto na Política de Segurança da Informação do CONTRATANTE;

Resolvem celebrar o presente TERMO DE COMPROMISSO DE MANUTENÇÃO DE SIGILO, doravante TERMO, vinculado ao CONTRATO PRINCIPAL, mediante as seguintes cláusulas e condições:

Cláusula Primeira – DO OBJETO

Constitui objeto deste TERMO o estabelecimento de condições específicas para regulamentar as obrigações a serem observadas pela CONTRATADA, no que diz



Poder Judiciário

Conselho Nacional de Justiça

respeito ao trato de informações sensíveis e sigilosas, disponibilizadas pelo CONTRATANTE, por força dos procedimentos necessários para a execução do objeto do CONTRATO PRINCIPAL celebrado entre as partes e em acordo com o que dispõe o Decreto n. 7.845/2012 - Salvaguarda de dados, informações, documentos e materiais sigilosos de interesse da segurança da sociedade e do Estado.

Cláusula Segunda – DOS CONCEITOS E DEFINIÇÕES

Para os efeitos deste TERMO, são estabelecidos os seguintes conceitos e definições:

Informação: conjunto de dados organizados de acordo com procedimentos executados por meios eletrônicos ou não, que possibilitam a realização de atividades específicas e/ou tomada de decisão.

Informação Pública ou Ostensiva: aquelas cujo acesso é irrestrito, obtida por divulgação pública ou por meio de canais autorizados pelo CONTRATANTE.

Informações Sensíveis: todos os conhecimentos estratégicos que, em função de seu potencial no aproveitamento de oportunidades ou desenvolvimento nos ramos econômicos, político, científico, tecnológico, militar e social, possam beneficiar a Sociedade e o Estado brasileiros.

DECLARAÇÃO DE CIÊNCIA DO TERMO DE COMPROMISSO DE MANUTENÇÃO DE SIGILO

PREGÃO ELETRÔNICO N. 00X/20XX

DECLARAÇÃO DE CIÊNCIA DE TCMS

Por meio desta, o(a) Sr(a) [nome do(a) diretor, consultor, prestador de serviço, empregado ou preposto], CPF _____, ocupante do cargo [cargo que



Poder Judiciário

Conselho Nacional de Justiça

ocupa] na empresa [Nome (Razão Social) da empresa], CNPJ [número do CNPJ da empresa], declara sob as penas da Lei, ter tomado conhecimento do TERMO DE COMPROMISSO DE MANUTENÇÃO DE SIGILO (TCMS), emitido por ocasião da assinatura do contrato n. ____/20__, e se compromete a seguir, naquilo que lhe couber, todas as disposições do referido Termo.

Local e data

Assinatura