PREGÃO ELETRÔNICO

118/2026

CONSELHO NACIONAL DE DESENVOLVIMENTO CIENTÍFICO E TECNOLÓGICO – CNPq (364102)

OBJETO

Aquisição de solução corporativa de Application Delivery Controller (ADC), baseada na plataforma F5 BIG-IP, com funcionalidades integradas de Web Application Firewall (WAF), a ser instalada em ambiente on-premise no data center do CNPq, contemplando o fornecimento dos appliances, das licenças de software F5 BIG-IP, da garantia e do suporte técnico oficial do fabricante, das subscrições e assinaturas de segurança da solução, bem como dos serviços especializados de instalação, configuração e implantação, dos serviços de suporte técnico especializado da contratada em regime 24x7 e dos serviços de consultoria técnica especializada sob demanda, pelo prazo de 60 (sessenta) meses, conforme condições e exigências estabelecidas no Termo de Referência.

VALOR TOTAL DA CONTRATAÇÃO

R$ 6.046.270,63 (seis milhões, quarenta e seis mil duzentos e setenta reais e sessenta e três centavos).

DATA DA SESSÃO PÚBLICA

Dia **22/09/2026** às **14h30 (horário de Brasília)**

CRITÉRIO DE JULGAMENTO:

menor preço por grupo

MODO DE DISPUTA:

aberto e fechado

Baixe o APP Compras.gov.br
e apresente sua proposta!

TRATAMENTO FAVORECIDO ME/EPP/EQUIPARADAS

NÃO

MARGEM DE PREFERÊNCIA PARA ALGUM ITEM

NÃO

Câmara Nacional de Modelos de Licitações e Contratos da Consultoria-Geral da União
Modelo de Edital - Pregão e Concorrência - TIC - Lei nº 14.133, de 2021.
Aprovado pela Secretaria de Governo Digital
Identidade visual pela Secretaria de Gestão e Inovação
Atualização: ABR/2026

Sumário

1. DO OBJETO 4
2. DA PARTICIPAÇÃO NA LICITAÇÃO 4
3. DO ORÇAMENTO ESTIMADO 6
4. DA APRESENTAÇÃO DA PROPOSTA E DOS DOCUMENTOS DE HABILITAÇÃO 6
5. DO PREENCHIMENTO DA PROPOSTA 7
6. DA ABERTURA DA SESSÃO, CLASSIFICAÇÃO DAS PROPOSTAS E FORMULAÇÃO DE LANCES . 8
7. DA FASE DE JULGAMENTO 11
8. DA FASE DE HABILITAÇÃO 12
9. DO TERMO DE CONTRATO 15
10. DOS RECURSOS 15
11. DAS INFRAÇÕES ADMINISTRATIVAS E SANÇÕES 16
12. DA IMPUGNAÇÃO AO EDITAL E DO PEDIDO DE ESCLARECIMENTO 18
13. DAS DISPOSIÇÕES GERAIS 19

Câmara Nacional de Modelos de Licitações e Contratos da Consultoria-Geral da União
Modelo de Edital - Pregão e Concorrência - TIC - Lei nº 14.133, de 2021.
Aprovado pela Secretaria de Governo Digital
Identidade visual pela Secretaria de Gestão e Inovação
Atualização: ABR/2026

EDITAL – SOLUÇÃO DE TECNOLOGIA DA INFORMAÇÃO E COMUNICAÇÃO

CONSELHO NACIONAL DE DESENVOLVIMENTO CIENTÍFICO E TECNOLÓGICO - CNPq

PREGÃO ELETRÔNICO Nº 118/2026
(Processo Administrativo n° 01300.003396/2025-91)

Torna-se público que o CONSELHO NACIONAL DE DESENVOLVIMENTO CIENTÍFICO E TECNOLÓGICO - CNPq, por meio do Serviço de Compras e Licitações – SELIC, sediado no Setor de Autarquias Sul (SAUS), Quadra 01, Lote 06, Bloco H, Edifício Telemundi II, Bairro Asa Sul, Brasília/DF - CEP: 70.070-010, realizará licitação, , na modalidade **PREGÃO ELETRÔNICO**, na forma ELETRÔNICA, nos termos da Lei nº 14.133, de 1º de abril de 2021, , e demais legislação aplicável e, ainda, de acordo com as condições estabelecidas neste Edital.

1. DO OBJETO

1.1. O objeto da presente licitação é a contratação de solução de tecnologia da informação e comunicação de aquisição de solução corporativa de Application Delivery Controller (ADC), baseada na plataforma F5 BIG-IP, com funcionalidades integradas de Web Application Firewall (WAF), a ser instalada em ambiente on-premise no data center do CNPq, contemplando o fornecimento dos appliances, das licenças de software F5 BIG-IP, da garantia e do suporte técnico oficial do fabricante, das subscrições e assinaturas de segurança da solução, bem como dos serviços especializados de instalação, configuração e implantação, dos serviços de suporte técnico especializado da contratada em regime 24x7 e dos serviços de consultoria técnica especializada sob demanda, pelo prazo de 60 (sessenta) meses**,** conforme condições, quantidades e exigências estabelecidas neste Edital e seus anexos.

1.2. A licitação será realizada em grupo único, formados por 7 itens, conforme tabela constante no Termo de Referência, devendo o licitante oferecer proposta para todos os itens que o compõem.

2. DA PARTICIPAÇÃO NA LICITAÇÃO

2.1. Poderão participar deste certame os interessados que estiverem previamente credenciados no Sistema de Cadastramento Unificado de Fornecedores - SICAF e no Sistema de Compras do Governo Federal (www.gov.br/compras).

2.2. Os interessados deverão atender às condições exigidas no cadastramento no Sicaf até o terceiro dia útil anterior à data prevista para recebimento das propostas.

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 relacionados no item anterior e mantê-los atualizados junto aos órgãos responsáveis pela informação, devendo proceder, imediatamente, à correção ou à alteração dos registros tão logo identifique incorreção ou aqueles se tornem desatualizados.

Câmara Nacional de Modelos de Licitações e Contratos da Consultoria-Geral da União
Modelo de Edital - Pregão e Concorrência - TIC - Lei nº 14.133, de 2021.
Aprovado pela Secretaria de Governo Digital
Identidade visual pela Secretaria de Gestão e Inovação
Atualização: ABR/2026

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

2.6. Não poderão disputar esta licitação:

2.6.1 aquele que não atenda às condições deste Edital e seu(s) anexo(s);

2.6.2 sociedade que desempenhe atividade incompatível com o objeto da licitação;

2.6.3 empresas estrangeiras que não tenham representação legal no Brasil com poderes expressos para receber citação e responder administrativa ou judicialmente;

2.6.4 autor do anteprojeto, do projeto básico ou do projeto executivo, pessoa física ou jurídica, quando a licitação versar sobre serviços ou fornecimento de bens a ele relacionados;

2.6.5 empresa, isoladamente ou em consórcio, responsável pela elaboração do projeto básico ou do projeto 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 serviços ou fornecimento de bens a ela necessários;

2.6.6 pessoa física ou jurídica que se encontre, ao tempo da licitação, impossibilitada de participar da licitação em decorrência de sanção que lhe foi imposta;

2.6.7 aquele que mantenha vínculo de natureza técnica, comercial, econômica, financeira, trabalhista ou civil com dirigente do órgão ou entidade contratante ou com agente público que desempenhe função na licitação ou 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;

2.6.8 empresas controladoras, controladas ou coligadas, nos termos da Lei nº 6.404, de 15 de dezembro de 1976, concorrendo entre si;

2.6.9 pessoa física ou jurídica que, nos 5 (cinco) anos anteriores à divulgação do edital, tenha sido condenada judicialmente, com trânsito em julgado, por exploração de trabalho infantil, por submissão de trabalhadores a condições análogas às de escravo ou por contratação de adolescentes nos casos vedados pela legislação trabalhista;

2.6.10 Organizações da Sociedade Civil de Interesse Público - OSCIP, atuando nessa condição;

2.6.11 pessoas físicas.

2.7. 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 nº 14.133, de 2021.

2.8. O impedimento de que trata o item 2.6.6 será também aplicado ao licitante que atue em substituição a outra pessoa, física ou jurídica, com o intuito de burlar a efetividade da sanção a ela aplicada, inclusive a sua controladora, controlada ou coligada, desde que devidamente comprovado o ilícito ou a utilização fraudulenta da personalidade jurídica do licitante.

2.9. A critério da Administração e exclusivamente a seu serviço, o autor dos projetos e a empresa a que se referem os itens 2.6.4 e 2.6.5 poderão participar no apoio das atividades de planejamento da contratação, de execução da licitação ou de gestão do contrato, desde que sob supervisão exclusiva de agentes públicos do órgão ou entidade.

2.10. Equiparam-se aos autores do projeto as empresas integrantes do mesmo grupo econômico.

2.11. O disposto nos itens 2.6.4 e 2.6.5 não impede a licitação ou a contratação de serviço que inclua como encargo do contratado a elaboração do projeto básico e do projeto executivo, nas contratações integradas, e do projeto executivo, nos demais regimes de execução.

Câmara Nacional de Modelos de Licitações e Contratos da Consultoria-Geral da União
Modelo de Edital - Pregão e Concorrência - TIC - Lei nº 14.133, de 2021.
Aprovado pela Secretaria de Governo Digital
Identidade visual pela Secretaria de Gestão e Inovação
Atualização: ABR/2026

2.12. Em licitações e contratações realizadas no âmbito de projetos e programas parcialmente financiados por agência oficial de cooperação estrangeira ou por organismo financeiro internacional com recursos do financiamento ou da contrapartida nacional, não poderá participar pessoa física ou jurídica que integre o rol de pessoas sancionadas por essas entidades ou que seja declarada inidônea nos termos da Lei nº 14.133, de 2021.

2.13. A vedação de que trata o item 2.7 estende-se a terceiro que auxilie a condução da contratação na qualidade de integrante de equipe de apoio, profissional especializado ou funcionário ou representante de empresa que preste assessoria técnica.

3. DO ORÇAMENTO ESTIMADO

3.1. O orçamento estimado da presente contratação não será de caráter sigiloso.

4. DA APRESENTAÇÃO DA PROPOSTA E DOS DOCUMENTOS DE HABILITAÇÃO

4.1. Na presente licitação, a fase de habilitação sucederá as fases de apresentação de propostas e lances e de julgamento.

4.2. Os licitantes encaminharão, exclusivamente por meio do sistema eletrônico, a proposta com o preço ou o percentual de desconto, conforme o critério de julgamento adotado neste Edital, até a data e o horário estabelecidos para abertura da sessão pública.

4.3. Caso a fase de habilitação anteceda as fases de apresentação de propostas e lances, os licitantes encaminharão, na forma e no prazo estabelecidos no item anterior, simultaneamente os documentos de habilitação e a proposta com o preço ou o percentual de desconto, observado o disposto nos itens 8.1.1 e 8.13.2 deste Edital.

4.4. No cadastramento da proposta inicial, o licitante declarará, em campo próprio do sistema, que:

4.4.1. está ciente e concorda com as condições contidas no edital e seus anexos, bem como de que a proposta apresentada compreende a integralidade dos custos para atendimento dos direitos trabalhistas assegurados na Constituição Federal, nas leis trabalhistas, nas normas infralegais, nas convenções coletivas de trabalho e nos termos de ajustamento de conduta vigentes na data de sua entrega em definitivo e que cumpre plenamente os requisitos de habilitação definidos no instrumento convocatório;

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

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

4.4.4. cumpre as exigências de reserva de cargos para pessoa com deficiência e para reabilitado da Previdência Social, previstas em lei e em outras normas específicas.

4.5. O licitante organizado em cooperativa deverá declarar, ainda, em campo próprio do sistema eletrônico, que cumpre os requisitos estabelecidos no artigo 16 da Lei nº 14.133, de 2021.

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

4.5.2. .

4.6. O licitante deverá declarar em campo próprio do sistema que desenvolve programa de integridade, nos termos do Decreto nº 12.304, de 2024, e da Portaria Normativa SE/CGU nº 226, de 9 de setembro de 2025, para fazer jus ao benefício do critério de desempate previsto no art. 60, caput, inciso IV, da Lei nº 14.133, de 2021.

4.7. A falsidade da declaração de que trata o item 4.4, ou 4.6 sujeitará o licitante às sanções previstas na Lei nº 14.133, de 2021, e neste Edital.

4.8. Os licitantes poderão retirar ou substituir a proposta ou, na hipótese de a fase de habilitação anteceder as fases de apresentação de propostas e lances e de julgamento, os documentos de habilitação anteriormente inseridos no sistema, até a abertura da sessão pública.

4.9. Não haverá ordem de classificação na etapa de apresentação da proposta e dos documentos de habilitação pelo licitante, o que ocorrerá somente após os procedimentos de abertura da sessão pública e da fase de envio de lances.

4.10. Serão disponibilizados para acesso público os documentos que compõem a proposta dos licitantes convocados para apresentação de propostas, após a fase de envio de lances.

4.11. Desde que disponibilizada a funcionalidade no sistema, o licitante poderá parametrizar o seu valor final mínimo ou o seu percentual de desconto máximo quando do cadastramento da proposta e obedecerá às seguintes regras:

4.11.1. a aplicação do intervalo mínimo de diferença de valores entre os lances, que incidirá tanto em relação aos lances intermediários quanto em relação ao lance que cobrir a melhor oferta; e

4.11.2. os lances serão de envio automático pelo sistema, respeitado o valor final mínimo, caso estabelecido, e o intervalo de que trata o subitem acima.

4.12. O valor final mínimo parametrizado no sistema poderá ser alterado pelo fornecedor durante a fase de disputa, sendo vedado:

4.12.1. valor superior a lance já registrado pelo fornecedor no sistema, quando adotado o critério de julgamento por menor preço; e

4.13. O valor final mínimo parametrizado na forma do item 4.11 possuirá caráter sigiloso para os demais fornecedores e para o órgão ou entidade promotora da licitação, podendo ser disponibilizado estrita e permanentemente aos órgãos de controle externo e interno.

4.14. Caberá ao licitante interessado em participar da licitação acompanhar as operações no sistema eletrônico durante o processo licitatório e se responsabilizar pelo ônus decorrente da perda de negócios diante da inobservância de mensagens emitidas pela Administração ou de sua desconexão.

4.15. O licitante deverá comunicar imediatamente ao provedor do sistema qualquer acontecimento que possa comprometer o sigilo ou a segurança, para imediato bloqueio de acesso.

5. DO PREENCHIMENTO DA PROPOSTA

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

5.1.1. valor, unitário e total do item;

5.1.2. Marca;

5.1.3. Fabricante;

5.2. Todas as especificações do objeto contidas na proposta vinculam o licitante.

5.3. Nos valores propostos estarão inclusos todos os custos operacionais, encargos previdenciários, trabalhistas, tributários, comerciais e quaisquer outros que incidam direta ou indiretamente na execução do objeto.

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

5.5. Se o regime tributário da empresa implicar o recolhimento de tributos em percentuais variáveis, a cotação adequada será a que corresponde à média dos efetivos recolhimentos da empresa nos últimos doze meses.

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

5.7. Na presente licitação, a Microempresa e a Empresa de Pequeno Porte poderão se beneficiar do regime de tributação pelo Simples Nacional.

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

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

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

5.11. Caso o critério de julgamento seja o de menor preço, os licitantes devem respeitar os preços máximos previstos no Termo de Referência/Projeto Básico;

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

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

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

6.2. Os licitantes poderão retirar ou substituir a proposta ou os documentos de habilitação, quando for o caso, anteriormente inseridos no sistema, até a abertura da sessão pública.

6.3. O sistema disponibilizará campo próprio para troca de mensagens entre o Pregoeiro/Agente de Contratação/Comissão e os licitantes.

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

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

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

Câmara Nacional de Modelos de Licitações e Contratos da Consultoria-Geral da União
Modelo de Edital - Pregão e Concorrência - TIC - Lei nº 14.133, de 2021.
Aprovado pela Secretaria de Governo Digital
Identidade visual pela Secretaria de Gestão e Inovação
Atualização: ABR/2026

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

6.8. O intervalo mínimo de diferença de valores entre os lances, que incidirá tanto em relação aos lances intermediários quanto em relação à proposta que cobrir a melhor oferta deverá ser de R$ 0,20 (vinte centavos).

6.9. 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.

6.10. O procedimento seguirá de acordo com o modo de disputa adotado.

6.11. Caso seja adotado para o envio de lances o modo de disputa “aberto e fechado”, os licitantes apresentarão lances públicos e sucessivos, com lance final e fechado.

6.11.1. A etapa de lances da sessão pública terá duração inicial de quinze minutos. Após esse prazo, o sistema encaminhará aviso de fechamento iminente dos lances, após o que transcorrerá o período de até dez minutos, aleatoriamente determinado, findo o qual será automaticamente encerrada a recepção de lances.

6.11.2. Encerrado o prazo previsto no subitem anterior, o sistema abrirá oportunidade para que o autor da oferta de valor mais baixo e os das ofertas com preços até 10% (dez por cento) superiores àquela possam ofertar um lance final e fechado em até cinco minutos, o qual será sigiloso até o encerramento deste prazo.

6.11.3. No procedimento de que trata o subitem supra, o licitante poderá optar por manter o seu último lance da etapa aberta, ou por ofertar melhor lance.

6.11.4. Não havendo pelo menos três ofertas nas condições definidas neste item, poderão os autores dos melhores lances subsequentes, na ordem de classificação, até o máximo de três, oferecer um lance final e fechado em até cinco minutos, o qual será sigiloso até o encerramento deste prazo.

6.12. Após o término dos prazos estabelecidos nos subitens anteriores, o sistema ordenará e divulgará os lances segundo a ordem crescente de valores.

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

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

6.15. No caso de desconexão com o Pregoeiro/Agente de Contratação/Comissão, no decorrer da etapa competitiva da licitação, o sistema eletrônico poderá permanecer acessível aos licitantes para a recepção dos lances.

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

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

6.18. 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.

6.19. Havendo eventual empate entre propostas ou lances, o critério de desempate será aquele previsto no art. 60 da Lei nº 14.133, de 2021, nesta ordem:

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

Câmara Nacional de Modelos de Licitações e Contratos da Consultoria-Geral da União
Modelo de Edital - Pregão e Concorrência - TIC - Lei nº 14.133, de 2021.
Aprovado pela Secretaria de Governo Digital
Identidade visual pela Secretaria de Gestão e Inovação
Atualização: ABR/2026

6.19.1.2. avaliação do desempenho contratual prévio dos licitantes, para a qual deverão preferencialmente ser utilizados registros cadastrais para efeito de atesto de cumprimento de obrigações previstos nesta Lei;

6.19.1.3. desenvolvimento pelo licitante de ações de equidade entre homens e mulheres no ambiente de trabalho, nos termos do Decreto nº 11.430, de 2023, e da Instrução Normativa SEGES/MGI nº 382, de 17 de setembro de 2025;

6.19.1.4. declaração do licitante de que desenvolve programa de integridade, conforme Decreto n° 12.304, de 2024, e Portaria Normativa SE/CGU n° 226, de 9 de setembro de 2025.

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

6.19.2.1. empresas 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;

6.19.2.2. empresas brasileiras;

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

6.19.2.4. empresas que comprovem a prática de mitigação, nos termos da Lei nº 12.187, de 29 de dezembro de 2009.

6.20. Esgotados todos os demais critérios de desempate previstos em lei, a escolha do licitante vencedor ocorrerá por sorteio, em ato público, para o qual todos os licitantes serão convocados, vedado qualquer outro processo.

6.21. Encerrada a etapa de envio de lances da sessão pública, na hipótese da proposta do primeiro colocado permanecer acima do preço máximo ou inferior ao desconto definido para a contratação, o Pregoeiro/Agente de Contratação/Comissão poderá negociar condições mais vantajosas, após definido o resultado do julgamento.

6.21.1. Tratando-se de licitação em grupo, a contratação posterior de item específico do grupo exigirá prévia pesquisa de mercado e demonstração de sua vantagem para o órgão ou a entidade e serão observados como critério de aceitabilidade os preços unitários máximos definidos no Termo de Referência.

6.21.2. A negociação poderá ser feita com os demais licitantes, segundo a ordem de classificação inicialmente estabelecida, quando o primeiro colocado, mesmo após a negociação, for desclassificado em razão de sua proposta permanecer acima do preço máximo definido pela Administração.

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

6.21.4. O resultado da negociação será divulgado a todos os licitantes e anexado aos autos do processo licitatório.

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

6.21.6. É facultado ao Pregoeiro/Agente de Contratação/Comissão prorrogar o prazo estabelecido, a partir de solicitação fundamentada feita no chat pelo licitante, antes de findo o prazo.

6.22. Após a negociação do preço, o Pregoeiro/Agente de Contratação/Comissão iniciará a fase de aceitação e julgamento da proposta.

Câmara Nacional de Modelos de Licitações e Contratos da Consultoria-Geral da União
Modelo de Edital - Pregão e Concorrência - TIC - Lei nº 14.133, de 2021.
Aprovado pela Secretaria de Governo Digital
Identidade visual pela Secretaria de Gestão e Inovação
Atualização: ABR/2026

7. DA FASE DE JULGAMENTO

7.1. Encerrada a etapa de negociação, o Pregoeiro/Agente de Contratação/Comissão verificará se o licitante provisoriamente classificado em primeiro lugar atende às condições de participação no certame, conforme previsto no art. 14 da Lei nº 14.133, de 2021, legislação correlata e no item 2.6 do edital, especialmente quanto à existência de sanção que impeça a participação no certame ou a futura contratação, mediante a consulta aos seguintes cadastros:

7.1.1 SICAF;

7.1.2 Cadastro Nacional de Empresas Inidôneas e Suspensas – CEIS;

7.1.3 Cadastro Nacional de Empresas Punidas – CNEP e

7.1.4 Lista de licitantes inidôneos, mantida pelo Tribunal de Contas da União.

7.2. A consulta aos cadastros será realizada no nome e no CNPJ da empresa licitante.

7.2.1 A consulta no CEIS quanto às sanções previstas na Lei nº 8.429, de 1992, também ocorrerá no nome e no CPF do sócio majoritário da empresa licitante, se houver, por força do art. 12 da citada lei.

7.3. Para a consulta de licitantes pessoa jurídica poderá haver a substituição das consultas ao CEIS, CNEP e Lista de licitantes inidôneos pela Consulta Consolidada de Pessoa Jurídica do TCU.

7.4. Caso conste na Consulta de Situação do licitante a existência de Ocorrências Impeditivas Indiretas, o Pregoeiro/Agente de Contratação/Comissão diligenciará para verificar se houve fraude por parte das empresas apontadas no Relatório de Ocorrências Impeditivas Indiretas.

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

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

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

7.5. Na hipótese de inversão das fases de habilitação e julgamento, caso atendidas as condições de participação, será iniciado o procedimento de habilitação.

7.6. Será desclassificada a proposta vencedora que:

7.6.1. contiver vícios insanáveis;

7.6.2. não obedecer às especificações técnicas contidas no Termo de Referência;

7.6.3. apresentar preços inexequíveis ou permanecerem acima do preço máximo definido para a contratação;

7.6.4. não tiverem sua exequibilidade demonstrada, quando exigido pela Administração;

7.6.5. não cumpra os critérios de aceitabilidade de preços definidos no Termo de Referência;

7.6.6. apresentar desconformidade com quaisquer outras exigências deste Edital ou seus anexos, desde que insanável.

7.7. No caso de bens e serviços em geral, é indício de inexequibilidade das propostas valores inferiores a 50% (cinquenta por cento) do valor orçado pela Administração.

7.8. A inexequibilidade, na hipótese de que trata o item anterior, só será considerada após diligência do Pregoeiro/Agente de Contratação/Comissão, que comprove:

7.8.1.1. que o custo do licitante ultrapassa o valor da proposta; e

Câmara Nacional de Modelos de Licitações e Contratos da Consultoria-Geral da União
Modelo de Edital - Pregão e Concorrência - TIC - Lei nº 14.133, de 2021.
Aprovado pela Secretaria de Governo Digital
Identidade visual pela Secretaria de Gestão e Inovação
Atualização: ABR/2026

7.8.1.2. inexistirem custos de oportunidade capazes de justificar o vulto da oferta.

7.9. Se houver indícios de inexequibilidade da proposta de preço, ou em caso da necessidade de esclarecimentos complementares, poderão ser efetuadas diligências, para que a empresa comprove a exequibilidade da proposta.

7.10. Caso o custo global estimado do objeto licitado tenha sido decomposto em seus respectivos custos unitários por meio de Planilha de Custos e Formação de Preços elaborada pela Administração, o licitante classificado em primeiro lugar será convocado para apresentar Planilha por ele elaborada, com os respectivos valores adequados ao valor final da sua proposta, sob pena de não aceitação da proposta.

7.11. Erros no preenchimento da planilha não constituem motivo para a desclassificação da proposta. A planilha poderá ser ajustada pelo fornecedor, no prazo indicado pelo sistema, desde que não haja majoração do preço e que se comprove que este é o bastante para arcar com todos os custos da contratação;

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

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

7.15. Caso o Termo de Referência exija a apresentação de carta de solidariedade emitida pelo fabricante, que assegure a execução do contrato, no caso de licitante revendedor ou distribuidor, o licitante classificado em primeiro lugar deverá apresentá-la, sob pena de não aceitação da proposta.

8. DA FASE DE HABILITAÇÃO

8.1. Os documentos previstos no Termo de Referência, necessários e suficientes para demonstrar a capacidade do licitante de realizar o objeto da licitação, serão exigidos para fins de habilitação, nos termos dos arts. 62 a 70 da Lei nº 14.133, de 2021.

8.1.1. A documentação exigida para fins de habilitação jurídica, fiscal, social e trabalhista e econômico-financeira, poderá ser substituída pelo registro cadastral no SICAF.

8.2. Quando permitida a participação de empresas estrangeiras que não funcionem no País, as exigências de habilitação serão atendidas mediante documentos equivalentes, inicialmente apresentados em tradução livre.

8.3. Na hipótese de o licitante vencedor ser empresa estrangeira que não funcione no País, para fins de assinatura do contrato ou da ata de registro de preços, os documentos exigidos para a habilitação serão traduzidos por tradutor juramentado no País e apostilados nos termos do disposto no Decreto nº 8.660, de 29 de janeiro de 2016, ou de outro que venha a substituí-lo, ou consularizados pelos respectivos consulados ou embaixadas.

8.4. Quando permitida a participação de consórcio de empresas, a habilitação técnica, quando exigida, será feita por meio do somatório dos quantitativos de cada consorciado e, para efeito de habilitação econômico-financeira, quando exigida, será observado o somatório dos valores de cada consorciado.

8.4.1. Se o consórcio não for formado integralmente por microempresas ou empresas de pequeno porte e o termo de referência exigir requisitos de habilitação econômico-financeira, haverá um acréscimo de 10% (dez por cento) para o consórcio em relação ao valor exigido para os licitantes individuais.

8.5. Os documentos exigidos para fins de habilitação poderão ser apresentados em original, por cópia ou por arquivo pdf, no sistema Compras.gov.

Câmara Nacional de Modelos de Licitações e Contratos da Consultoria-Geral da União
Modelo de Edital - Pregão e Concorrência - TIC - Lei nº 14.133, de 2021.
Aprovado pela Secretaria de Governo Digital
Identidade visual pela Secretaria de Gestão e Inovação
Atualização: ABR/2026

8.6. Os documentos exigidos para fins de habilitação poderão ser substituídos por registro cadastral emitido por órgão ou entidade pública, desde que o registro tenha sido feito em obediência ao disposto na Lei nº 14.133/2021.

8.7. Será verificado se o licitante apresentou declaração de que atende aos requisitos de habilitação, e o declarante responderá pela veracidade das informações prestadas, na forma da lei.

8.8. Será verificado se o licitante apresentou no sistema, sob pena de inabilitação, a declaração de que cumpre as exigências de reserva de cargos para pessoa com deficiência e para reabilitado da Previdência Social, previstas em lei e em outras normas específicas.

8.9. O licitante deverá apresentar, sob pena de desclassificação, declaração de que suas propostas econômicas compreendem a integralidade dos custos para atendimento dos direitos trabalhistas assegurados na Constituição Federal, nas leis trabalhistas, nas normas infralegais, nas convenções coletivas de trabalho e nos termos de ajustamento de conduta vigentes na data de entrega das propostas.

8.10. Considerando que na presente contratação a avaliação prévia do local de execução é imprescindível para o conhecimento pleno das condições e peculiaridades do objeto a ser contratado, o licitante deve atestar, sob pena de inabilitação, que conhece o local e as condições de realização do serviço, assegurado a ele o direito de realização de vistoria prévia.

8.10.1. O licitante que optar por realizar vistoria prévia terá disponibilizado pela Administração data e horário exclusivos, a ser agendado pelo e-mail: contratos_ti@cnpq.br, de modo que seu agendamento não coincida com o agendamento de outros licitantes.

8.10.2. A vistoria será realizada em dias úteis, de segunda a sexta-feira, no horário compreendido entre 09h00 (nove horas) e 17h00 (dezessete horas), sendo acompanhada por servidor designado pelo CNPq.

8.10.3. A vistoria será realizada nas dependências do Conselho Nacional de Desenvolvimento Científico e Tecnológico - CNPq, no seguinte endereço: Setor de Autarquias Sul (SAUS), Quadra 01, Lote 06, Bloco H – Edifício Telemundi II, Asa Sul, Brasília/DF, CEP 70070-010.

8.10.4. O representante da empresa deverá estar devidamente identificado, mediante apresentação de documento de identidade civil e comprovação de vínculo com a empresa interessada.

8.10.5. Quando realizada, a vistoria técnica será formalizada por meio de Termo de Vistoria Técnica, conforme modelo constante no Anexo V deste Termo de Referência, o qual deverá ser assinado pelo representante da empresa e pelo servidor designado pela CONTRATANTE.

8.10.6. Caso o licitante opte por não realizar vistoria, poderá substituir a declaração exigida no presente item por declaração formal assinada pelo seu responsável técnico acerca do conhecimento pleno das condições e peculiaridades da contratação, conforme modelo constante no Anexo VI (Termo de recusa de vistoria técnica).

8.10.7. A não realização da vistoria não poderá ser utilizada como justificativa para alegações posteriores de desconhecimento das condições do ambiente, das instalações ou das exigências necessárias à execução dos serviços, permanecendo sob responsabilidade exclusiva da CONTRATADA a adequada formulação de sua proposta.

8.11. A habilitação será verificada por meio do Sicaf, nos documentos por ele abrangidos.

8.11.1. Somente haverá a necessidade de comprovação do preenchimento de requisitos mediante apresentação dos documentos originais não-digitais quando houver dúvida em relação à integridade do documento digital ou quando a lei expressamente o exigir.

Câmara Nacional de Modelos de Licitações e Contratos da Consultoria-Geral da União
Modelo de Edital - Pregão e Concorrência - TIC - Lei nº 14.133, de 2021.
Aprovado pela Secretaria de Governo Digital
Identidade visual pela Secretaria de Gestão e Inovação
Atualização: ABR/2026

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

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

8.13. A verificação pelo Pregoeiro/Agente de Contratação/Comissão, em sítios eletrônicos oficiais de órgãos e entidades emissores de certidões constitui meio legal de prova, para fins de habilitação.

8.13.1. Os documentos exigidos para habilitação que não estejam contemplados no Sicaf serão enviados por meio do sistema, em formato digital, no prazo de 2 (duas) horas, prorrogável por igual período, contado da solicitação do Pregoeiro/Agente de Contratação/Comissão.

8.13.2. Na hipótese de a fase de habilitação anteceder a fase de apresentação de propostas e lances, os licitantes encaminharão, por meio do sistema, simultaneamente os documentos de habilitação e a proposta com o preço ou o percentual de desconto, observado o disposto no § 1º do art. 36 e no § 1º do art. 39 da Instrução Normativa SEGES nº 73, de 30 de setembro de 2022.

8.14. A verificação no Sicaf ou a exigência dos documentos nele não contidos somente será feita em relação ao licitante vencedor.

8.14.1. Os documentos relativos à regularidade fiscal que constem do Termo de Referência somente serão exigidos, em qualquer caso, em momento posterior ao julgamento das propostas, e apenas do licitante mais bem classificado.

8.14.2. Respeitada a exceção do subitem anterior, relativa à regularidade fiscal, quando a fase de habilitação anteceder as fases de apresentação de propostas e lances e de julgamento, a verificação ou exigência do presente subitem ocorrerá em relação a todos os licitantes.

8.15. Encerrado o prazo para envio da documentação de que trata o item 8.13.1, poderá ser admitida, mediante decisão fundamentada do Pregoeiro/Agente de Contratação, a apresentação de novos documentos de habilitação ou a complementação de informações acerca dos documentos já apresentados pelos licitantes, em até 2 (duas) horas, para:

8.15.1 a aferição das condições de habilitação do licitante, desde que decorrentes de fatos existentes à época da abertura do certame;

8.15.2 atualização de documentos cuja validade tenha expirado após a data de recebimento das propostas;

8.15.3 suprimento da ausência de documento de cunho declaratório emitido unilateralmente pelo licitante;

8.15.4 suprimento da ausência de certidão e/ou documento de cunho declaratório expedido por órgão ou entidade cujos atos gozem de presunção de veracidade e fé pública.

8.16. Findo o prazo assinalado sem o envio da nova documentação, restará preclusa essa oportunidade conferida ao licitante, implicando sua inabilitação.

8.17. Na análise dos documentos de habilitação, a comissão de contratação poderá sanar erros ou falhas, que não alterem a substância dos documentos e sua validade jurídica, mediante decisão fundamentada, registrada em ata e acessível a todos, atribuindo-lhes eficácia para fins de habilitação e classificação.

8.18. Na hipótese de o licitante não atender às exigências para habilitação, o Pregoeiro/Agente de Contratação/Comissão examinará a proposta subsequente e assim sucessivamente, na ordem de classificação, até a apuração de uma proposta que atenda ao presente edital, observado o prazo disposto no subitem 8.13.1.

Câmara Nacional de Modelos de Licitações e Contratos da Consultoria-Geral da União
Modelo de Edital - Pregão e Concorrência - TIC - Lei nº 14.133, de 2021.
Aprovado pela Secretaria de Governo Digital
Identidade visual pela Secretaria de Gestão e Inovação
Atualização: ABR/2026

8.19. Somente serão disponibilizados para acesso público os documentos de habilitação do licitante cuja proposta atenda ao edital de licitação, após concluídos os procedimentos de que trata o subitem anterior.

8.20. A comprovação de regularidade fiscal e trabalhista das microempresas e das empresas de pequeno porte somente será exigida para efeito de contratação, e não como condição para participação na licitação.

8.21. Quando a fase de habilitação anteceder a de julgamento e já tiver sido encerrada, não caberá exclusão de licitante por motivo relacionado à habilitação, salvo em razão de fatos supervenientes ou só conhecidos após o julgamento.

9. DO TERMO DE CONTRATO

9.1. Após a homologação e adjudicação, caso se conclua pela contratação, será firmado termo de contrato, ou outro instrumento equivalente.

9.2. O adjudicatário terá o prazo de 10 dias úteis, contados a partir da data de sua convocação, para assinar o termo de contrato ou instrumento equivalente, sob pena de decair o direito à contratação, sem prejuízo das sanções previstas neste Edital.

9.3. Alternativamente à convocação para comparecer perante o órgão ou entidade para a assinatura do Termo de Contrato ou instrumento equivalente, a Administração poderá: a) encaminhá-lo para assinatura, mediante correspondência postal com aviso de recebimento (AR), para que seja assinado e devolvido no prazo de 10 dias úteis, a contar da data de seu recebimento; b) disponibilizar acesso a sistema de processo eletrônico para que seja assinado digitalmente em até 10 dias úteis; ou c) outro meio eletrônico, assegurado o prazo de 10 dias úteis para resposta após recebimento da notificação pela Administração.

9.4. Os prazos dos itens 9.2 e 9.3 poderão ser prorrogados, por igual período, por solicitação justificada do adjudicatário e aceita pela Administração.

9.5. O prazo de vigência da contratação é o estabelecido no Termo de Referência.

9.6. Na assinatura do contrato ou instrumento equivalente será exigido o Cadastro Informativo de Créditos não Quitados do Setor Público Federal – Cadin e a comprovação das condições de habilitação e contratação consignadas neste Edital, que deverão ser mantidas pelo fornecedor durante a vigência do contrato.

9.6.1 A existência de registro no Cadin constitui fator impeditivo para a contratação.

10. DOS RECURSOS

10.1. A interposição de recurso referente ao julgamento das propostas, à habilitação ou inabilitação de licitantes, à anulação ou revogação da licitação, observará o disposto no art. 165 da Lei nº 14.133, de 2021.

10.2. O prazo recursal é de 3 (três) dias úteis, contados da data de intimação ou de lavratura da ata.

10.3. Quando o recurso apresentado impugnar o julgamento das propostas ou o ato de habilitação ou inabilitação do licitante:

10.3.1. a intenção de recorrer deverá ser manifestada imediatamente, sob pena de preclusão;

10.3.2. o prazo para a manifestação da intenção de recorrer não será inferior a 10 (dez) minutos.

10.3.3. o prazo para apresentação das razões recursais será iniciado na data de intimação ou de lavratura da ata de habilitação ou inabilitação;

10.3.4. na hipótese de adoção da inversão de fases prevista no § 1º do art. 17 da Lei nº 14.133, de 2021, o prazo para apresentação das razões recursais será iniciado na data de intimação da ata de julgamento.

Câmara Nacional de Modelos de Licitações e Contratos da Consultoria-Geral da União
Modelo de Edital - Pregão e Concorrência - TIC - Lei nº 14.133, de 2021.
Aprovado pela Secretaria de Governo Digital
Identidade visual pela Secretaria de Gestão e Inovação
Atualização: ABR/2026

10.4. Os recursos deverão ser encaminhados em campo próprio do sistema.

10.5. O recurso será dirigido à autoridade que tiver editado o ato ou proferido a decisão recorrida, a qual poderá reconsiderar sua decisão no prazo de 3 (três) dias úteis, ou, nesse mesmo prazo, encaminhar recurso para a autoridade superior, a qual deverá proferir sua decisão no prazo de 10 (dez) dias úteis, contado do recebimento dos autos.

10.6. Os recursos interpostos fora do prazo não serão conhecidos.

10.7. O prazo para apresentação de contrarrazões ao recurso pelos demais licitantes será de 3 (três) dias úteis, contados da data da intimação pessoal ou da divulgação da interposição do recurso, assegurada a vista imediata dos elementos indispensáveis à defesa de seus interesses.

10.8. O recurso e o pedido de reconsideração terão efeito suspensivo do ato ou da decisão recorrida até que sobrevenha decisão final da autoridade competente.

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

10.10. Os autos do processo permanecerão com vista franqueada aos interessados no sítio eletrônico sei.cnpq.br.

11. DAS INFRAÇÕES ADMINISTRATIVAS E SANÇÕES

11.1. Comete infração administrativa, nos termos da lei, o licitante que, com dolo ou culpa:

11.1.1. deixar de entregar a documentação exigida para o certame ou não entregar qualquer documento que tenha sido solicitado pelo/a Pregoeiro/Agente de Contratação/Comissão/a durante o certame;

11.1.2. Salvo em decorrência de fato superveniente devidamente justificado, não mantiver a proposta em especial quando:

11.1.2.1. não enviar a proposta adequada ao último lance ofertado ou após a negociação;

11.1.2.2. recusar-se a enviar o detalhamento da proposta quando exigível;

11.1.2.3. pedir para ser desclassificado quando encerrada a etapa competitiva; ou

11.1.2.4. deixar de apresentar amostra;

11.1.2.5. apresentar proposta ou amostra em desacordo com as especificações do edital;

11.1.3. não celebrar o contrato ou não entregar a documentação exigida para a contratação, quando convocado dentro do prazo de validade de sua proposta;

11.1.4. recusar-se, sem justificativa, a assinar o contrato ou a ata de registro de preço, ou a aceitar ou retirar o instrumento equivalente no prazo estabelecido pela Administração;

11.1.5. apresentar declaração ou documentação falsa exigida para o certame ou prestar declaração falsa durante a licitação;

11.1.6. fraudar a licitação;

11.1.7. comportar-se de modo inidôneo ou cometer fraude de qualquer natureza, em especial quando:

11.1.7.1. agir em conluio ou em desconformidade com a lei;

11.1.7.2. induzir deliberadamente a erro no julgamento;

11.1.7.3. apresentar amostra falsificada ou deteriorada;

Câmara Nacional de Modelos de Licitações e Contratos da Consultoria-Geral da União
Modelo de Edital - Pregão e Concorrência - TIC - Lei nº 14.133, de 2021.
Aprovado pela Secretaria de Governo Digital
Identidade visual pela Secretaria de Gestão e Inovação
Atualização: ABR/2026

11.1.8. praticar atos ilícitos com vistas a frustrar os objetivos da licitação

11.1.9. praticar ato lesivo previsto no art. 5º da Lei n.º 12.846, de 2013.

11.2. Com fulcro na Lei nº 14.133, de 2021, a Administração poderá, após regular processo administrativo, garantida a prévia defesa, aplicar aos licitantes e/ou adjudicatários as seguintes sanções, sem prejuízo das responsabilidades civil e criminal:

11.2.1. advertência;

11.2.2. multa;

11.2.3. impedimento de licitar e contratar e

11.2.4. declaração de inidoneidade para licitar ou contratar, enquanto perdurarem os motivos determinantes da punição ou até que seja promovida sua reabilitação perante a própria autoridade que aplicou a penalidade.

11.3. Na aplicação das sanções serão considerados:

11.3.1. a natureza e a gravidade da infração cometida.

11.3.2. as peculiaridades do caso concreto

11.3.3. as circunstâncias agravantes ou atenuantes

11.3.4. os danos que dela provierem para a Administração Pública

11.3.5. a implantação ou o aperfeiçoamento de programa de integridade, conforme normas e orientações dos órgãos de controle.

11.4. A multa será recolhida no prazo máximo de 10 (dez) dias úteis, a contar da comunicação oficial.

11.4.1. Para as infrações previstas nos itens 11.1.1, 11.1.2 e 11.1.3, a multa será de 0,5% a 15% do valor do contrato licitado.

11.4.2. Para as infrações previstas nos itens 11.1.5, 11.1.6, 11.1.7, 11.1.8, 11.1.9 e 11.1.9, a multa será de 15% a 30% do valor do contrato licitado.

11.5. As sanções de advertência, impedimento de licitar e contratar e declaração de inidoneidade para licitar ou contratar poderão ser aplicadas, cumulativamente ou não, à penalidade de multa.

11.6. Na aplicação da sanção de multa será facultada a defesa do interessado no prazo de 15 (quinze) dias úteis, contado da data de sua intimação.

11.7. A sanção de impedimento de licitar e contratar será aplicada ao responsável em decorrência das infrações administrativas relacionadas nos itens 11.1.1, 11.1.2, 11.1.3 e 11.1.4, quando não se justificar a imposição de penalidade mais grave, e impedirá o responsável de licitar e contratar no âmbito da Administração Pública direta e indireta do ente federativo a qual pertencer o órgão ou entidade, pelo prazo máximo de 3 (três) anos.

11.8. Poderá ser aplicada ao responsável a sanção de declaração de inidoneidade para licitar ou contratar, em decorrência da prática das infrações dispostas nos itens 11.1.5, 11.1.6, 11.1.7, 11.1.8 e 11.1.9, bem como pelas infrações administrativas previstas nos itens 11.1.1, 11.1.2 e 11.1.3 que justifiquem a imposição de penalidade mais grave que a sanção de impedimento de licitar e contratar, cuja duração observará o prazo previsto no art. 156, §5º, da Lei nº 14.133, de 2021

11.9. A recusa injustificada do adjudicatário em assinar o contrato ou a ata de registro de preço, ou em aceitar ou retirar o instrumento equivalente no prazo estabelecido pela Administração, descrita no item 11.1.3, caracterizará o descumprimento total da obrigação assumida e o sujeitará às penalidades e à imediata perda

Câmara Nacional de Modelos de Licitações e Contratos da Consultoria-Geral da União
Modelo de Edital - Pregão e Concorrência - TIC - Lei nº 14.133, de 2021.
Aprovado pela Secretaria de Governo Digital
Identidade visual pela Secretaria de Gestão e Inovação
Atualização: ABR/2026

da garantia de proposta em favor do órgão ou entidade promotora da licitação, nos termos do art. 45, §4º da IN SEGES/ME n.º 73, de 2022.

11.10. A apuração de responsabilidade relacionadas às sanções de impedimento de licitar e contratar e de declaração de inidoneidade para licitar ou contratar demandará a instauração de processo de responsabilização a ser conduzido por comissão composta por 2 (dois) ou mais servidores estáveis, que avaliará fatos e circunstâncias conhecidos e intimará o licitante ou o adjudicatário para, no prazo de 15 (quinze) dias úteis, contado da data de sua intimação, apresentar defesa escrita e especificar as provas que pretenda produzir.

11.11. Caberá recurso no prazo de 15 (quinze) dias úteis da aplicação das sanções de advertência, multa e impedimento de licitar e contratar, contado da data da intimação, o qual será dirigido à autoridade que tiver proferido a decisão recorrida, que, se não a reconsiderar no prazo de 5 (cinco) dias úteis, encaminhará o recurso com sua motivação à autoridade superior, que deverá proferir sua decisão no prazo máximo de 20 (vinte) dias úteis, contado do recebimento dos autos.

11.12. Caberá a apresentação de pedido de reconsideração da aplicação da sanção de declaração de inidoneidade para licitar ou contratar no prazo de 15 (quinze) dias úteis, contado da data da intimação, e decidido no prazo máximo de 20 (vinte) dias úteis, contado do seu recebimento.

11.13. O recurso e o pedido de reconsideração terão efeito suspensivo do ato ou da decisão recorrida até que sobrevenha decisão final da autoridade competente.

11.14. A aplicação das sanções previstas neste edital não exclui, em hipótese alguma, a obrigação de reparação integral dos danos causados.

11.15. Para a garantia da ampla defesa e contraditório dos licitantes, as notificações serão enviadas eletronicamente para os endereços de e-mail informados na proposta comercial, bem como os cadastrados pela empresa no SICAF.

11.15.1 Os endereços de e-mail informados na proposta comercial e/ou cadastrados no Sicaf serão considerados de uso contínuo da empresa, não cabendo alegação de desconhecimento das comunicações a eles comprovadamente enviadas.

12. DA IMPUGNAÇÃO AO EDITAL E DO PEDIDO DE ESCLARECIMENTO

12.1. Qualquer pessoa é parte legítima para impugnar este Edital por irregularidade na aplicação da Lei nº 14.133, de 2021, devendo protocolar o pedido até 3 (três) dias úteis antes da data da abertura do certame.

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

12.3. A impugnação e o pedido de esclarecimento poderão ser realizados por forma eletrônica, pelos seguintes meios:licitacao@cnpq.br ou por petição dirigida ou protocolada no endereço Setor de Autarquias Sul (SAUS) Quadra 01, Lote 06, Bloco H, Edifício Telemundi II, Bairro Asa Sul, Brasília/DF – CEP: 70.070010 – Serviço de Compras e Licitações – SELIC, 4° andar.

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

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

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

Câmara Nacional de Modelos de Licitações e Contratos da Consultoria-Geral da União
Modelo de Edital - Pregão e Concorrência - TIC - Lei nº 14.133, de 2021.
Aprovado pela Secretaria de Governo Digital
Identidade visual pela Secretaria de Gestão e Inovação
Atualização: ABR/2026

13. DAS DISPOSIÇÕES GERAIS

13.1. Será divulgada ata da sessão pública no sistema eletrônico.

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

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

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

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

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

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

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

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

13.10. O Edital e seus anexos estão disponíveis, na íntegra, no Portal Nacional de Contratações Públicas (PNCP) e endereço eletrônico www.gov.br/compras/pt-br e http://memoria2.cnpq.br/web/guest/licitacoes/.

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

13.11.1 Anexo I - Termo de Referência;

13.11.1.1. Apêndice do Anexo I – Estudo Técnico Preliminar;

13.11.1.2. Anexo I do Termo de Referência - ESPECIFICACAO TECNICA MINIMA DA SOLUCAO;

13.11.1.3. Anexo II do Termo de Referência - MATRIZ DE COMPROVACAO DE ATENDIMENTO A ESPECIFICACAO TÉCNICA MINIMA DA SOLUÇÃO;

13.11.1.4. Anexo III do Termo de Referência - TERMO DE COMPROMISSO DE MANUTENÇÃO DE SIGILO;

13.11.1.5. Anexo IV do Termo de Referência - TERMO DE CIÊNCIA;

13.11.1.6. Anexo V do Termo de Referência - MODELO DO TERMO DE VISTORIA TÉCNICA;

13.11.1.7. Anexo VI do Termo de Referência - MODELO DE RECUSA DE VISTORIA TÉCNICA;

13.11.1.8. Anexo VII do Termo de Referência - MODELO DA PLANILHA DE CUSTOS E FORMACAO DE PREÇOS PARA LICENÇAS/SUBSCRIÇÃO;

13.11.1.9. Anexo VIII do Termo de Referência - MODELO DE PLANILHA DE COMPOSICAO DE CUSTOS E FORMACAO DE PREÇOS PARA CONSULTORIA; e

Câmara Nacional de Modelos de Licitações e Contratos da Consultoria-Geral da União
Modelo de Edital - Pregão e Concorrência - TIC - Lei nº 14.133, de 2021.
Aprovado pela Secretaria de Governo Digital
Identidade visual pela Secretaria de Gestão e Inovação
Atualização: ABR/2026

13.11.1.10. Anexo II – Minuta de Termo de Contrato

Brasília, 08 de setembro de 2026.

Victor Ferreira Dantas
Pregoeiro Oficial Portaria CNPq n° 2.600/2026

Equipe de Apoio: Anderson Cleiton Fernandes Leite

Câmara Nacional de Modelos de Licitações e Contratos da Consultoria-Geral da União
Modelo de Edital - Pregão e Concorrência - TIC - Lei nº 14.133, de 2021.
Aprovado pela Secretaria de Governo Digital
Identidade visual pela Secretaria de Gestão e Inovação
Atualização: ABR/2026

CONSELHO NACIO DE DESEN. CIENT. E TECNOLÓGICO

Termo de Referência 69/2026

Informações Básicas

Número do artefato	UASG	Editado por	Atualizado em
69/2026	364102-CONSELHO NACIO DE DESEN. CIENT. E TECNOLÓGICO	FILIPE JOSE ALVES OLIVEIRA	19/08/2026 15:06 (v 0.7)

Status

ASSINADO

Outras informações

Categoria	Número da Contratação	Processo Administrativo
VII - contratações de tecnologia da informação e de comunicação/Bens de TIC		01300.003396/2025-91

1. CONDIÇÕES GERAIS DA CONTRATAÇÃO

1.1. Aquisição de solução corporativa de *Application Delivery Controller (ADC)*, baseada na plataforma F5 BIG-IP, com funcionalidades integradas de *Web Application Firewall (WAF)*, a ser instalada em ambiente *on-premise* no data center do CNPq, contemplando o fornecimento dos *appliances*, das licenças de software F5 BIG-IP, da garantia e do suporte técnico oficial do fabricante, das subscrições e assinaturas de segurança da solução, bem como dos serviços especializados de instalação, configuração e implantação, dos serviços de suporte técnico especializado da contratada em regime 24x7 e dos serviços de consultoria técnica especializada sob demanda, pelo prazo de 60 (sessenta) meses, nos termos da tabela abaixo e conforme condições e exigências estabelecidas neste instrumento.

Tabela 01 - Itens da Contratação

GRUPO	ITEM	ESPECIFICAÇÃO	CATMAT /CATSER	MÉTRICA	QUANTIDADE	VALOR UNITÁRIO	VALOR TOTAL
1	1	*Appliance de Application Delivery Controller (ADC)* baseada na plataforma F5 BIG-IP, com funcionalidades integradas de *Web Application Firewall (WAF)*	481646	Unidade	2	R$ 704.871,29	**R$ 1.409.742,58**
	2	Licenças de software F5 BIG-IP	27464	Unidade	2	R$ 522.396,45	**R$ 1.044.792,90**
	3	Garantia e suporte técnico oficial do fabricante para a solução F5 BIG-IP	27740	Unidade	2	R$ 770.832,49	**R$ 1.541.664,98**
	4	Subscrições e assinaturas de segurança da plataforma F5 BIG-IP	27502	Unidade	2	R$ 468.107,56	**R$ 936.215,12**
	5	Serviços especializados de instalação, configuração e implantação da solução	26972	Unidade	1	R$ 259.951,25	**R$ 259.951,25**

	6	Serviços de consultoria técnica especializada (sob demanda)	27340	Hora	480	R$ 572,00	**R$ 274.560,00**
	7	Serviços de suporte técnico especializado da contratada em regime 24x7	27740	Mês	60	R$ 9.655,73	**R$ 579.343,80**
VALOR TOTAL							**R$ 6.046.270,63**

1.2. CLASSIFICAÇÃO DO OBJETO QUANTO À HETEROGENEIDADE OU COMPLEXIDADE

1.2.1. Os bens objeto desta contratação são caracterizados como comuns, conforme justificativa constante do Estudo Técnico Preliminar.

1.3. CLASSIFICAÇÃO DO OBJETO COMO BEM DE LUXO

1.3.1. O objeto desta contratação não se enquadra como bem de luxo, conforme Decreto nº 10.818, de 27 de setembro de 2021.

1.4. CLASSIFICAÇÃO DO OBJETO QUANTO AO MODELO DE EXECUÇÃO

1.4.1. O fornecimento de bens é enquadrado como fornecimento não continuado, por se tratar da entrega de equipamentos de forma pontual, sem demanda de caráter permanente.

1.4.2. A contratação contempla, ainda, a prestação de serviços associados à solução, compreendendo os serviços especializados de instalação, configuração e implantação, os serviços de consultoria técnica especializada sob demanda, o suporte técnico especializado da contratada e a garantia e suporte técnico oficial do fabricante durante o período contratual.

1.4.3. A adoção de vigência plurianual para os serviços mostra-se mais vantajosa para a Administração, conforme demonstrado no Estudo Técnico Preliminar, considerando a necessidade de assegurar a continuidade do suporte técnico, a manutenção das atualizações de segurança e o pleno funcionamento da solução ao longo de seu ciclo de vida.

1.5. PRAZO DE VIGÊNCIA

1.5.1. O prazo de vigência da contratação é de 5 anos contados da assinatura do contrato, prorrogável por até 10 anos, na forma dos artigos 106 e 107 da Lei n° 14.133, de 2021. Observado que a prorrogação aplica-se aos serviços de natureza continuada, permanecendo os itens de fornecimento sujeitos à execução única, nos termos deste Termo de Referência.

1.5.2. Nas eventuais prorrogações da vigência contratual, serão considerados exclusivamente os itens de natureza continuada, tais como garantia e suporte técnico oficial do fabricante, subscrições e assinaturas de segurança, serviços de consultoria técnica especializada e serviços de suporte técnico especializado da CONTRATADA, não integrando a base de cálculo da prorrogação os itens de fornecimento único já executados e pagos, especialmente o fornecimento dos *appliances*, o licenciamento da solução e os serviços de instalação, configuração e implantação. Dessa forma, eventuais reajustes e acréscimos decorrentes da prorrogação incidirão estritamente sobre os itens de natureza continuada, observadas as condições previstas neste Termo de Referência.

1.5.3. O contrato ou outro instrumento hábil que o substitua oferece maior detalhamento das regras que serão aplicadas em relação à vigência da contratação.

2. FUNDAMENTAÇÃO E DESCRIÇÃO DA NECESSIDADE DA CONTRATAÇÃO

2.1. A presente contratação justifica-se pela necessidade de assegurar a continuidade operacional, a disponibilidade, a segurança e o desempenho do ambiente de entrega e proteção de aplicações que integra o núcleo de rede do Data Center do Conselho Nacional de Desenvolvimento Científico e Tecnológico - CNPq, responsável pela sustentação de sistemas institucionais críticos utilizados na gestão administrativa, orçamentária, científica e de fomento à pesquisa.

2.2. O ambiente atualmente em operação é baseado na plataforma F5 BIG-IP, desempenhando papel central na arquitetura de rede e aplicações do CNPq, atuando como camada intermediária responsável pelo controle, inspeção e distribuição do tráfego entre usuários e sistemas institucionais, incluindo funcionalidades de balanceamento de carga em camadas L4 e L7, terminação de conexões criptografadas, aplicação de políticas de segurança e otimização de desempenho.

2.3. Registra-se ainda que a infraestrutura atualmente em operação encontra-se em versão significativamente defasada, fora do ciclo de suporte do fabricante (*End of Technical Support – EoTS*), não dispondo de atualizações de segurança, correções de falhas ou melhorias evolutivas, caracterizando cenário de obsolescência tecnológica.

2.4. Adicionalmente, levantamento técnico realizado no âmbito do Estudo Técnico Preliminar evidenciou que o ambiente possui elevado grau de dependência funcional da plataforma atualmente utilizada, incluindo:

2.4.1. utilização de configurações avançadas de virtual servers, pools e perfis de tráfego;

2.4.2. aplicação de políticas de segurança de aplicações (WAF) específicas por sistema;

2.4.3. uso de mecanismos de customização e lógica avançada de tratamento de tráfego (tais como scripts e regras específicas);

2.4.4. integração com soluções institucionais de monitoramento, auditoria e segurança.

2.5. A permanência da infraestrutura atual implica na operação de ambiente em estado avançado de obsolescência tecnológica, expondo o CNPq a riscos relevantes, tais como:

2.5.1. indisponibilidade de sistemas institucionais críticos;

2.5.2. exploração de vulnerabilidades conhecidas, sem possibilidade de correção;

2.5.3. degradação de desempenho no acesso às aplicações;

2.5.4. limitações na adoção de novas arquiteturas e tecnologias;

2.5.5. não conformidade com boas práticas e normativos de segurança da informação aplicáveis à Administração Pública Federal.

2.6. Considerando a criticidade do ambiente e o elevado grau de acoplamento tecnológico à plataforma atualmente utilizada (F5 BIG-IP), a substituição integral por solução de fabricante distinto implicaria na necessidade de reimplementação de configurações, políticas de segurança, regras de tratamento de tráfego e integrações existentes, incluindo mecanismos avançados como *iRules* e políticas de *Web Application Firewall* (WAF).

2.6.1. Tal cenário acarretaria aumento significativo da complexidade operacional, riscos à continuidade dos serviços institucionais, possibilidade de indisponibilidade de sistemas críticos e custos adicionais relacionados à adaptação, capacitação da equipe técnica e estabilização do ambiente.

2.6.2. Dessa forma, a adoção de solução compatível com a arquitetura tecnológica existente mostra-se tecnicamente justificada, visando garantir a continuidade operacional, a integridade das configurações atualmente em produção e a mitigação de riscos associados à transição de plataforma.

2.6.3. A presente abordagem encontra respaldo no art. 41, inciso I, da Lei nº 14.133/2021, que admitem a indicação de marca ou modelo quando necessária para assegurar a padronização, compatibilidade e continuidade tecnológica da solução.

2.7. Nesse contexto, torna-se necessária a modernização da plataforma de entrega e proteção de aplicações, mediante a implantação de solução corporativa de *Application Delivery Controller* (ADC) com funcionalidades integradas de *Web Application Firewall* (WAF), capaz de prover:

2.7.1. distribuição inteligente de tráfego em camadas L4 e L7;

2.7.2. inspeção e processamento de conexões criptografadas;

2.7.3. proteção contra ataques direcionados a aplicações web e APIs;

2.7.4. integração com mecanismos institucionais de segurança e monitoramento;

2.7.5. suporte a arquiteturas modernas de aplicações.

2.8. Estimativa de Demanda:

2.8.1. A estimativa de demanda foi consolidada conforme justificativas registradas no Estudo Técnico Preliminar - ETP, que considerou:

2.8.1.1. a arquitetura atual do ambiente em alta disponibilidade;

2.8.1.2. a criticidade dos sistemas suportados;

2.8.1.3. a carga atual de processamento e projeção de crescimento;

2.8.1.4. a necessidade de cobertura integral de suporte e garantia durante o período contratual.

2.8.2. A solução proposta contempla o fornecimento de *appliances*, licenças de software, garantia e suporte técnico oficial do fabricante, subscrições e assinaturas de segurança, além da prestação de serviços especializados de instalação, configuração e implantação, suporte técnico especializado da contratada e consultoria técnica sob demanda, necessários para garantir a adequada implantação, operação e sustentação da solução durante toda a vigência contratual.

2.8.3. A definição da solução está alinhada às práticas adotadas por órgãos da Administração Pública que operam ambientes de missão crítica, nos quais soluções de *Application Delivery Controller* com funcionalidades de proteção de aplicações são utilizadas como componente essencial para garantia de disponibilidade, desempenho e segurança de serviços digitais.

2.9. Parcelamento da Solução de TIC:

2.9.1. A contratação está organizada em grupo único, formado por 7 (sete) itens, conforme tabela constante no subitem 1.1 deste Termo de Referência.

2.9.2. Embora a solução esteja estruturada em itens distintos para fins de precificação e formação da proposta, o parcelamento da contratação não se mostra tecnicamente adequado, considerando a necessária integração entre os *appliances*, as licenças de software, a garantia e o suporte técnico oficial do fabricante, as subscrições e assinaturas de segurança e os serviços especializados de implantação, suporte e consultoria, conforme registrado no Estudo Técnico Preliminar - ETP.

2.10. Resultados e benefícios a serem alcançados:

2.10.1. Dentre os principais benefícios a serem alcançados com a contratação, pode-se destacar:

2.10.1.1. assegurar a continuidade operacional dos serviços institucionais, com a manutenção dos serviços de balanceamento de carga e proteção de aplicações;

2.10.1.2. garantir a elevada disponibilidade, confiabilidade e resiliência dos sistemas finalísticos do CNPq;

2.10.1.3. promover a modernização da infraestrutura de entrega e proteção de aplicações, com adoção de tecnologias atualizadas e suportadas pelo fabricante;

2.10.1.4. melhorar o desempenho no acesso às aplicações institucionais, com redução de latência e otimização do uso dos recursos de rede;

2.10.1.5. otimizar a utilização dos links de comunicação, por meio de mecanismos avançados de distribuição e aceleração de tráfego;

2.10.1.6. fortalecer a segurança da informação, com proteção das aplicações contra ameaças cibernéticas, incluindo ataques de negação de serviço e vulnerabilidades de camada de aplicação;

2.10.1.7. possibilitar a inspeção e o controle do tráfego de aplicações, com maior visibilidade e capacidade de resposta a incidentes de segurança;

2.10.1.8. padronizar e fortalecer as políticas de segurança de aplicações, com uso consistente de mecanismos de proteção e mitigação de riscos;

2.10.1.9. reduzir a complexidade arquitetural do ambiente, evitando a introdução de múltiplas soluções heterogêneas e diminuindo a superfície de falhas;

2.10.1.10. aumentar a eficiência operacional da equipe técnica, com aproveitamento da expertise já existente no ambiente institucional;

2.10.1.11. possibilitar a evolução tecnológica contínua da infraestrutura, de forma compatível com o crescimento das demandas institucionais;

2.10.1.12. aprimorar a governança da infraestrutura de TIC, com maior controle, rastreabilidade e gestão centralizada da solução.

2.11. O objeto da contratação está previsto no Plano de Contratações Anual 2026, conforme consta das informações básicas deste termo de referência.

2.12. O objeto da contratação também está alinhado com a Estratégia Nacional de Governo Digital 2024/2027 e em consonância com o Plano Diretor de Tecnologia da Informação (PDTI) 2025/2027 do Conselho Nacional de Desenvolvimento Científico e Tecnológico - CNPq, conforme demonstrado abaixo:

Tabela 02 - Alinhamento a ENGD 2024/2027

ALINHAMENTO AOS PLANOS ESTRATÉGICOS	
ID	**Objetivos Estratégicos**
Objetivo 5.3	Contribuir para a elaboração e adotar um modelo de compartilhamento de dados que permita ao cidadão no uso seguro dos seus dados e melhore sua experiência no acesso a serviços

Tabela 03 - Alinhamento ao PDTI CNPq 2025/2027

ALINHAMENTO AO PDTI 2025/2027		
Necessidades de Gerais de Contratação (NG)		
ID	**Ação do PDTI**	**Meta do PDTI associada**
NG.04	Soluções e serviços de segurança da informação	Solução de proteção para a rede
NG.06	Modernização e manutenção de TIC	Manutenção e atualização de redes

Tabela 04 - Alinhamento ao PGC 2026

ALINHAMENTO AO PLANO DE GERENCIAMENTO DE CONTRATAÇÕES 2026 (PGC)	
DFD 210 /2025	Solução de balanceamento de cargas de rede e Firewall de Aplicações Web (WAF)

3. DESCRIÇÃO DA SOLUÇÃO COMO UM TODO CONSIDERADO O CICLO DE VIDA DO OBJETO E ESPECIFICAÇÃO DO PRODUTO

3.1. A descrição da solução como um todo encontra-se pormenorizada em tópico específico dos Estudos Técnicos Preliminares.

3.2. A solução de TIC consiste na contratação integrada de bens e serviços destinados à modernização da solução atualmente em uso no CNPq (F5 BIG-IP), no âmbito da infraestrutura de entrega e proteção de aplicações do Conselho Nacional de Desenvolvimento Científico e Tecnológico - CNPq, considerando todo o ciclo de vida do objeto, desde a implantação da nova infraestrutura tecnológica até sua operação assistida, suporte técnico especializado e evolução controlada ao longo da vigência contratual.

3.3. Os quantitativos dos bens e serviços foram definidos com base no levantamento técnico do ambiente existente, considerando a arquitetura atual em alta disponibilidade, a criticidade dos sistemas suportados, a necessidade de fornecimento dos *appliances*, das licenças de *software*, da garantia e suporte técnico oficial do fabricante, das subscrições e assinaturas de segurança, bem como a estimativa de demanda por serviços técnicos especializados ao longo da vigência contratual.

3.4. A solução de *Application Delivery Controller* (ADC) com funcionalidades integradas de *Web Application Firewall* (WAF) a ser contratada deverá prover, no mínimo, as seguintes funcionalidades e capacidades:

3.4.1. balanceamento de carga de aplicações em camadas L4 e L7, com distribuição inteligente de tráfego entre múltiplos servidores ou instâncias de aplicação;

3.4.2. inspeção, terminação e recriptografia de conexões seguras, com suporte a protocolos modernos de segurança e criptografia;

3.4.3. proteção de aplicações web e APIs contra ameaças da camada de aplicação, incluindo ataques conhecidos e comportamentais;

3.4.3. aplicação de políticas de segurança baseadas em assinaturas, comportamento e análise de tráfego;

3.4.4. proteção contra ataques de negação de serviço (DoS/DDoS), incluindo mecanismos de mitigação automática;

3.4.5. suporte à publicação segura de aplicações na internet, com controle de acesso, visibilidade e governança do tráfego;

3.4.6. mecanismos de otimização, compressão e aceleração de tráfego de aplicações;

3.4.7. persistência de sessão e controle avançado de conexões;

3.4.8. monitoramento contínuo da saúde dos serviços, com balanceamento baseado em desempenho e disponibilidade;

3.4.9. integração com soluções institucionais de monitoramento, auditoria e segurança da informação;

3.4.10. suporte à automação e integração com ambientes modernos de infraestrutura e orquestração;

3.4.11. geração de logs detalhados e relatórios de tráfego, segurança e desempenho;

3.4.12. gerenciamento centralizado da solução, com controle de políticas, visibilidade operacional e administração unificada.

3.5. A solução deverá possuir funcionalidades de firewall de aplicações web (WAF), contemplando, no mínimo:

3.5.1. proteção contra ataques de camada de aplicação, incluindo injeção de código, *cross-site scripting* (XSS), entre outros;

3.5.2. implementação de modelo de segurança positivo e negativo para definição de políticas;

3.5.3. suporte à proteção de aplicações web tradicionais e APIs;

3.5.4. capacidade de inspeção de tráfego criptografado;

3.5.5. aplicação de políticas baseadas em geolocalização, reputação e comportamento;

3.5.6. atualização contínua de assinaturas de segurança;

3.5.7. geração de logs e relatórios específicos de eventos de segurança;

3.5.8. mitigação automatizada de ameaças e ataques.

3.6. A solução assegura cobertura completa ao longo de todo o ciclo de vida do objeto, compreendendo:

3.6.1. implantação da nova infraestrutura;

3.6.2. entrada em produção assistida;

3.6.3. suporte técnico contínuo;

3.6.4. manutenção evolutiva;

3.6.5. tratamento de incidentes e ajustes operacionais.

3.7. As funcionalidades descritas deverão ser atendidas de forma integrada pela solução, admitindo-se a composição por componentes, desde que estes operem de forma plenamente integrada, não comprometam a gestão centralizada, a interoperabilidade, o desempenho ou a segurança do ambiente.

4. REQUISITOS DA CONTRATAÇÃO

4.1. REQUISITOS DE NEGÓCIO

4.1.1. A presente contratação orienta-se pelos seguintes requisitos de negócio:

4.1.1.1. Assegurar a continuidade operacional, a disponibilidade e a confiabilidade dos serviços de aplicações institucionais do CNPq, por meio da modernização da plataforma de balanceamento de carga e segurança de aplicações, eliminando riscos decorrentes da obsolescência tecnológica do ambiente atualmente em operação.

4.1.1.2. Garantir que a solução adotada esteja alinhada ao ciclo de suporte do fabricante, com acesso a suporte técnico oficial, atualizações regulares de software e correções de vulnerabilidades, de forma a reduzir riscos operacionais, de segurança e de indisponibilidade dos serviços institucionais.

4.1.1.3. Assegurar a disponibilidade contínua dos serviços, inclusive durante atividades de manutenção, atualização de software, substituição de componentes ou tratamento de falhas, de modo a não impactar o acesso dos usuários às funcionalidades críticas disponibilizadas pela instituição.

4.1.1.4. Atender às demandas atuais e futuras do negócio, suportando a evolução tecnológica dos sistemas institucionais, bem como a ampliação do volume de acessos, transações e integrações com outros órgãos e sistemas governamentais.

4.1.1.5. Promover a melhoria da experiência do usuário no acesso às aplicações institucionais, garantindo desempenho adequado, baixa latência e elevada taxa de disponibilidade, especialmente em períodos de maior utilização ou de demandas sazonais.

4.1.1.6. Reduzir a exposição a riscos de segurança da informação, por meio da correção de falhas de segurança conhecidas, mitigação de vulnerabilidades críticas e adoção de mecanismos atualizados de proteção às aplicações e aos dados institucionais.

4.1.1.7. Garantir que a solução de balanceamento de carga possua capacidade adequada de processamento e desempenho, evitando gargalos que possam comprometer a prestação dos serviços institucionais, mesmo em cenários de aumento súbito de demanda.

4.1.1.8. Assegurar o correto dimensionamento da solução, considerando:

4.1.1.8.1. A carga atual de trabalho, de forma a garantir fluidez, estabilidade e desempenho no acesso às aplicações e sistemas em produção.

4.1.1.8.2. A carga futura estimada, assegurando escalabilidade, crescimento sustentável e longevidade da solução, evitando novas contratações emergenciais no curto ou médio prazo.

4.1.1.9. Garantir a manutenção evolutiva da solução, com acesso a atualizações regulares de software disponibilizadas pelo fabricante, incluindo melhorias de desempenho, compatibilidade com novas tecnologias e correções de falhas de segurança durante toda a vigência contratual.

4.1.1.10. Assegurar a proteção das aplicações web institucionais contra ataques cibernéticos direcionados à camada de aplicação, tais como injeção de código, cross-site scripting (XSS), exploração de vulnerabilidades, ataques automatizados e outras ameaças descritas em boas práticas internacionais de segurança de aplicações.

4.1.1.11. Possibilitar a inspeção, análise e controle do tráfego de aplicações web por meio de mecanismos especializados de firewall de aplicações web (WAF), capazes de identificar, bloquear e mitigar atividades maliciosas antes que estas atinjam os servidores de aplicação.

4.1.1.12. Prover mecanismos de distribuição inteligente de tráfego entre múltiplos servidores ou instâncias de aplicação, permitindo a otimização do uso dos recursos computacionais disponíveis e evitando sobrecarga em componentes individuais da infraestrutura.

4.1.1.13. Permitir a implementação de arquiteturas de alta disponibilidade e recuperação de desastres, possibilitando o redirecionamento automático do tráfego para ambientes alternativos em caso de falhas ou indisponibilidade de serviços.

4.1.1.14. Assegurar compatibilidade com arquiteturas modernas de aplicações, incluindo ambientes virtualizados, plataformas de containers, microsserviços e interfaces de programação de aplicações (APIs), de modo a suportar a evolução tecnológica dos sistemas institucionais.

4.1.1.15. Possibilitar a integração com ferramentas de automação e gerenciamento de infraestrutura, permitindo a adoção de práticas modernas de operação de ambientes de tecnologia da informação, tais como automação de configurações, integração com pipelines de desenvolvimento e gerenciamento programático da infraestrutura.

4.1.1.16. Prover mecanismos de monitoramento, auditoria e geração de relatórios que permitam maior visibilidade sobre o tráfego das aplicações, identificação de comportamentos anômalos e suporte às atividades de governança e gestão da segurança da informação.

4.1.1.17. Reduzir a complexidade operacional da infraestrutura de entrega e proteção de aplicações, consolidando funcionalidades de balanceamento de carga, segurança de aplicações e otimização de tráfego em uma plataforma integrada, contribuindo para maior eficiência operacional e melhor aproveitamento dos recursos tecnológicos disponíveis.

4.2. REQUISITOS DE CAPACITAÇÃO

4.2.1. Não faz parte do escopo da contratação a realização de capacitação técnica na utilização dos recursos relacionados ao objeto da presente contratação. Contudo, a CONTRATADA deverá garantir a transferência de conhecimento da solução que deve ser realizada sem ônus para o CNPq.

4.3. REQUISITOS LEGAIS

4.3.1. O presente processo de contratação deve estar aderente à:

4.3.1.1. Constituição Federal;

4.3.1.2. Lei nº 14.133, de 1º de abril de 2021 (Lei de Licitações e Contratos Administrativos);

4.3.1.3. Instrução Normativa SGD/ME nº 94, de 23 de dezembro de 2022, que dispõe sobre o processo de contratação de soluções de Tecnologia da Informação e Comunicação - TIC pelos órgãos e entidades integrantes do Sistema de Administração dos Recursos de Tecnologia da Informação - SISP do Poder Executivo Federal;

4.3.1.4. Portaria SGD/MGI nº 5.950, de 26 de outubro de 2023, que estabelece modelo de contratação de software e de serviços de computação em nuvem, no âmbito dos órgãos e entidades integrantes do Sistema de Administração dos Recursos de Tecnologia da Informação - SISP do Poder Executivo Federal;

4.3.1.5. Instrução Normativa SEGES/ME nº 65, de 7 de julho de 2021, que dispõe sobre o procedimento administrativo para a realização de pesquisa de preços para aquisição de bens e contratação de serviços em geral, no âmbito da administração pública federal direta, autárquica e fundacional;

4.3.1.6. Lei nº 13.709, de 14 de agosto de 2018 (Lei Geral de Proteção de Dados Pessoais – LGPD);

4.3.1.7. Decreto nº 10.947, de 25 de janeiro de 2022, que regulamenta o plano de contratações anual e institui o Sistema de Planejamento e Gerenciamento de Contratações no âmbito da administração pública federal direta, autárquica e fundacional;

4.3.1.8. Decreto nº 12.122, de 30 de julho de 2024, que institui o Programa Federal de Prevenção e Enfrentamento do Assédio e da Discriminação;

4.3.1.9. Plano Diretor de Logística Sustentável do CNPq 2026/2028 (CPLS/CNPq);

4.3.1.10. Resolução CGD/CNPq nº 2, de 3 de novembro de 2025, que dispõe sobre a estratégia de uso de software e de serviços de computação em nuvem, no âmbito do CNPq;

4.3.1.11. Decreto nº 12.572, de 24 de agosto de 2025, que institui a Política Nacional de Segurança da Informação e dispõe sobre a governança da segurança da informação no âmbito da administração pública federal;

4.3.1.12. Decreto nº 7.174, de 12 de maio de 2010, que regulamenta a contratação de bens e serviços de informática e automação pela administração pública federal, assegurando as preferências e certificações adequadas;
4.3.1.13. Instrução Normativa SLTI/MP nº 01, de 19 de janeiro de 2010, que dispõe sobre os critérios de sustentabilidade ambiental na aquisição de bens e contratação de serviços;
4.3.1.14. Lei nº 12.305, de 2 de agosto de 2010, que institui a Política Nacional de Resíduos Sólidos (PNRS), aplicada especificamente à logística reversa e desfazimento ambientalmente adequado dos equipamentos substituídos;
4.3.1.15. Portaria SGD/MGI nº 1.070, de 1º de junho de 2023, que estabelece o Modelo de Contratação de Serviços de Operação de Infraestrutura e Atendimento a Usuários de Tecnologia da Informação e Comunicação;
4.3.1.16. Padrões de Governo Eletrônico, especificamente os Padrões de Interoperabilidade (e-PING), o Modelo de Acessibilidade (e-MAG) e os Padrões Web (e-PWG) , que devem ser observados nas soluções de TIC do Poder Executivo;
4.3.1.17. Lei nº 12.527, de 18 de novembro de 2011, Lei de Acesso à Informação (LAI), em atendimento à garantia de transparência, tratamento e segurança das informações no âmbito dos serviços prestados;
4.3.1.18. Instrução Normativa GSI/PR nº 5, de 30 de agosto de 2021, que dispõe sobre os requisitos mínimos de segurança da informação para utilização de soluções de computação em nuvem.

4.3.1.19. Demais normas legais, regulamentares e orientações dos órgãos de controle aplicáveis à contratação, execução e fiscalização de soluções de TIC.

4.4. REQUISITOS DE MANUTENÇÃO E SUPORTE TÉCNICO

4.4.1. Considerando a criticidade da infraestrutura de balanceamento de carga e proteção de aplicações do CNPq, a solução de TIC a ser contratada deverá contemplar garantia e suporte técnico oficial do fabricante, subscrições e assinaturas de segurança, bem como serviços de suporte técnico especializado da CONTRATADA, durante toda a vigência contratual.

4.4.2. Esses serviços deverão assegurar o funcionamento contínuo da solução implantada, bem como a atualização tecnológica e a correção de eventuais falhas identificadas durante sua operação.

4.4.3. A garantia e o suporte técnico oficial do fabricante, bem como os serviços de suporte técnico especializado da CONTRATADA, deverão ser disponibilizados a partir da emissão do Termo de Recebimento Definitivo da solução implantada no ambiente tecnológico do CNPq.

4.4.4. Deverão ser contempladas, no mínimo, as seguintes requisitos:

4.4.4.1. disponibilização de atualizações de software, firmware, assinaturas e bases de inteligência de segurança, sempre que novas versões forem disponibilizadas pelo fabricante;

4.4.4.2. correção de falhas de software identificadas durante o período de vigência contratual, sem custos adicionais para o CNPq;

4.4.4.3. acesso à documentação técnica, base de conhecimento e demais recursos disponibilizados pelo fabricante;

4.4.4.4. disponibilização de canais oficiais de suporte técnico para abertura e acompanhamento de chamados;

4.4.4.5. execução de procedimentos necessários para restabelecimento do funcionamento normal da solução em caso de falhas ou incidentes;

4.4.4.6. disponibilização de atualizações tecnológicas necessárias para manter a solução aderente às boas práticas de segurança da informação e desempenho.

4.4.5. O suporte técnico deverá ser disponibilizado por meio de Central de Atendimento que permita a abertura e acompanhamento de chamados técnicos por meio de sistema web, correio eletrônico ou telefone.

4.4.6. O atendimento deverá estar disponível em regime 24 (vinte e quatro) horas por dia, 7 (sete) dias por semana, durante toda a vigência contratual.

4.4.7. Os atendimentos poderão ser realizados de forma remota ou presencial, conforme a natureza do incidente ou demanda técnica.

4.4.8. Quando necessário, poderá ser realizado atendimento presencial nas dependências do CNPq.

4.4.9. Os serviços de manutenção deverão contemplar, no mínimo, as seguintes modalidades:

4.4.9.1. Manutenção preventiva: A manutenção preventiva consiste na execução planejada de verificações periódicas do funcionamento da solução, com o objetivo de identificar possíveis falhas ou degradações de desempenho antes que causem indisponibilidade dos serviços. Essas atividades poderão incluir:

4.4.9.1.1. verificação da saúde da solução;

4.4.9.1.2. análise de desempenho e utilização de recursos;

4.4.9.1.3. revisão de configurações relevantes;

4.4.9.1.4. verificação de atualizações recomendadas pelo fabricante.

4.4.9.1.5. Quando aplicável, deverá ser emitido relatório técnico contendo as atividades realizadas e eventuais recomendações de melhoria.

4.4.9.2. Manutenção corretiva: A manutenção corretiva consiste na execução de procedimentos destinados a restabelecer o funcionamento normal da solução em caso de falhas, defeitos ou degradação de desempenho. Essas atividades poderão incluir:

4.4.9.2.1. diagnóstico de incidentes;

4.4.9.2.2. correção de falhas de software;

4.4.9.2.3. substituição de componentes defeituosos;

4.4.9.2.4. reinstalação ou reconfiguração de softwares e serviços.

4.4.9.2.2. Caso seja necessária substituição de componentes defeituosos, a CONTRATADA deverá providenciar a reposição por componentes equivalentes ou superiores, sem custos adicionais para o CNPq.

4.4.9.3. Manutenção evolutiva: A manutenção evolutiva consiste na disponibilização e implantação de novas versões de software ou firmware que venham a ser disponibilizadas pelo fabricante durante a vigência contratual. Essas atualizações poderão incluir:

4.4.9.3.1. melhorias de desempenho;

4.4.9.3.2. correções de segurança;

4.4.9.3.3. inclusão de novas funcionalidades;

4.4.9.3.4. adequações tecnológicas recomendadas pelo fabricante.

4.4.10. Os incidentes e solicitações de suporte técnico deverão ser registrados por meio de sistema de chamados, permitindo o acompanhamento de todas as etapas do atendimento.

4.4.10.1. Cada chamado deverá possuir identificação única e conter, no mínimo:

4.4.10.1.1. data e hora de abertura;

4.4.10.1.2. descrição do incidente ou solicitação;

4.4.10.1.3. nível de severidade;

4.4.10.1.4. registro das ações executadas;

4.4.10.1.5. data e hora de encerramento.

4.4.10.1.6. O chamado somente poderá ser considerado encerrado após validação da solução aplicada pelo responsável técnico do CNPq.

4.4.11. Os incidentes registrados deverão ser classificados conforme o nível de severidade, considerando o impacto causado ao ambiente tecnológico e às aplicações institucionais.

4.4.11.1. Os níveis de severidade deverão considerar, entre outros fatores:

4.4.11.1.1. indisponibilidade total da solução;

4.4.11.1.2. degradação significativa de desempenho;

4.4.11.1.3. falhas parciais ou intermitentes;

4.4.11.1.4. solicitações de configuração ou esclarecimentos técnicos.

4.4.12. Durante toda a vigência contratual, a CONTRATADA deverá disponibilizar relatórios periódicos contendo informações sobre os atendimentos realizados.

4.4.12.1. Esses relatórios deverão incluir, no mínimo:

4.4.12.1.1. quantidade de chamados registrados no período;

4.4.12.1.2. classificação por nível de severidade;

4.4.12.1.3. tempo médio de atendimento e resolução;

4.4.12.1.4. descrição dos incidentes e soluções aplicadas.

4.4.12.1.5. Os relatórios servirão como instrumento de acompanhamento dos níveis de serviço contratados e de avaliação da qualidade do suporte prestado.

4.4.13. A solução fornecida deverá contar com garantia e suporte técnico válidos no território nacional durante toda a vigência contratual.

4.4.13.1. A garantia deverá abranger tanto os componentes de hardware quanto os componentes de software que integram a solução.

4.4.13.2. Durante o período de garantia e suporte técnico deverão estar disponíveis, sem custos adicionais para o CNPq:

4.4.13.2.1. atualizações de software e firmware;

4.4.13.2.2. correções de segurança;

4.4.13.2.3. suporte técnico especializado;

4.4.13.2.4. substituição de componentes defeituosos, quando aplicável.

4.5. REQUISITOS TEMPORAIS

4.5.1. Os requisitos temporais da presente contratação estabelecem os prazos estimados para formalização contratual, implantação da solução e início da prestação dos serviços de suporte técnico, considerando a criticidade da infraestrutura de balanceamento de carga e segurança de aplicações do CNPq.

4.5.2. Após a assinatura do contrato, deverá ser realizada reunião inicial de alinhamento entre a equipe técnica do CNPq e a CONTRATADA, com o objetivo de apresentar o ambiente tecnológico do órgão, alinhar as etapas de implantação da solução, definir os responsáveis técnicos e estabelecer os procedimentos operacionais iniciais.

4.5.3. Essa reunião deverá ocorrer no prazo máximo de 10 (dez) dias corridos, contados da assinatura do contrato, observando as boas práticas de planejamento e gestão contratual previstas na Instrução Normativa SGD/ME nº 94/2022, que dispõe sobre o processo de contratação de soluções de tecnologia da informação e comunicação no âmbito da Administração Pública Federal.

4.5.4. O prazo máximo para execução das atividades relacionadas ao fornecimento, entrega e disponibilização dos *appliances*, das licenças de software, das subscrições, dos componentes, acessórios e demais recursos necessários à solução será de até 60 (sessenta) dias corridos, contados a partir da emissão da Ordem de Fornecimento de Bens (OFB) ou instrumento equivalente.

4.5.5. O prazo máximo para execução das atividades relacionadas à instalação, configuração, implantação, integração, testes, validação técnica e disponibilização da solução para entrada em operação será de até 60 (sessenta) dias corridos, contados a partir da emissão da Ordem de Serviço (OS).

4.5.6. Os prazos previstos nos itens 4.5.4 e 4.5.5 poderão ser prorrogados, uma única vez e por igual período, mediante justificativa formal da contratada e aprovação da Administração.

4.5.7. Após a conclusão da implantação da solução e a emissão do Termo de Recebimento Definitivo, terão início a garantia e suporte técnico oficial do fabricante e os serviços de suporte técnico especializado da CONTRATADA, observadas as condições estabelecidas neste Termo de Referência.

4.5.8. O período de garantia e suporte técnico oficial do fabricante e dos serviços de suporte técnico especializado da CONTRATADA deverá ser de 60 (sessenta) meses, contados da emissão do Termo de Recebimento Definitivo.

4.5.9. Após a implantação da solução, poderão ser executadas atividades de apoio técnico especializado destinadas à estabilização do ambiente, ajustes de configuração e otimização de desempenho.

4.5.10. Essas atividades poderão ocorrer durante todo o período contratual, conforme necessidade identificada pelo órgão.

4.5.11. O cronograma de execução deverá contemplar as principais etapas relacionadas à implantação da solução, incluindo planejamento, fornecimento dos equipamentos, instalação, configuração, testes e entrada em produção.

4.5.12. A tabela abaixo apresenta um cronograma indicativo das etapas previstas.

Tabela 05 - Cronograma Indicativo das Etapas Previstas

ATIVIDADE, TAREFA OU SERVIÇO	PRAZO DE ATENDIMENTO
Assinatura do contrato	Contagem Inicial
Reunião inicial de alinhamento	Até 10 dias corridos após assinatura do contrato
Fornecimento dos appliances, licenças de software, subscrições e demais componentes da solução	Até 60 dias corridos a contar da emissão da OFB
Instalação e configuração da solução	Até 60 dias corridos a contar da emissão da OS
Testes e validação técnica	Antes da entrada em produção
Emissão do Termo de Recebimento Definitivo	Até 15 dias úteis após validação da solução
Início dos serviços de garantia e suporte técnico	Após recebimento definitivo da Solução

4.5.12. Os prazos estabelecidos buscam assegurar a implantação adequada da solução sem comprometer a continuidade dos serviços institucionais atualmente suportados pela infraestrutura de balanceamento de carga do CNPq.

4.5.13. A definição desses prazos considera a complexidade da solução a ser implantada, a necessidade de integração com o ambiente tecnológico existente e a criticidade das aplicações institucionais suportadas pela plataforma.

4.5.14. Os atendimentos de suporte técnico deverão observar, no mínimo, os seguintes níveis de serviço (SLA), conforme classificação de severidade:

Tabela 06 – Níveis de Serviço de Suporte Técnico

SEVERIDADE	DESCRIÇÃO	TEMPO DE RESPOSTA	TEMPO DE SOLUÇÃO
Crítica	Indisponibilidade total da solução ou impacto severo em sistemas críticos	Até 1 hora	Até 4 horas
Alta	Degradação significativa de desempenho ou falha relevante	Até 2 horas	Até 8 horas
Média	Falhas parciais ou impacto moderado	Até 4 horas	Até 24 horas

Baixa	Dúvidas, ajustes ou solicitações de serviço	Até 8 horas	Até 48 horas

4.6. REQUISITOS DE SEGURANÇA E PRIVACIDADE

4.6.1. A solução a ser contratada deverá observar integralmente as diretrizes, normas e políticas de segurança da informação adotadas pelo Conselho Nacional de Desenvolvimento Científico e Tecnológico - CNPq, bem como a legislação vigente aplicável à proteção de dados e segurança da informação.

4.6.2. A solução e os serviços associados deverão observar as diretrizes estabelecidas na Política de Segurança da Informação e Comunicações do CNPq (POSIC), bem como a legislação aplicável à proteção de dados pessoais e segurança da informação, especialmente a Lei nº 13.709/2018 (Lei Geral de Proteção de Dados Pessoais – LGPD), além das normas e boas práticas aplicáveis à Administração Pública Federal.

4.6.3. A CONTRATADA deverá manter absoluto sigilo sobre todas as informações, dados, configurações, documentos e comunicações a que tiver acesso em razão da execução contratual. Tais informações não poderão ser divulgadas, reproduzidas ou utilizadas para finalidade diversa da execução do objeto contratado, salvo mediante autorização formal do CNPq.

4.6.4. A obrigação de confidencialidade deverá ser estendida a todos os empregados, prepostos e eventuais subcontratados envolvidos na execução do contrato e permanecerá vigente mesmo após o término ou rescisão da contratação.

4.6.4.1. Todos os profissionais designados pela Contratada deverão assinar Termo de Responsabilidade e Confidencialidade, previamente ao início das atividades, a ser fornecido pela Contratante.

4.6.5. A CONTRATADA deverá observar integralmente o disposto na Lei nº 13.709/2018 (Lei Geral de Proteção de Dados Pessoais – LGPD), adotando medidas técnicas e administrativas adequadas para proteger dados pessoais eventualmente acessados durante a execução contratual. Essas medidas deverão ser suficientes para prevenir acessos não autorizados, perda acidental ou ilícita, destruição, alteração, comunicação ou qualquer forma de tratamento inadequado ou ilícito de dados pessoais.

4.6.6. A CONTRATADA deverá adotar controles adequados de acesso físico e lógico aos recursos tecnológicos do CNPq sob sua responsabilidade, garantindo que o acesso aos sistemas, equipamentos e informações institucionais seja restrito exclusivamente às atividades necessárias à execução do contrato.

4.6.7. Os acessos concedidos deverão permanecer sob controle do CNPq e poderão ser alterados, suspensos ou revogados a qualquer tempo.

4.6.8. Ao término do contrato, ou quando solicitado pela CONTRATANTE, todos os perfis de acesso, contas e credenciais concedidos deverão ser imediatamente revogados.

4.6.9. A CONTRATADA deverá informar ao CNPq todas as credenciais administrativas eventualmente criadas ou utilizadas durante a execução contratual.

4.6.10. As senhas e demais credenciais poderão ser alteradas pela CONTRATANTE a qualquer momento, especialmente ao término do contrato ou quando identificado risco à segurança da informação.

4.6.11. Os recursos de tecnologia da informação disponibilizados pelo CNPq para execução das atividades contratuais deverão ser utilizados exclusivamente para os fins relacionados à execução do objeto contratado, sendo vedada sua utilização para quaisquer outras finalidades que não estejam diretamente relacionadas às atividades previstas no contrato.

4.6.12. A CONTRATADA poderá manter registros técnicos estritamente necessários à execução contratual, desde que tais registros sejam armazenados em ambiente seguro e controlado e utilizados exclusivamente para fins relacionados ao contrato. Esses registros deverão ser protegidos contra acesso não autorizado e, ao término da contratação, deverão ser eliminados ou transferidos ao CNPq, quando aplicável.

4.6.13. A CONTRATADA deverá assegurar que a solução permaneça atualizada com versões oficialmente suportadas pelo fabricante, incluindo atualizações de software, correções de vulnerabilidades e demais melhorias de segurança disponibilizadas durante a vigência contratual.

4.6.14. Todos os documentos, relatórios técnicos, configurações e procedimentos produzidos no âmbito da contratação serão considerados propriedade do CNPq.

4.7. REQUISITOS SOCIAIS, AMBIENTAIS E CULTURAIS

4.7.1. Os equipamentos e serviços devem estar aderentes às seguintes diretrizes sociais, ambientais e culturais:

4.7.1.1. Requisitos Sociais:

4.7.1.1.1. Todos os profissionais da CONTRATADA que desempenharão as atividades em contato direto (físico ou virtual) com a CONTRATANTE deverão cumprir os seguintes requisitos:

4.7.1.1.2. Apresentar-se vestidos de forma adequada ao ambiente de trabalho físico ou virtual, evitando-se o vestuário que caracterize o comprometimento da boa imagem institucional da CONTRATANTE.

4.7.1.1.3. Respeitar todos os servidores, funcionários e colaboradores, em qualquer posição hierárquica, preservando a comunicação e o relacionamento interpessoal construtivo.

4.7.1.1.4. Quando da execução de tarefas no ambiente do CNPq os funcionários da CONTRATADA deverão observar, no trato com os servidores e o público em geral, a urbanidade e os bons costumes de comportamento, tais como: asseio, pontualidade, cooperação, respeito mútuo, discrição e zelo com o patrimônio público. Deverão ainda portar identificação pessoal, conforme as normas internas da Instituição.

4.7.1.1.5. A execução contratual deverá observar, no que couber, as diretrizes estabelecidas pelo Decreto nº 12.122, de 30 de julho de 2024, que institui o Programa Federal de Prevenção e Enfrentamento do Assédio e da Discriminação, devendo a contratada promover ambiente de trabalho pautado pelo respeito, ética, integridade, urbanidade e não discriminação no relacionamento com servidores, colaboradores, terceirizados e demais usuários envolvidos na execução contratual.

4.7.1.2. Requisitos Ambientais:

4.7.1.2.1. A CONTRATADA deverá seguir, no que couber, os requisitos definidos no Guia Nacional de Contratações Sustentáveis da Advocacia Geral da União (AGU) — 8ª Edição, Outubro/2025, disponível em: https://www.gov.br/agu/pt-br/assuntos-1/agu-na-cop30 /central-de-conteudos/edicao_2025_do_guia_final_para_cop30.pdf/

4.7.1.2.2. Igualmente, a CONTRATADA deverá adotar práticas de sustentabilidade ambiental na execução do objeto, no que couber, conforme disposto na Instrução Normativa SLTI/MP nº 01/2010, que dispõe sobre os critérios de sustentabilidade ambiental na aquisição de bens, contratação de serviços ou obras pela Administração Pública Federal direta, autárquica e fundacional e dá outras providências.

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

4.7.1.2.4. As soluções deverão observar práticas de eficiência operacional e uso racional dos recursos computacionais e energéticos, buscando maximizar desempenho, disponibilidade e capacidade de processamento com o menor impacto possível sobre a infraestrutura tecnológica da CONTRATANTE.

4.7.1.2.5. As configurações de hardware e software deverão ser realizadas visando alto desempenho com a utilização racional de energia, evitando-se a sobrecarga de equipamentos ou dispositivos elétricos e eletrônicos.

4.7.1.2.6. Fornecer aos empregados os equipamentos de segurança que se fizerem necessários, para a execução de serviços.

4.7.1.2.7. Respeitar as Normas Brasileiras – NBR publicadas pela Associação Brasileira de Normas Técnicas sobre resíduos sólidos.

4.7.1.2.8. Que os bens devam ser, preferencialmente, acondicionados em embalagem individual adequado, com menor volume possível, que utilize materiais recicláveis, de forma a garantir a máxima proteção durante o transporte e o armazenamento.

4.7.1.2.9. Que os bens não contenham substâncias perigosas em concentração acima da recomendada na diretiva RoHS (*Restriction of Certain Hazardous Substances*), tais como mercúrio (Hg), chumbo (Pb), cromo hexavalente (Cr(VI)), cádmio (Cd), bifenil-polibromados (PBBs), éteres difenil-polibromados (PBDEs).

4.7.1.2.10. Deverá entregar os documentos solicitados na forma digital, com vistas a evitar ou reduzir o uso de papel e impressão, em atendimento ao Art. 9º da Política de Nacional de Resíduos Sólidos (Lei n.º 12.305/ 2010).

4.7.1.2.11. Considerando que a presente contratação poderá contemplar o fornecimento de equipamentos, componentes, acessórios ou outros ativos tecnológicos, deverão ser observadas práticas relacionadas à gestão ambiental durante todo o ciclo de vida dos bens, incluindo reutilização, logística reversa, reciclagem, desfazimento e descarte ambientalmente adequado de equipamentos, componentes e resíduos eletroeletrônicos eventualmente gerados.

4.7.1.2.12. Deverá ser observado planejamento para destinação ambientalmente adequada dos ativos atualmente instalados que venham a ser substituídos, descontinuados ou impactados pela solução objeto da contratação.

4.7.1.2.13. Considerando a eventual substituição ou descontinuidade dos equipamentos atualmente instalados no ambiente do CNPq, após a migração e validação da nova solução, os ativos desativados deverão ser submetidos às seguintes etapas, quando aplicável:

4.7.1.2.13.1. desligamento controlado e retirada do ambiente produtivo;

4.7.1.2.13.2. inventário e avaliação patrimonial dos ativos;

4.7.1.2.13.3. sanitização segura das informações eventualmente armazenadas, incluindo arquivos de configuração, credenciais, certificados digitais, chaves criptográficas, logs e demais dados operacionais;

4.7.1.2.13.4. definição da destinação administrativa aplicável, podendo contemplar remanejamento interno, reaproveitamento, desfazimento, logística reversa, reciclagem ou descarte ambientalmente adequado;

4.7.1.2.13.5. observância da legislação aplicável ao gerenciamento de resíduos eletroeletrônicos e das normas internas do CNPq relativas ao desfazimento patrimonial.

4.7.1.2.14. Previamente ao desfazimento, remanejamento, descarte ou destinação dos ativos substituídos, deverá ser realizada sanitização segura das informações eventualmente armazenadas, visando impedir recuperação indevida ou vazamento de informações institucionais.

4.7.1.3. Requisitos Culturais:

4.7.1.3.1. Toda a documentação produzida e/ou fornecida pela CONTRATADA referente ao objeto deverá estar preferencialmente no idioma Português-BR, de forma clara e objetiva.

4.8. REQUISITOS DA ARQUITETURA TECNOLÓGICA

4.8.1. Os equipamentos e serviços deverão observar integralmente os requisitos de arquitetura tecnológica estabelecidos pela área técnica do CONTRATANTE.

4.8.2. A solução de Application Delivery Controller (ADC) deverá ser fornecida em arquitetura de alta disponibilidade, composta por 02 (dois) appliances, destinados à operação em cluster, de forma a garantir a continuidade e disponibilidade dos serviços institucionais.

4.8.3. Todos os equipamentos fornecidos deverão ser novos, de primeiro uso, estar em linha de produção do fabricante e disponíveis comercialmente no mercado, não sendo aceitas funcionalidades previstas apenas em roadmap ou em estágio experimental (beta).

4.8.4. A solução deverá ser composta por plataforma especializada de balanceamento de aplicações e segurança de aplicações, baseada em appliances dedicados, não sendo aceitas soluções baseadas em servidores de uso geral, estações de trabalho ou equipamentos genéricos adaptados para execução das funções de balanceamento de carga e proteção de aplicações.

4.8.5. Toda a solução deverá ser fornecida por um único fabricante, incluindo hardware e software, garantindo integração plena entre os componentes da plataforma, interoperabilidade, simplificação da administração do ambiente e redução da complexidade operacional.

4.8.6. A arquitetura deverá permitir operação em cluster de alta disponibilidade, assegurando sincronização de configurações e continuidade operacional em caso de falha de um dos equipamentos.

4.8.7. A CONTRATADA deverá fornecer todos os recursos necessários ao pleno funcionamento da solução, incluindo os appliances, as licenças de software, as subscrições, acessórios, cabeamentos e demais componentes necessários à implantação e operação da plataforma no ambiente tecnológico do CNPq.

4.8.8. Nenhum dos componentes da solução poderá possuir anúncio de *End of Sale (EoS) ou End of Life (EoL)* no momento do aceite definitivo da solução. Caso tal situação seja identificada, o fornecedor deverá substituir o equipamento por modelo equivalente ou superior, sem custos adicionais para o CNPq.

4.8.9. Caso, durante a vigência contratual, qualquer componente da solução venha a ser descontinuado pelo fabricante ou tenha anúncio de *End of Sale (EoSale), End of Support (EoSup), End of Life (EoL)* ou condição equivalente que comprometa a continuidade do suporte técnico, garantia, atualizações, disponibilidade de peças de reposição ou manutenção da solução, a CONTRATADA deverá providenciar, sem ônus adicional para o CNPq, a substituição por outro componente novo e de primeiro uso, com características técnicas iguais ou superiores, plenamente compatível com a arquitetura da solução e que possua suporte técnico oficial vigente do fabricante durante todo o período remanescente da contratação.

4.8.10. Todos os componentes e funcionalidades da solução deverão ser fornecidos com as respectivas licenças de software, subscrições e demais direitos de uso necessários ao seu pleno funcionamento, incluindo todas as funcionalidades requeridas para operação da plataforma de balanceamento de carga e proteção de aplicações.

4.8.11. As licenças de software fornecidas deverão possuir caráter permanente, permitindo a permanência operacional da solução após o término do período contratual, assegurando a continuidade de funcionamento da plataforma, ainda que sem acesso a novas atualizações, subscrições, assinaturas de segurança ou suporte técnico.

4.8.12. Os equipamentos deverão possuir fontes de alimentação redundantes e hot-swappable, compatíveis com a infraestrutura elétrica do ambiente tecnológico do CNPq.

4.8.13. Os equipamentos deverão ser compatíveis com racks padrão de 19 (dezenove) polegadas, devendo ser fornecidos com todos os acessórios necessários à instalação física.

4.8.14. Os equipamentos fornecidos deverão possuir certificações e homologações aplicáveis no Brasil, emitidas pelos órgãos competentes, quando exigidas pela legislação.

4.8.15. A CONTRATADA deverá realizar todas as atividades necessárias à implantação da solução, incluindo instalação, configuração, integração com o ambiente existente, migração de configurações, testes de funcionamento e entrada em operação.

4.8.16. As especificações técnicas mínimas da solução, incluindo requisitos de desempenho, funcionalidades e características complementares, encontram-se descritas no Anexo I - Especificação Técnica Mínima da Solução, integrante deste Termo de Referência.

4.8.17. Os requisitos arquiteturais definidos visam assegurar a padronização tecnológica do ambiente de entrega de aplicações do CNPq, garantindo interoperabilidade entre componentes, simplificação da administração da plataforma e redução da complexidade operacional, especialmente em ambiente de missão crítica.

4.9. REQUISITOS DE PROJETO E DE IMPLEMENTAÇÃO

4.9.1. A implantação da solução deverá contemplar todas as atividades necessárias para que a plataforma de balanceamento de aplicações e firewall de aplicações web seja plenamente operacional no ambiente tecnológico do CNPq.

4.9.2. Durante a fase de implantação, a CONTRATADA deverá elaborar e apresentar Projeto Executivo de Implantação, contendo o detalhamento das etapas de implementação da solução, cronograma de execução e descrição das atividades técnicas necessárias para a plena operacionalização do ambiente.

4.9.3. O Projeto Executivo deverá ser submetido à análise e aprovação da equipe técnica do CNPq antes do início das atividades de implantação.

4.9.4. O Projeto Executivo deverá contemplar, no mínimo:

4.9.4.1. levantamento da infraestrutura tecnológica relacionada à solução, incluindo equipamentos, softwares, licenças, conectividade e demais componentes envolvidos;

4.9.4.2. definição do escopo da solução a ser implantada e dos componentes que a integram;

4.9.4.3. identificação dos ativos que compõem a arquitetura da solução, incluindo interconexões físicas e lógicas, interfaces de rede e integrações necessárias;

4.9.4.4. definição dos parâmetros de configuração da solução, incluindo endereçamento IP, segmentação de rede, políticas de balanceamento de carga, políticas de segurança, parâmetros de roteamento e demais elementos necessários ao funcionamento da plataforma;

4.9.4.5. elaboração da arquitetura lógica da solução, com representação da topologia proposta e das integrações com a infraestrutura existente;

4.9.4.6. elaboração da arquitetura física da solução, incluindo o mapeamento das conexões físicas necessárias entre os equipamentos da solução e os dispositivos de rede do ambiente do CNPq;

4.9.4.7. definição de procedimentos de contingência e plano de *rollback*, descrevendo as ações necessárias para restabelecimento do ambiente em caso de falhas durante o processo de implantação;

4.9.4.8. elaboração e execução de plano de migração das regras, políticas e *iRules* atualmente configuradas no ambiente em operação, assegurando sua adequada transposição, compatibilidade e funcionamento na nova solução.

4.9.5. A instalação e configuração da solução deverão ser planejadas e executadas de forma a assegurar a interoperabilidade com a infraestrutura tecnológica existente no CNPq, evitando impactos aos serviços em produção.

4.9.6. Durante a execução das atividades de implantação, a CONTRATADA deverá atuar sob supervisão da equipe técnica do CNPq, garantindo que as mudanças no ambiente sejam realizadas de forma controlada e documentada.

4.9.7. Caso sejam identificadas necessidades de ajustes no projeto durante a execução das atividades de implantação, a CONTRATADA deverá submeter as alterações propostas à avaliação e aprovação do Fiscal Técnico do Contrato antes de sua implementação.

4.10. REQUISITOS DE IMPLANTAÇÃO

4.10.1. A CONTRATADA será responsável pela execução integral das atividades necessárias para implantação da solução de balanceamento de aplicações e firewall de aplicações web no ambiente tecnológico do CNPq.

4.10.2. A implantação deverá contemplar todas as etapas necessárias para que a solução seja plenamente operacional, incluindo o fornecimento dos appliances, das licenças de software, das subscrições, instalação física, configuração lógica, integração com a infraestrutura existente, realização de testes e entrada em produção.

4.10.3. Compete à CONTRATADA, no mínimo:

4.10.3.1. responsabilizar-se pela completa implantação da solução, incluindo todos os custos necessários à operacionalização dos appliances, das licenças de software, das subscrições e dos demais componentes fornecidos;

4.10.3.2. disponibilizar todos os instrumentos, ferramentas e recursos técnicos necessários para execução das atividades de instalação, configuração e testes da solução;

4.10.3.3. realizar a entrega dos equipamentos e demais componentes da solução nos locais de instalação definidos pelo CNPq, responsabilizando-se pelas atividades de transporte, embalagem, desembalagem e demais procedimentos logísticos necessários;

4.10.3.4. realizar a instalação física e lógica dos equipamentos e componentes da solução, de acordo com o Projeto Executivo previamente aprovado;

4.10.3.5. executar as atividades necessárias de configuração e adequação dos equipamentos e softwares fornecidos, garantindo sua correta integração com o ambiente tecnológico do CNPq;

4.10.3.6. realizar a migração controlada das configurações e serviços existentes para a nova solução, incluindo políticas de balanceamento, regras de segurança, certificados digitais e demais parâmetros necessários ao funcionamento do ambiente;

4.10.3.7. planejar e executar as atividades de integração da solução com a infraestrutura de rede existente, de modo a evitar impactos nos serviços em produção;

4.10.3.8. elaborar e apresentar Plano de Homologação e Testes, contendo a descrição dos procedimentos e critérios de validação da solução implantada;

4.10.3.9. executar os testes funcionais e operacionais previstos no Plano de Homologação e Testes, de forma a verificar o correto funcionamento de todos os componentes de hardware e software envolvidos;

4.10.3.10. elaborar e entregar a documentação técnica final da solução implantada, incluindo registros de configuração, arquitetura implementada e demais informações necessárias para operação e manutenção do ambiente.

4.10.4. Durante a implantação da solução poderão ser executadas atividades como instalação de softwares, migração de regras e políticas de segurança, elaboração e execução de scripts, ajustes de configuração, análise de desempenho, otimização de parâmetros de funcionamento e resolução de eventuais incidentes técnicos.

4.10.5. Quando necessário, determinadas atividades poderão ser executadas em janelas de manutenção previamente acordadas com o CNPq, inclusive em horários noturnos ou fins de semana, de forma a minimizar impactos nos serviços institucionais.

4.10.6. Compete ao CNPq acompanhar as atividades de implantação, fornecer informações necessárias sobre a infraestrutura existente e definir, quando necessário, as janelas de intervenção para execução das atividades técnicas.

4.10.7. Ao término das atividades de implantação deverá ser realizado processo formal de validação da solução implantada, com verificação do atendimento aos requisitos técnicos definidos.

4.10.8. A CONTRATADA deverá realizar a análise detalhada do ambiente atual da CONTRATANTE, contemplando a identificação, documentação, adaptação e migração de todas as configurações existentes, incluindo, mas não se limitando a:

4.10.8.1. virtual servers;
4.10.8.2. pools e nodes;

4.10.8.3. perfis de tráfego;
4.10.8.4. políticas de balanceamento;
4.10.8.5. políticas de segurança (WAF);
4.10.8.6. *iRules* e demais mecanismos de customização;
4.10.8.7. integrações com sistemas institucionais.

4.10.9. A migração deverá ser executada de forma controlada, planejada e validada, garantindo a preservação integral das funcionalidades atualmente em operação, sem degradação de desempenho, disponibilidade ou segurança.

4.10.10. A CONTRATADA será responsável por realizar testes de validação, homologação e operação assistida, assegurando a plena funcionalidade da solução no ambiente de produção.

4.11. REQUISITOS DE GARANTIA, MANUTENÇÃO E ASSISTÊNCIA TÉCNICA

4.11.1. A solução fornecida deverá possuir garantia e suporte técnico oficial do fabricante, bem como as respectivas subscrições e assinaturas de segurança, pelo período mínimo de 60 (sessenta) meses, contados da emissão do Termo de Recebimento Definitivo da solução implantada no ambiente tecnológico do CNPq.

4.11.2. O prazo de garantia estabelecido considera a natureza da solução a ser contratada, composta por ativos de rede, segurança e entrega de aplicações de missão crítica, cuja vida útil estimada é de, no mínimo, 5 (cinco) anos, sendo a contratação da garantia durante todo esse período medida tecnicamente adequada e economicamente mais vantajosa para a Administração.

4.11.3. A garantia e suporte técnico oficial do fabricante deverão abranger todos os componentes da solução fornecida, incluindo, no mínimo:

4.11.3.1. hardware;

4.11.3.2. software;

4.11.3.3. licenças;

4.11.3.4. módulos e funcionalidades contratadas;

4.11.3.5. firmwares;

4.11.3.6. assinaturas, bases de proteção e demais mecanismos associados à segurança da solução, quando aplicável.

4.11.4. Durante o período de garantia, suporte técnico oficial do fabricante e vigência das subscrições de segurança deverão estar contemplados, sem ônus adicional para o CNPq:

4.11.4.1. correção de falhas e defeitos de hardware e software;

4.11.4.2. atualização de versões do sistema operacional da plataforma;

4.11.4.3. atualização de módulos de software e funcionalidades da solução;

4.11.4.4. atualização de firmwares e componentes embarcados;

4.11.4.5. disponibilização de correções de segurança, patches e hotfixes publicados pelo fabricante;

4.11.4.6. atualização de assinaturas, mecanismos de proteção e demais recursos de segurança associados às funcionalidades contratadas, quando aplicável;

4.11.4.7. direito ao recebimento e utilização de novas versões, correções, melhorias e evoluções disponibilizadas pelo fabricante para a solução fornecida.

4.11.4.8. A garantia técnica deverá assegurar a plena operacionalidade da solução em todas as funcionalidades contratadas, abrangendo tanto aquelas descritas nas especificações do objeto quanto as previstas nos manuais, catálogos e demais documentos técnicos oficiais do fabricante.

4.11.5. A garantia deverá cobrir a resolução de falhas, erros, defeitos, instabilidades, vulnerabilidades, degradação de desempenho ou quaisquer ocorrências que venham a afetar os componentes físicos ou lógicos da solução fornecida.

4.11.6. Sempre que necessário, a garantia deverá incluir a substituição total ou parcial de *appliances*, módulos, licenças ou componentes que apresentem defeito ou falha de funcionamento, sem ônus adicional para o CNPq.

4.11.7. Os equipamentos, peças, módulos ou componentes substituídos deverão ser novos, originais, de primeiro uso e possuir características técnicas equivalentes ou superiores às dos itens substituídos.

4.11.8. Os componentes substituídos durante o período de garantia deverão manter, no mínimo, o mesmo prazo de garantia originalmente contratado, observando-se a solução como um todo e suas funcionalidades associadas.

4.11.9. A CONTRATADA deverá assegurar que a solução permaneça plenamente suportada pelo fabricante durante todo o período de vigência da garantia, do suporte técnico oficial e das subscrições contratadas, incluindo a disponibilidade de peças de reposição, atualizações, correções de software e demais recursos necessários à manutenção da solução em operação.

4.11.10. As atualizações, correções e novas versões disponibilizadas pelo fabricante deverão ser instaladas pela CONTRATADA sempre que necessário, mediante planejamento conjunto com a equipe técnica do CNPq, de forma a preservar a estabilidade do ambiente e minimizar impactos aos serviços em produção.

4.11.11. A garantia deverá ser prestada pelo fabricante, permanecendo, em qualquer hipótese, a CONTRATADA integralmente responsável pelo cumprimento das condições estabelecidas no contrato.

4.11.12. Correrão por conta exclusiva da CONTRATADA todas as despesas relacionadas ao deslocamento de pessoal técnico, transporte, retirada, entrega, frete, reposição, substituição e demais providências necessárias à execução dos serviços de garantia.

4.11.13. Os componentes eventualmente removidos ou substituídos durante atividades de manutenção não ficarão sob responsabilidade do CNPq, cabendo à contratada providenciar sua retirada e destinação final ambientalmente adequada, em conformidade com a legislação aplicável, especialmente a Lei nº 12.305/2010, que institui a Política Nacional de Resíduos Sólidos.

4.11.13.1. Quando aplicável, deverão ser observadas práticas de reutilização, reaproveitamento, logística reversa, reciclagem e descarte ambientalmente adequado dos equipamentos, peças, componentes e resíduos eletroeletrônicos decorrentes das atividades de garantia e substituição da solução.

4.11.13.2. Os ativos eventualmente substituídos ou descontinuados em decorrência da contratação deverão observar procedimento de desligamento controlado, sanitização segura das informações eventualmente armazenadas e destinação final ambientalmente adequada, observadas o art. 18, §1º, inciso XII da Lei nº 14.133/2021, normas internas do CNPq e legislações aplicáveis.

4.11.14. Caso, durante a vigência contratual, qualquer componente da solução venha a ser descontinuado pelo fabricante ou deixe de possuir suporte técnico oficial (*End of Support – EoSup*, *End of Sale – EoS* ou *End of Life – EoL*), a CONTRATADA deverá providenciar, sem ônus adicional para o CNPq, a substituição por outro componente novo, de primeiro uso, com características técnicas equivalentes ou superiores, plenamente compatível com a arquitetura da solução e com suporte vigente durante todo o período remanescente do contrato.

4.11.15. A substituição prevista no item anterior deverá assegurar a continuidade da operação da solução, preservando as funcionalidades existentes, os níveis de desempenho, as integrações com o ambiente tecnológico do CNPq e as políticas de segurança previamente estabelecidas.

4.11.16. O detalhamento dos procedimentos, prazos, níveis de atendimento e demais condições relativas à garantia, suporte técnico e assistência técnica observará as disposições estabelecidas neste Termo de Referência e em seus anexos.

4.12. REQUISITOS DE EXPERIÊNCIA PROFISSIONAL

4.12.1. Os serviços de implantação, configuração, suporte técnico e garantia da solução deverão ser prestados por profissionais devidamente capacitados nos produtos em questão, com qualificação compatível com os produtos e tecnologias envolvidos, bem como com todos os recursos técnicos e ferramentais necessários à adequada execução contratual.

4.12.2. Para fins de qualificação técnica, a licitante deverá comprovar aptidão para a execução de objeto compatível com o desta contratação, por meio da apresentação de atestado(s) de capacidade técnica emitido(s) por pessoa jurídica de direito público ou privado.

4.12.3. Os atestados deverão comprovar experiência na execução de serviços relacionados ao fornecimento, implantação, configuração ou suporte de soluções de Application Delivery Controller (ADC) com funcionalidades de Web Application Firewall (WAF), em ambiente de produção e, preferencialmente, em arquitetura de alta disponibilidade.

4.12.4. Para fins de comprovação da capacidade técnico-operacional, será exigida a apresentação de, no mínimo, 1 (um) atestado de capacidade técnica compatível, em características e complexidade, com o objeto desta contratação.

4.12.5. Os atestados deverão conter informações suficientes para a verificação de sua autenticidade e veracidade, incluindo, sempre que possível:

4.12.5.1. identificação da entidade contratante;
4.12.5.2. descrição do objeto contratado;
4.12.5.3. período de execução;
4.12.5.4. identificação do responsável pelas informações.

4.12.6. Será admitida a apresentação de um ou mais atestados para fins de comprovação da experiência exigida, desde que demonstrada a compatibilidade com o objeto da contratação.

4.12.7. A Administração poderá, a qualquer tempo, realizar diligências junto aos emitentes dos atestados, com o objetivo de verificar a efetiva execução dos serviços declarados, nos termos da legislação vigente.

4.13. REQUISITOS DE FORMAÇÃO DA EQUIPE

4.13.1. Considerando a natureza e a complexidade técnica da solução, a contratada deverá dispor de equipe técnica em quantidade e qualificação suficientes para execução integral das atividades previstas no objeto da contratação.

4.13.2. O dimensionamento da equipe técnica necessária à execução do objeto será de responsabilidade exclusiva da contratada, devendo ser compatível com o escopo contratado e suficiente para assegurar o cumprimento integral dos requisitos, prazos, níveis de serviço e demais obrigações estabelecidas neste Termo de Referência.

4.13.3. Caberá à contratada definir a composição, quantidade e distribuição dos profissionais necessários à execução das atividades de fornecimento, instalação, configuração, implantação, migração, suporte técnico, garantia e demais serviços associados à solução.

4.13.4. A equipe disponibilizada deverá possuir capacitação técnica compatível com as atividades executadas, observadas as tecnologias, níveis de criticidade e requisitos operacionais envolvidos na contratação.

4.14. REQUISITOS DE METODOLOGIA DE TRABALHO

4.14.1. O fornecimento dos bens e a execução dos serviços estarão condicionados ao recebimento, pela CONTRATADA, de Ordem de Fornecimento de Bens (OFB) e/ou Ordem de Serviço (OS), emitida pela CONTRATANTE.

4.14.2. A OFB/OS indicará o tipo de fornecimento ou serviço, a quantidade, o local de execução e demais informações necessárias para a realização das atividades.

4.14.3. O CONTRATADO deve fornecer meios para contato e registro de ocorrências da seguinte forma: com funcionamento ***24*** horas por dia e ***7*** dias por semana de maneira eletrônica e ***24*** horas por dia e ***7*** dias por semana por via telefônica.

4.14.4. O andamento do fornecimento dos equipamentos e da execução dos serviços deverá ser acompanhado pela CONTRATADA, que dará ciência de eventuais acontecimentos à Contratante.

4.14.5. A execução contratual observará o princípio da segregação de responsabilidades, cabendo à CONTRATANTE a gestão e fiscalização do contrato e à CONTRATADA a execução dos serviços e a gestão de seus recursos.

4.14.6. Os serviços deverão ser executados em conformidade com as boas práticas de mercado, recomendações do fabricante da solução e diretrizes técnicas do ambiente do CONTRATANTE.

4.14.7. A CONTRATADA deverá registrar e manter documentação atualizada das atividades realizadas, incluindo atendimentos, manutenções, atualizações e demais intervenções no ambiente.

4.14.8. A CONTRATADA deverá indicar formalmente preposto responsável pela interlocução com a CONTRATANTE e pelo acompanhamento da execução contratual.

4.14.9. Os serviços prestados estarão sujeitos à avaliação da CONTRATANTE quanto ao atendimento dos requisitos técnicos, níveis de serviço e demais condições contratuais.

4.15. REQUISITOS DE SEGURANÇA DA INFORMAÇÃO E PRIVACIDADE

4.15.1. O Contratado deverá observar integralmente os requisitos de Segurança da Informação e Privacidade descritos a seguir:

4.15.1.1. A solução a ser contratada deverá observar integralmente as diretrizes, normas e políticas de segurança da informação adotadas pelo Conselho Nacional de Desenvolvimento Científico e Tecnológico - CNPq, bem como a legislação vigente aplicável à proteção de dados e segurança da informação.

4.15.1.2. A solução e os serviços associados deverão observar as diretrizes estabelecidas na Política de Segurança da Informação e Comunicações do CNPq (POSIC), bem como a legislação aplicável à proteção de dados pessoais e segurança da informação, especialmente a Lei nº 13.709/2018 (Lei Geral de Proteção de Dados Pessoais – LGPD), além das normas e boas práticas aplicáveis à Administração Pública Federal.

4.15.1.3. A CONTRATADA deverá manter absoluto sigilo sobre todas as informações, dados, configurações, documentos e comunicações a que tiver acesso em razão da execução contratual. Tais informações não poderão ser divulgadas, reproduzidas ou utilizadas para finalidade diversa da execução do objeto contratado, salvo mediante autorização formal do CNPq.

4.15.1.4. A obrigação de confidencialidade deverá ser estendida a todos os empregados, prepostos e eventuais subcontratados envolvidos na execução do contrato e permanecerá vigente mesmo após o término ou rescisão da contratação.

4.15.1.5. A CONTRATADA deverá observar integralmente o disposto na Lei nº 13.709/2018 (Lei Geral de Proteção de Dados Pessoais – LGPD), adotando medidas técnicas e administrativas adequadas para proteger dados pessoais eventualmente acessados durante a execução contratual. Essas medidas deverão ser suficientes para prevenir acessos não autorizados, perda acidental ou ilícita, destruição, alteração, comunicação ou qualquer forma de tratamento inadequado ou ilícito de dados pessoais.

4.15.1.6. A CONTRATADA deverá adotar controles adequados de acesso físico e lógico aos recursos tecnológicos do CNPq sob sua responsabilidade, garantindo que o acesso aos sistemas, equipamentos e informações institucionais seja restrito exclusivamente às atividades necessárias à execução do contrato.

4.15.1.7. Os acessos concedidos deverão permanecer sob controle do CNPq e poderão ser alterados, suspensos ou revogados a qualquer tempo.

4.15.1.8. Ao término do contrato, ou quando solicitado pela CONTRATANTE, todos os perfis de acesso, contas e credenciais concedidos deverão ser imediatamente revogados.

4.15.1.9. A CONTRATADA deverá informar ao CNPq todas as credenciais administrativas eventualmente criadas ou utilizadas durante a execução contratual.

4.15.1.10. As senhas e demais credenciais poderão ser alteradas pela CONTRATANTE a qualquer momento, especialmente ao término do contrato ou quando identificado risco à segurança da informação.

4.15.1.11. Os recursos de tecnologia da informação disponibilizados pelo CNPq para execução das atividades contratuais deverão ser utilizados exclusivamente para os fins relacionados à execução do objeto contratado, sendo vedada sua utilização para quaisquer outras finalidades que não estejam diretamente relacionadas às atividades previstas no contrato.

4.15.1.12. A CONTRATADA poderá manter registros técnicos estritamente necessários à execução contratual, desde que tais registros sejam armazenados em ambiente seguro e controlado e utilizados exclusivamente para fins relacionados ao contrato. Esses registros deverão ser protegidos contra acesso não autorizado e, ao término da contratação, deverão ser eliminados ou transferidos ao CNPq, quando aplicável.

4.15.1.13. A CONTRATADA deverá assegurar que a solução permaneça atualizada com versões oficialmente suportadas pelo fabricante, incluindo atualizações de software, correções de vulnerabilidades e demais melhorias de segurança disponibilizadas durante a vigência contratual.

4.15.1.14. Todos os documentos, relatórios técnicos, configurações e procedimentos produzidos no âmbito da contratação serão considerados propriedade do CNPq.

4.16. VISTORIA

4.16.1. Considerando as características do objeto, faculta-se aos interessados a realização de vistoria técnica prévia, com a finalidade exclusiva de obtenção de conhecimento adicional acerca das condições e peculiaridades do ambiente onde os serviços poderão ser executados.

4.16.2. A vistoria técnica, quando houver interesse do licitante, deverá ser previamente agendada junto à CONTRATANTE por meio dos seguintes canais:

4.16.2.1. E-mail: ***contratos_ti@cnpq.br***

4.16.3. A vistoria será realizada em dias úteis, de segunda a sexta-feira, no horário compreendido entre 09h00 (nove horas) e 17h00 (dezessete horas), sendo acompanhada por servidor designado pelo CNPq.

4.16.4. A vistoria será realizada nas dependências do Conselho Nacional de Desenvolvimento Científico e Tecnológico - CNPq, no seguinte endereço: ***Setor de Autarquias Sul (SAUS), Quadra 01, Lote 06, Bloco H – Edifício Telemundi II, Asa Sul, Brasília/DF, CEP 70070-010.***

4.16.5. O representante da empresa deverá estar devidamente identificado, mediante apresentação de documento de identidade civil e comprovação de vínculo com a empresa interessada.

4.16.6. Quando realizada, a vistoria técnica será formalizada por meio de Termo de Vistoria Técnica, conforme modelo constante no Anexo V deste Termo de Referência, o qual deverá ser assinado pelo representante da empresa e pelo servidor designado pela CONTRATANTE.

4.16.7. Caso o interessado opte por não realizar a vistoria, poderá apresentar declaração formal de que possui pleno conhecimento das condições e peculiaridades do objeto da contratação, conforme modelo constante no Anexo VI (Termo de recusa de vistoria técnica).

4.16.8. A não realização da vistoria não poderá ser utilizada como justificativa para alegações posteriores de desconhecimento das condições do ambiente, das instalações ou das exigências necessárias à execução dos serviços, permanecendo sob responsabilidade exclusiva da CONTRATADA a adequada formulação de sua proposta.

4.17. SUSTENTABILIDADE

4.17.1. Além dos critérios de sustentabilidade eventualmente inseridos no item 4.7 (Requisitos sociais, ambientais e culturais), devem ser atendidos os seguintes requisitos, que se baseiam no Guia Nacional de Contratações Sustentáveis, no que for aplicável ao objeto:

4.17.1.1. Os critérios e práticas de sustentabilidade deverão ser fundamentados no desenvolvimento econômico, social e na conservação do meio ambiente, além de serem baseados nas diretrizes de sustentabilidade como menor impacto sobre recursos naturais, preferência para materiais, tecnologias e matérias-primas de origem local e maior eficiência na utilização de recursos naturais como água e energia.

4.18. INDICAÇÃO DE MARCAS OU MODELOS

4.18.1. Na presente contratação será admitida a indicação da(s) seguinte(s) marca(s), característica(s) ou modelo(s), de acordo com as justificativas contidas nos Estudos Técnicos Preliminares:

4.18.1.1. Admite-se a indicação da solução da fabricante F5 Networks, linha BIG-IP, como referência tecnológica, em razão da sua utilização consolidada no ambiente do CNPq, o que assegura a compatibilidade com a arquitetura existente, a manutenção da padronização tecnológica e a continuidade operacional dos serviços institucionais.

4.18.1.2. A adoção da referida solução mostra-se adequada para garantir os níveis de desempenho, disponibilidade e segurança requeridos para o ambiente de balanceamento de carga e proteção de aplicações, não configurando restrição indevida à competitividade, uma vez que a solução é amplamente disponível no mercado por meio de diversos fornecedores e canais autorizados de comercialização.

4.19. DA VEDAÇÃO DE UTILIZAÇÃO DE MARCA/PRODUTO NA EXECUÇÃO DO SERVIÇO

4.19.1. Não se aplica para essa contratação.

4.20. DA EXIGÊNCIA DE CARTA DE SOLIDARIEDADE

4.20.1. Em caso de fornecedor, revendedor ou distribuidor, será exigida do licitante provisoriamente classificado em primeiro lugar, como condição para a assinatura do contrato, carta de solidariedade emitida pelo fabricante, que assegure a execução do contrato, nos termos do art. 41, inciso IV, da Lei nº 14.133/2021.

4.20.2. A exigência, de caráter excepcional e devidamente justificada no Estudo Técnico Preliminar (SEI nº 2745503), decorre da criticidade da solução de *Application Delivery Controller (ADC)* e *Web Application Firewall (WAF)*, responsável pela entrega, disponibilidade e proteção de aplicações institucionais críticas do CNPq, bem como da necessidade de assegurar a continuidade do suporte oficial do fabricante, a atualização tecnológica, a disponibilidade de peças de reposição, as correções de segurança e a regularidade da cadeia de fornecimento da solução ofertada.

4.21. SUBCONTRATAÇÃO

4.21.1. Não será admitida a subcontratação do objeto contratual.

4.22. DA EXIGÊNCIA DE AMOSTRA

4.22.1. Não se aplica, tendo em vista a natureza da solução.

4.23. GARANTIA DA CONTRATAÇÃO

4.23.1. Será exigida a garantia da contratação de que tratam os arts. 96 e seguintes da Lei nº 14.133, de 2021, com validade durante a execução do contrato e 90 (noventa) dias após término da vigência contratual, podendo o Contratado optar pela caução em dinheiro ou em títulos da dívida pública, seguro-garantia, fiança bancária ou título de capitalização, em valor correspondente a 5% (cinco por cento) do valor total da contratação

4.23.2. Em caso de opção pelo seguro-garantia, a parte adjudicatária deverá apresentá-la, no máximo, até a data de assinatura do contrato.

4.23.2.1. A apólice de seguro-garantia permanecerá em vigor mesmo que o Contratado não pague o prêmio nas datas convencionadas.

4.23.2.2. Caso o adjudicatário não apresente a apólice de seguro de garantia antes da assinatura do contrato, ocorrerá a preclusão do direito de escolha dessa modalidade de garantia.

4.23.2.3. A apólice de seguro-garantia deverá acompanhar as modificações referentes à vigência do contrato principal mediante a emissão do respectivo endosso pela seguradora.

4.23.2.4. Será permitida a substituição da apólice de seguro-garantia na data de renovação ou de aniversário, desde que mantidas as condições e coberturas da apólice vigente e nenhum período fique descoberto, ressalvados os períodos de suspensão contratual.

4.23.2.5. Caso o adjudicatário não opte pelo seguro-garantia ou não apresente a apólice de seguro de garantia antes da assinatura do contrato, deverá apresentar, no prazo máximo de 10 (dez) dias úteis, prorrogáveis por igual período, a critério do CONTRATANTE, contado da assinatura do contrato, comprovante de prestação de garantia nas modalidades de caução em dinheiro ou títulos da dívida pública, fiança bancária ou títulos de capitalização.

4.23.3. Caso seja a garantia em dinheiro a modalidade de garantia escolhida pelo Contratado, deverá ser efetuada em favor do CONTRATANTE, em conta específica na Caixa Econômica Federal, com correção monetária

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

4.23.5. No caso de garantia na modalidade de fiança bancária, deverá ser emitida por banco ou instituição financeira devidamente autorizada a operar no País pelo Banco Central do Brasil, e deverá constar expressa renúncia do fiador aos benefícios do artigo 827 do Código Civil.

4.23.6. Na hipótese de opção pelo título de capitalização, a garantia deverá ser custeada por pagamento único, com resgate pelo valor total, sob a modalidade de instrumento de garantia, emitido por sociedades de capitalização regulamente constituídas e autorizadas pelo Governo Federal.

4.23.6.1. O título de capitalização deverá ser apresentado ao CONTRATANTE juntamente com as condições gerais e o número do processo administrativo sob o qual o plano de capitalização foi aprovado pela Susep (art. 8º, III, da Circular SUSEP nº 656, de 11 de março de 2022).

4.23.7. A garantia assegurará, qualquer que seja a modalidade escolhida, sob pena de não aceitação, o pagamento de:

4.23.7.1. prejuízos advindos do não cumprimento do objeto do contrato e do não adimplemento das demais obrigações nele previstas;

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

4.23.7.3. obrigações trabalhistas e previdenciárias de qualquer natureza e para com o FGTS, não adimplidas pelo Contratado.

4.23.8. Em caso de seguro-garantia, a apólice deverá ter cobertura para pagamento direto ao empregado após decisão definitiva em processo administrativo que apure montante líquido e certo a ele devido em razão de inadimplência do Contratado, independentemente de trânsito em julgado de decisão judicial

4.23.9. No caso de alteração do valor do contrato, ou prorrogação de sua vigência, a garantia deverá ser ajustada ou renovada, no prazo máximo de 10 (dez) dias úteis, prorrogáveis por igual período, contado da data de assinatura do termo aditivo ou da emissão do apostilamento, seguindo os mesmos parâmetros utilizados quando da contratação.

4.23.10. Na hipótese de suspensão do contrato por ordem ou inadimplemento da Administração, o Contratado ficará desobrigado de renovar a garantia ou de endossar a apólice de seguro até a ordem de reinício da execução ou o adimplemento pela Administração.

4.23.11. Se o valor da garantia for utilizado total ou parcialmente em pagamento de qualquer obrigação, o Contratado obriga-se a fazer a respectiva reposição no prazo máximo de 10 (dez) dias úteis, prorrogáveis por igual período, a critério do CONTRATANTE, contados da data em que for notificada

4.23.12. O CONTRATANTE executará a garantia na forma prevista na legislação que rege a matéria.

4.23.12.1. O emitente da garantia ofertada pelo Contratado deverá ser notificado pelo CONTRATANTE quanto ao início de processo administrativo para apuração de descumprimento de cláusulas contratuais.

4.23.12.2. Caso se trate da modalidade seguro-garantia, ocorrido o sinistro durante a vigência da apólice, sua caracterização e comunicação poderão ocorrer fora desta vigência, não caracterizando fato que justifique a negativa do sinistro, desde que respeitados os prazos prescricionais aplicados ao contrato de seguro, nos termos do art. 20 da Circular Susep n° 662, de 11 de abril de 2022.

4.23.13. Extinguir-se-á a garantia com a restituição da carta fiança, autorização para a liberação de importâncias depositadas em dinheiro a título de garantia ou anuência ao resgate do título de capitalização, acompanhada de declaração do CONTRATANTE, mediante termo circunstanciado, de que o Contratado cumpriu todas as cláusulas do contrato.

4.23.13.1. A extinção da garantia na modalidade seguro-garantia observará a regulamentação da Susep.

4.23.13.2. A Administração deverá apurar se há alguma pendência contratual antes do término da vigência da apólice.

4.23.14. A garantia somente será liberada ou restituída após a fiel execução do contrato ou após a sua extinção por culpa exclusiva da Administração e, quando em dinheiro, será atualizada monetariamente.

4.23.15. O Contratado autoriza o CONTRATANTE a reter, a qualquer tempo, a garantia, na forma prevista neste Termo de Referência.

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

4.23.17. A garantia de execução é independente de eventual garantia do produto ou serviço prevista neste Termo de Referência.

4.24. INFORMAÇÕES RELEVANTES PARA O DIMENSIONAMENTO E/OU APRESENTAÇÃO DA PROPOSTA

4.24.1. A demanda do órgão tem como base a solução e os quantitativos estabelecidos na tabela constante do subitem 1.1 deste Termo de Referência e seus anexos.

4.25. RESERVA DE COTAS PARA MICROEMPRESAS E EMPRESAS DE PEQUENO PORTE

4.25.1. Na presente licitação, não será aplicada a reserva de cota de até 25% para microempresas (ME) e empresas de pequeno porte (EPP), prevista no art. 48 da Lei Complementar nº 123/2006 e no Decreto nº 8.538/2015.

4.25.2. A não aplicação do tratamento diferenciado decorre das características do objeto, que consiste em solução corporativa de Application Delivery Controller (ADC) com funcionalidades integradas de Web Application Firewall (WAF), de elevada complexidade técnica, natureza integrada e caráter indivisível.

4.25.3. A eventual divisão do objeto em cotas comprometeria a padronização tecnológica, a interoperabilidade entre os componentes da solução, a gestão unificada da infraestrutura e a adequada execução contratual, podendo acarretar riscos à disponibilidade, segurança e desempenho dos serviços institucionais.

4.25.4. Dessa forma, a não adoção da reserva de cotas encontra amparo no art. 49 da Lei Complementar nº 123/2006, bem como no §1º do art. 4º da Lei nº 14.133/2021.

4.26. MARGEM DE PREFERÊNCIA

4.26.1. O objeto da contratação não se enquadra na aplicação de margem de preferência, seja normal ou adicional, prevista no Decreto nº 11.890/2024 e Resolução da Comissão Internacional de Contratações Públicas para o Desenvolvimento Sustentável - CICS-Resolução CICS/MDIC nº 1, de 16 de fevereiro de 2024.

5. PAPÉIS E RESPONSABILIDADES

5.1. São obrigações da CONTRATANTE:

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

5.1.2. encaminhar formalmente a demanda por meio de Ordem de Serviço ou de Fornecimento de Bens, de acordo com os critérios estabelecidos no Termo de Referência;

5.1.3. receber o objeto fornecido pelo contratado que esteja em conformidade com a proposta aceita, conforme inspeções realizadas;

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

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

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

5.1.7. definir produtividade ou capacidade mínima de fornecimento da solução de TIC por parte do contratado, com base em pesquisas de mercado, quando aplicável;

5.1.8. prever que os direitos de propriedade intelectual e direitos autorais da solução de TIC sobre os diversos artefatos e produtos cuja criação ou alteração seja objeto da relação contratual pertençam à Administração, incluindo a documentação, o código-fonte de aplicações, os modelos de dados e as bases de dados, justificando os casos em que isso não ocorrer.

5.2. São obrigações do CONTRATADO:

5.2.1. indicar formalmente preposto apto a representá-la junto à CONTRATANTE, que deverá responder pela fiel execução do contrato;

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

5.2.3. reparar quaisquer danos diretamente causados à CONTRATANTE ou a terceiros por culpa ou dolo de seus representantes legais, prepostos ou empregados, em decorrência da relação contratual, não excluindo ou reduzindo a responsabilidade da fiscalização ou o acompanhamento da execução do contrato pela Contratante;

5.2.5. propiciar todos os meios necessários à fiscalização do contrato pela CONTRATANTE, cujo representante terá poderes para sustar o fornecimento, total ou parcial, em qualquer tempo, desde que motivadas as causas e justificativas desta decisão;

5.2.6. manter, durante toda a execução do contrato, as mesmas condições da habilitação;

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

5.2.8. quando especificado, manter a produtividade ou a capacidade mínima de fornecimento da solução de TIC durante a execução do contrato;

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

5.2.10. fazer a transição contratual, com transferência de conhecimento, tecnologia e técnicas empregadas, sem perda de informações, podendo exigir, inclusive, a capacitação dos técnicos do CONTRATANTE ou da nova empresa que continuará a execução do contrato, quando for o caso.

6. MODELO DE EXECUÇÃO DO CONTRATO

6.1. ROTINAS DE EXECUÇÃO

6.1.1. Do Encaminhamento Formal de Demandas

6.1.1.1. O gestor do contrato emitirá a Ordem de Fornecimento de Bens (OFB) e/ou a Ordem de Serviço (OS), conforme o caso, para a execução dos bens e serviços contratados.

6.1.1.2. A CONTRATADA deverá fornecer os bens e executar os serviços conforme as especificações, configurações, quantitativos e condições definidos na respectiva OFB ou OS.

6.1.1.3. O recebimento provisório e definitivo dos bens e serviços é disciplinado em tópico próprio deste TR.

6.1.1.4. A execução do objeto compreenderá, no mínimo, as seguintes etapas:

6.1.1.4.1. fornecimento dos equipamentos, licenças, garantia e suporte técnico do fabricante e subscrições;

6.1.1.4.2. instalação física e lógica da solução no ambiente do CNPq;

6.1.1.4.3. configuração inicial, incluindo políticas de balanceamento, segurança e WAF;

6.1.1.4.4. integração com os ambientes existentes, incluindo serviços de rede, diretórios e aplicações institucionais;

6.1.1.4.5. realização de testes de funcionamento, desempenho e segurança;

6.1.1.4.6. apoio assistido à operação durante o período inicial de estabilização;

6.1.1.4.7. prestação de suporte técnico e consultoria especializada durante a vigência contratual.

6.2. FORMA DE EXECUÇÃO E ACOMPANHAMENTO DO CONTRATO

6.1.2. CONDIÇÕES DE ENTREGA

6.2.1. A execução do objeto compreenderá o fornecimento dos bens e a prestação dos serviços associados, conforme especificado neste Termo de Referência, observando-se as Ordens de Fornecimento de Bens (OFB) e Ordens de Serviço (OS) emitidas pela CONTRATANTE.

6.2.2. O prazo para fornecimento e entrega dos equipamentos, disponibilização das licenças de software, ativação da garantia e suporte técnico oficial do fabricante, das subscrições de segurança e dos demais recursos necessários à solução será de até 60 (sessenta) dias corridos, contados da emissão da respectiva Ordem de Fornecimento de Bens (OFB), Ordem de Serviço (OS) ou instrumento equivalente.

6.2.3. As atividades de instalação, configuração, implantação, migração, testes, validação e entrada em produção da solução deverão ser executadas em até 60 (sessenta) dias corridos, contados da conclusão da etapa prevista no item anterior.

6.2.4. Os prazos estabelecidos poderão ser prorrogados, uma única vez, por igual período, mediante justificativa formal da contratada e prévia aprovação da Administração.

6.2.5. Os serviços de suporte técnico especializado terão início após a conclusão da implantação da solução e emissão do Termo de Recebimento Definitivo, sendo prestados de forma contínua durante a vigência contratual.

6.2.6. Caso não seja possível cumprir os prazos estabelecidos, a CONTRATADA deverá comunicar formalmente à CONTRATANTE, com antecedência mínima de 5 (cinco) dias úteis, apresentando as devidas justificativas para análise e deliberação, ressalvadas as hipóteses de caso fortuito ou força maior.

6.2.7. Os bens deverão ser entregues no seguinte endereço: ***Setor de Autarquias Sul (SAUS), Quadra 01, Lote 06, Bloco H – Edifício Telemundi II, Asa Sul, Brasília/DF, CEP 70070-010.***

6.2.8. A entrega deverá contemplar todos os equipamentos, componentes, acessórios, cabos, licenças e demais itens necessários ao pleno funcionamento da solução, conforme especificações deste Termo de Referência.

6.2.9. O acompanhamento da execução contratual será realizado pela equipe de fiscalização designada pela CONTRATANTE, abrangendo tanto o fornecimento dos bens quanto a prestação dos serviços continuados, com base nas OFB e OS emitidas, nos prazos estabelecidos e nos critérios de aceitação definidos neste Termo de Referência.

6.2.10. O prazo de execução dos serviços e entrega dos bens observará, adicionalmente, o cronograma definido no subitem 4.5 (Requisitos Temporais), prevalecendo aquele que for mais restritivo em caso de divergência.

6.3. FORMAS DE TRANSFERÊNCIA DE CONHECIMENTO

6.3.1. A transferência do conhecimento deverá ser realizada observando-se o que segue:

6.3.1.1. A CONTRATADA deverá se comprometer a habilitar a equipe de técnicos da CONTRATANTE, ou outra por ela indicada, sem ônus para o CNPq, no uso da solução entregue/produtos fornecidos dentro do escopo do contrato. Isso com vistas a mitigar riscos de descontinuidade dos serviços e de dependência técnica.

6.4. PROCEDIMENTOS DE TRANSIÇÃO E FINALIZAÇÃO DO CONTRATO

6.4.1. Considerando as características do objeto, os procedimentos de transição e finalização do contrato deverão ser executados de forma planejada e coordenada, com o objetivo de assegurar a continuidade operacional da solução de balanceamento de carga e proteção de aplicações, sem prejuízo à disponibilidade, segurança ou desempenho do ambiente do CNPq.

6.4.2. Ao término da vigência contratual, ou em caso de rescisão antecipada, a CONTRATADA deverá colaborar com a CONTRATANTE na realização de transição técnica mínima, compreendendo, quando aplicável:

6.4.2.1. disponibilização de informações atualizadas acerca da situação operacional da solução, incluindo licenças de software, garantia e suporte técnico oficial do fabricante, subscrições de segurança e contratos de suporte técnico da CONTRATADA;

6.4.2.2. repasse de orientações técnicas necessárias à continuidade da operação do ambiente;

6.4.2.3. entrega ou atualização da documentação técnica relacionada aos itens contratados, incluindo, quando existente:

6.4.2.3.1. topologia lógica do ambiente;

6.4.2.3.2. versões de software, firmware e subscrições ativas;

6.4.2.3.3. registro das principais configurações implementadas;

6.4.2.3.4. histórico de chamados relevantes, incidentes críticos e intervenções realizadas durante a vigência contratual;

6.4.4. Os procedimentos de transição não implicarão cessão de profissionais, transferência de tecnologia proprietária, entrega de códigos-fonte ou obrigação de capacitação formal da equipe da CONTRATANTE ou de terceiros, salvo previsão expressa em instrumento contratual.

6.4.5. Todos os acessos lógicos concedidos à CONTRATADA deverão ser revogados ao término do contrato, mediante validação da CONTRATANTE.

6.5. QUANTIDADE MÍNIMA DE BENS OU SERVIÇOS PARA COMPARAÇÃO E CONTROLE

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

6.6. MECANISMOS FORMAIS DE COMUNICAÇÃO

6.6.1. São definidos como mecanismos formais de comunicação, entre a CONTRATANTE e a CONTRATADA, os seguintes:

6.6.1.1. Ordem de Fornecimento de Bens/Ordem de Serviço;

6.6.1.2. ata de Reunião;

6.6.1.3. ofício;

6.6.1.4. sistema de abertura de chamados;

6.6.1.5. e-mail e Cartas;

6.6.1.6. plataforma eletrônica de comunicação aderida pela CONTRATANTE (por exemplo: rocket.chat, Microsoft Teams etc.).

6.6.1.7. termos de Recebimento;

6.6.1.8. relatórios;

6.6.1.9. Demais Termos previstos no instrumento convocatório.

6.7. FORMAS DE PAGAMENTO

6.7.1. Os critérios de medição e pagamento serão tratados em tópico próprio do Modelo de Gestão do Contrato.

6.8. MANUTENÇÃO DE SIGILO E NORMAS DE SEGURANÇA

6.8.1. O Contratado deverá manter sigilo absoluto sobre quaisquer dados e informações contidos em quaisquer documentos e mídias, incluindo os equipamentos e seus meios de armazenamento, de que venha a ter conhecimento durante a execução do contrato, não podendo, sob qualquer pretexto, divulgar, reproduzir ou utilizar, sob pena de lei, independentemente da classificação de sigilo conferida pelo CONTRATANTE a tais documentos.

6.8.2. O Termo de Compromisso e Manutenção de Sigilo, contendo declaração de manutenção de sigilo e respeito às normas de segurança vigentes na entidade, a ser assinado pelo representante legal do Contratado, e Termo de Ciência, a ser assinado por todos os empregados do Contratado diretamente envolvidos na contratação, encontram-se nos Anexos III e IV deste Termo de Referência.

7. MODELO DE GESTÃO DO CONTRATO

7.1. O contrato deverá ser executado fielmente pelas partes, de acordo com as cláusulas avençadas e as normas da Lei nº 14.133, de 2021, e cada parte responderá pelas consequências de sua inexecução total ou parcial.

7.2. Em caso de impedimento, ordem de paralisação ou suspensão do contrato, o cronograma de execução será prorrogado automaticamente pelo tempo correspondente, anotadas tais circunstâncias mediante simples apostila.

7.3. As comunicações entre o órgão ou entidade e o Contratado devem ser realizadas por escrito sempre que o ato exigir tal formalidade, admitindo-se o uso de mensagem eletrônica para esse fim.

7.4. O órgão ou entidade poderá convocar o preposto da empresa para adoção de providências que devam ser cumpridas de imediato.

7.5. REUNIÃO INICIAL

7.5.1. Após a assinatura do Contrato e a nomeação do Gestor e Fiscais do Contrato, será realizada a Reunião Inicial de alinhamento com o objetivo de nivelar os entendimentos acerca das condições estabelecidas no Contrato, Edital e seus anexos, e esclarecer possíveis dúvidas acerca da execução do contrato.

7.5.2. A reunião será realizada em conformidade com o previsto no inciso I do Art. 31 da IN SGD/ME nº 94, de 2022, e ocorrerá em até 10 (dez) dias corridos da assinatura do Contrato, podendo ser prorrogada a critério da CONTRATANTE.

7.5.3. A pauta desta reunião observará, pelo menos:

7.5.3.1. Presença do representante legal da CONTRATADA, que apresentará o seu preposto;

7.5.3.2. entrega, por parte da CONTRATADA, do Termo de Compromisso e dos Termos de Ciência;

7.5.3.3. esclarecimentos relativos a questões operacionais, administrativas e de gestão do contrato;

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

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

7.6. FISCALIZAÇÃO

7.6.1. A execução do contrato deverá ser acompanhada e fiscalizada pelo(s) fiscal(is) do contrato, ou pelos respectivos substitutos, nos termos do art. 33 da IN SGD nº 94, de 2022, observando-se, em especial, as rotinas a seguir.

7.7. FISCALIZAÇÃO TÉCNICA

7.7.1. O fiscal técnico do contrato, além de exercer as atribuições previstas no art. 33, II, da IN SGD nº 94, de 2022, acompanhará a execução do contrato, para que sejam cumpridas todas as condições estabelecidas no contrato, de modo a assegurar os melhores resultados para a Administração.

7.7.2. O fiscal técnico do contrato anotará no histórico de gerenciamento do contrato todas as ocorrências relacionadas à execução do contrato, com a descrição do que for necessário para a regularização das faltas ou dos defeitos observados.

7.7.3. Identificada qualquer inexatidão ou irregularidade, o fiscal técnico do contrato emitirá notificações para a correção da execução do contrato, determinando prazo para a correção.

7.7.4. O fiscal técnico do contrato informará ao gestor do contato, em tempo hábil, a situação que demandar decisão ou adoção de medidas que ultrapassem sua competência, para que adote as medidas necessárias e saneadoras, se for o caso.

7.7.5. No caso de ocorrências que possam inviabilizar a execução do contrato nas datas aprazadas, o fiscal técnico do contrato comunicará o fato imediatamente ao gestor do contrato.

7.7.6. O fiscal técnico do contrato comunicará ao gestor do contrato, em tempo hábil, o término do contrato sob sua responsabilidade, com vistas à renovação tempestiva ou à prorrogação contratual.

7.8. FISCALIZAÇÃO ADMINISTRATIVA

7.8.1. O fiscal administrativo do contrato, além de exercer as atribuições previstas no art. 33, IV, da IN SGD nº 94, de 2022, verificará a manutenção das condições de habilitação da CONTRATADA, acompanhará o empenho, o pagamento, as garantias, as glosas e a formalização de apostilamento e termos aditivos, solicitando quaisquer documentos comprobatórios pertinentes, caso necessário.

7.8.2. Caso ocorra descumprimento das obrigações contratuais, o fiscal administrativo do contrato atuará tempestivamente na solução do problema, reportando ao gestor do contrato para que tome as providências cabíveis, quando ultrapassar a sua competência.

7.8.3. A fiscalização de que trata esta cláusula não exclui nem reduz a responsabilidade do Contratado, inclusive perante terceiros, por qualquer irregularidade, ainda que resultante de imperfeições técnicas, vícios redibitórios, ou emprego de material inadequado ou de qualidade inferior e, na ocorrência desta, não implica corresponsabilidade da CONTRATANTE ou de seus agentes, gestores e fiscais, de conformidade.

7.9. GESTOR DO CONTRATO

7.9.1. Cabe ao gestor do contrato, além de exercer as atribuições previstas no art. 33, I, da IN SGD nº 94, de 2022:

7.9.1.1. coordenar a atualização do processo de acompanhamento e fiscalização do contrato contendo todos os registros formais da execução no histórico de gerenciamento do contrato, a exemplo da ordem de serviço, do registro de ocorrências, das alterações e das prorrogações contratuais, elaborando relatório com vistas à verificação da necessidade de adequações do contrato para fins de atendimento da finalidade da administração.

7.9.1.2. acompanhar os registros realizados pelos fiscais do contrato, de todas as ocorrências relacionadas à execução do contrato e as medidas adotadas, informando, se for o caso, à autoridade superior àquelas que ultrapassarem a sua competência.

7.9.1.3. acompanhar a manutenção das condições de habilitação da CONTRATADA, para fins de empenho de despesa e pagamento, e anotará os problemas que obstem o fluxo normal da liquidação e do pagamento da despesa no relatório de riscos eventuais.

7.9.1.4. emitir documento comprobatório da avaliação realizada pelos fiscais técnico, administrativo e setorial quanto ao cumprimento de obrigações assumidas pelo Contratado, com menção ao seu desempenho na execução contratual, baseado nos indicadores objetivamente definidos e aferidos, e a eventuais penalidades aplicadas, devendo constar do cadastro de atesto de cumprimento de obrigações

7.9.1.5. tomar providências para a formalização de processo administrativo de responsabilização para fins de aplicação de sanções, a ser conduzido pela comissão de que trata o art. 158 da Lei nº 14.133, de 2021, ou pelo agente ou pelo setor com competência para tal, conforme o caso.

7.9.1.6. elaborar relatório final com informações sobre a consecução dos objetivos que tenham justificado a contratação e eventuais condutas a serem adotadas para o aprimoramento das atividades da Administração.

7.9.1.7. enviar a documentação pertinente ao setor de contratos para a formalização dos procedimentos de liquidação e pagamento, no valor dimensionado pela fiscalização e gestão nos termos do contrato.

7.9.2. O fiscal técnico do contrato comunicará ao gestor do contrato, em tempo hábil, o término do contrato sob sua responsabilidade, com vistas à tempestiva renovação ou prorrogação contratual.

7.10. CRITÉRIOS DE ACEITAÇÃO

7.10.1. A avaliação da qualidade dos produtos entregues, para fins de aceitação, consiste na verificação dos critérios relacionados a seguir:

7.10.2. Todos os equipamentos fornecidos deverão ser novos (incluindo todas as peças e componentes presentes nos produtos), de primeiro uso (sem sinais de utilização anterior), não recondicionados e em fase de comercialização normal através dos canais de venda do fabricante no Brasil (não serão aceitos produtos end-of-life).

7.10.3. Todos os componentes do(s) equipamento(s) e respectivas funcionalidades deverão ser compatíveis entre si, sem a utilização de adaptadores, frisagens, pinturas, usinagens em geral, furações, emprego de adesivos, fitas adesivas ou quaisquer outros procedimentos não previstos nas especificações técnicas ou, ainda, com emprego de materiais inadequados ou que visem adaptar forçadamente o produto ou suas partes que sejam fisicamente ou logicamente incompatíveis.

7.10.4. Todos os componentes internos do(s) equipamento(s) deverá(ão) estar instalado(s) de forma organizada e livres de pressões ocasionados por outros componentes ou cabos, que possam causar desconexões, instabilidade, ou funcionamento inadequado.

7.10.5. O número de série de cada equipamento deve ser obrigatório e único, afixado em local visível, na parte externa do gabinete e na embalagem que o contém. Esse número deverá ser identificado pelo fabricante, como válido para o produto entregue e para as condições do mercado brasileiro no que se refere à garantia e assistência técnica no Brasil.

7.10.6. Serão recusados os produtos que possuam componentes ou acessórios com sinais claros de oxidação, danos físicos, sujeira, riscos ou outro sinal de desgaste, mesmo sendo o componente ou acessório considerado como novos pelo fornecedor dos produtos.

7.10.7. Os produtos, considerando a marca e modelo apresentados na licitação, não poderão estar fora de linha comercial, considerando a data de LICITAÇÃO (abertura das propostas). Os produtos devem ser fornecidos completos e prontos para a utilização, com todos os acessórios, componentes, cabos etc.

7.10.8. Todas as licenças, referentes aos softwares e drivers solicitados, devem estar registrados para utilização do CONTRATANTE, em modo definitivo (licenças perpétuas), legalizado, não sendo admitidas versões “shareware” ou “trial”. O modelo do produto ofertado pelo licitante deverá estar em fase de produção pelo fabricante (no Brasil ou no exterior), sem previsão de encerramento de produção, até a data de entrega da proposta.

7.10.9. A CONTRATANTE poderá optar por avaliar a qualidade de todos os equipamentos fornecidos ou uma amostra dos equipamentos, atentando para a inclusão nos autos do processo administrativo de todos os documentos que evidenciem a realização dos testes de aceitação em cada equipamento selecionado, para posterior rastreabilidade.

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

7.11. PROCEDIMENTOS DE TESTE E INSPEÇÃO

7.11. Serão adotados como procedimentos de teste e inspeção, para fins de elaboração dos Termos de Recebimento Provisório e Definitivo:

7.11.1. Teste de funcionamento geral da solução, incluindo verificação de alta disponibilidade (HA);

7.11.2. Teste de balanceamento de carga entre servidores;

7.11.3. Teste de aplicação de políticas de segurança e WAF;

7.11.4. Teste de desempenho (throughput, conexões simultâneas e latência);

7.11.5. Teste de integração com sistemas e aplicações do ambiente do CNPq;

7.11.6. Teste de failover e continuidade operacional.

7.11.7. Verificação da ativação das licenças, das subscrições de segurança, da garantia e do suporte técnico oficial do fabricante, incluindo a validação do respectivo registro junto ao fabricante, quando aplicável.

7.12. NÍVEIS MÍNIMOS DE SERVIÇO EXIGIDOS

7.12.1. Os níveis mínimos de serviço são indicadores mensuráveis estabelecidos pelo CONTRATANTE para aferir objetivamente os resultados pretendidos com a contratação. São considerados para a presente contratação os seguintes indicadores:

Tabela 07 – Níveis Mínimos de Serviço Exigidos

IAE – INDICADOR DE ATRASO NA ENTREGA	
Finalidade	Medir o tempo de atraso na entrega dos bens e na execução dos serviços previstos nas respectivas Ordens de Fornecimento de Bens (OFB) e Ordens de Serviço (OS).
Meta a cumprir	IAE < = 0 *(A meta definida visa garantir a entrega dos produtos e serviços constantes nas OFB/OS dentro do prazo previsto).*
Instrumento de medição	OFB/OS, Termo de Recebimento Provisório (TRP)
Forma de acompanhamento	A avaliação será feita conforme linha de base do cronograma registrada na OFB/OS. Será subtraída a data de entrega dos produtos da OFB/OS (desde que o fiscal técnico reconheça aquela data, com registro em Termo de Recebimento Provisório) pela data de início da execução da OFB/OS.
Periodicidade	Para cada OFB/OS encerrada e com Termo de Recebimento Definitivo.
	IAE = TEX – TEST Onde:

Mecanismo de Cálculo (métrica)	**IAE** – Indicador de Atraso de Entrega da OFB/OS; **TEX** – Tempo de Execução – corresponde ao período de execução da OFB/OS, da sua data de início até a data de entrega dos produtos da OFB/OS. A data de início será aquela constante na OFB/OS; caso não esteja explícita, será o primeiro dia útil após a emissão da OFB/OS. A data de entrega da OFB/OS deverá ser aquela reconhecida pelo fiscal técnico, conforme critérios constantes neste Termo de Referência. Para os casos em que o fiscal técnico rejeita a entrega, o prazo de execução da OFB/OS continua a correr, findando-se apenas quanto o Contratado entrega os produtos da OFB/OS e haja aceitação por parte do fiscal técnico. **TEST** – Tempo Estimado para a execução da OFB/OS – constante na OFB/OS, conforme estipulado no Termo de Referência
Observações	Obs1: Serão utilizados dias corridos na medição. Obs2: Os dias com expediente parcial no órgão/entidade serão considerados como dias corridos no cômputo do indicador. Obs3: Atrasos decorrentes de caso fortuito ou força maior, devidamente justificados e aceitos pela Contratante, não serão considerados.
Início de Vigência	A partir da emissão da OFB/OS.
Faixas de ajuste no pagamento e Sanções	Para valores do indicador **IAE**: IAE ≤ 0 = pagamento integral IAE de 1 a 60 dias = glosa de 0,1666% por dia de atraso IAE > 60 dias = glosa de 10% + multa de 2%

Tabela 08 – Níveis Mínimos de Serviço Exigidos

ISA – INDICADOR DE ATENDIMENTO DE SUPORTE	
Finalidade	Medir a eficiência e tempestividade do suporte técnico prestado pela Contratada.
Meta a cumprir	Cumprimento de, no mínimo, 95% dos chamados dentro dos prazos de SLA estabelecidos.
Instrumento de medição	Sistema de chamados ou ferramenta de gestão de serviços adotada pela Contratante.
Forma de acompanhamento	Relatórios mensais de atendimento.
Periodicidade	Mensal.
Mecanismo de Cálculo (métrica)	ISA = (Número de chamados atendidos dentro do prazo / Total de chamados) x 100

Observações	Obs1: Serão considerados, para fins de apuração do indicador, todos os chamados registrados no período de medição, classificados conforme níveis de severidade definidos neste Termo de Referência. Obs2: Chamados cujo atraso seja decorrente exclusivamente de ação ou omissão da Contratante, devidamente comprovada, poderão ser desconsiderados no cálculo do indicador. Obs3: O tempo de atendimento será contabilizado a partir da abertura do chamado até a sua efetiva resolução ou mitigação, conforme critérios definidos nos níveis de serviço (SLA). Obs4: Chamados reabertos por solução inadequada ou incompleta serão contabilizados como não atendidos dentro do prazo.
Início de Vigência	A partir do início da prestação dos serviços de suporte técnico, após a emissão da Ordem de Serviço (OS).
Faixas de ajuste no pagamento e Sanções	ISA ≥ 95% = sem desconto ISA entre 90% e 94,99% = desconto de 5% na fatura mensal ISA entre 80% e 89,99% = desconto de 10% ISA < 80% = desconto de 15%

8. INFRAÇÕES E SANÇÕES ADMINISTRATIVAS E PROCEDIMENTOS PARA RETENÇÃO OU GLOSA NOS PAGAMENTOS

8.1. Nos casos de inadimplemento na execução do objeto, as ocorrências serão registradas pela CONTRATANTE, conforme a tabela abaixo:

Tabela 09 – Infrações e Sanções Administrativas e Procedimentos para Retenção ou Glosa nos Pagamentos

ID	OCORRÊNCIA	GLOSA/SANÇÃO
1	Dar causa à inexecução parcial do contrato.	Advertência. Em caso de reincidência, aplicar-se -á multa 2% (dois por cento) sobre o valor total do Contrato.
2	Dar causa à inexecução parcial do contrato que cause grave dano à Administração, ao funcionamento dos serviços públicos ou ao interesse coletivo.	A CONTRATADA será impedida de licitar ou no âmbito da Administração Pública direta e indireta do ente federativo que tiver aplicado a sanção, pelo prazo máximo de 3 (três) anos, sem prejuízo das demais penalidades previstas na Lei n° 14.133, de 2021.
3	Dar causa à inexecução total do contrato.	A CONTRATADA será impedida de licitar ou no âmbito da Administração Pública direta e indireta do ente federativo que tiver aplicado a sanção, pelo prazo máximo de 3 (três) anos, sem prejuízo das demais penalidades previstas na Lei n° 14.133, de 2021.
4	Deixar de entregar a documentação exigida para o certame.	A CONTRATADA será impedida de licitar ou no âmbito da Administração Pública direta e indireta do ente federativo que tiver aplicado a sanção, pelo prazo máximo de 3 (três) anos, sem prejuízo das demais penalidades previstas na Lei n° 14.133, de 2021.
		A CONTRATADA será impedida de licitar ou no âmbito da Administração Pública direta e indireta do ente federativo

5	Não manter a proposta, salvo em decorrência de fato superveniente devidamente justificado.	que tiver aplicado a sanção, pelo prazo máximo de 3 (três) anos, sem prejuízo das demais penalidades previstas na Lei n° 14.133, de 2021.
6	Não celebrar o contrato ou não entregar a documentação exigida para a contratação, quando convocado dentro do prazo de validade de sua proposta.	A CONTRATADA será impedida de licitar ou no âmbito da Administração Pública direta e indireta do ente federativo que tiver aplicado a sanção, pelo prazo máximo de 3 (três) anos, sem prejuízo das demais penalidades previstas na Lei n° 14.133, de 2021.
7	Ensejar o retardamento da entrega dos bens, da disponibilização das licenças, garantias, subscrições ou da execução dos serviços contratados, sem motivo justificado.	A CONTRATADA será impedida de licitar ou no âmbito da Administração Pública direta e indireta do ente federativo que tiver aplicado a sanção, pelo prazo máximo de 3 (três) anos, sem prejuízo das demais penalidades previstas na Lei n° 14.133, de 2021.
8	Apresentar declaração ou documentação falsa exigida para o certame ou prestar declaração falsa durante a licitação a execução do contrato.	A CONTRATADA será declarada inidônea para licitar ou contratar com a Administração Pública, pelo prazo mínimo de 3 (três) anos e no máximo de 6 (seis) anos, sem prejuízo das demais penalidades previstas na Lei n° 14.133, de 2021. Após o limite de 7 dias úteis, aplicar-se-á multa de 10% do valor total do contrato.
9	Fraudar a licitação ou praticar ato fraudulento na execução do contrato	A CONTRATADA será declarada inidônea para licitar ou contratar com a Administração Pública, pelo prazo mínimo de 3 (três) anos e no máximo de 6 (seis) anos, sem prejuízo das demais penalidades previstas na Lei n° 14.133, de 2021.
10	Comportar-se de modo inidôneo ou cometer fraude de qualquer natureza	A CONTRATADA será declarada inidônea para licitar ou contratar com a Administração Pública, pelo prazo mínimo de 3 (três) anos e no máximo de 6 (seis) anos, sem prejuízo das demais penalidades previstas na Lei n° 14.133, de 2021.
11	Praticar atos ilícitos com vistas a frustrar os objetivos da licitação.	A CONTRATADA será declarada inidônea para licitar ou contratar com a Administração Pública, pelo prazo mínimo de 3 (três) anos e no máximo de 6 (seis) anos, sem prejuízo das demais penalidades previstas na Lei n° 14.133, de 2021.
12	Não prestar esclarecimentos imediatamente sobre a execução dos serviços, ou não respondê-los na prazo máximo de 48 (quarenta e oito) horas úteis quando de caráter técnico.	Multa de 0,5% (meio por cento) sobre o valor total do contrato por dia útil de atraso, até o limite de 5 (cinco) dias úteis. Após esse limite aplica-se multa de 5% (cinco por cento) do valor total do contrato.
13	Ocorrência de violação de segurança comprovadamente originada por falha da solução, por erro de configuração, implantação, atualização ou manutenção sob responsabilidade da CONTRATADA.	Multa única de 10% (dez por cento) do valor total do contrato, além do custeio integral de todas as medidas corretivas e eventuais multas de órgão de controle decorrentes do incidente
14	Deixar de manter vigentes, durante a execução contratual, as licenças, garantias, subscrições ou o suporte técnico oficial do fabricante previstos neste Termo de Referência.	Multa de 5% (cinco por cento) sobre o valor total do contrato, sem prejuízo da obrigação de regularização imediata e da aplicação das demais sanções previstas na Lei nº 14.133/2021.

15	Não cumprir qualquer outra obrigação contratual não citada nesta tabela.	Advertência. Em caso de reincidência ou configurado prejuízo aos resultados pretendidos com a contratação, aplica-se multa de 3% (três por cento) do valor total do contrato.

8.2. Nos termos do art. 19, inciso III da Instrução Normativa SGD/ME nº 94, de 2022, será efetuada a retenção ou glosa no pagamento, proporcional à irregularidade verificada, sem prejuízo das sanções cabíveis, nos casos em que o contratado:

8.2.1. não atingir os valores mínimos aceitáveis fixados nos critérios de aceitação, não produzir os resultados ou deixar de executar as atividades contratadas; ou

8.2.2. deixar de utilizar materiais e recursos humanos exigidos para fornecimento da solução de TIC, ou utilizá-los com qualidade ou quantidade inferior à demandada;

8.3. Comete infração administrativa, nos termos da Lei nº 14.133, de 2021, o Contratado 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 nº 12.846, de 1º de agosto de 2013.

8.4. Serão aplicadas ao CONTRATADO que incorrer nas infrações acima descritas as seguintes sanções:

8.4.1. Advertência, quando o Contratado der causa à inexecução parcial do contrato, sempre que não se justificar a imposição de penalidade mais grave;

8.4.2. Impedimento de licitar e contratar, quando praticadas as condutas descritas nas alíneas “b”, “c” e “d” do subitem acima, sempre que não se justificar a imposição de penalidade mais grave;

8.4.3. Declaração de inidoneidade para licitar e contratar, quando praticadas as condutas descritas nas alíneas “e”, “f”, “g” e “h” do subitem acima, bem como nas alíneas “b”, “c” e “d”, que justifiquem a imposição de penalidade mais grave.

8.4.4. Multa:

8.4.4.1. Moratória, para as infrações descritas no item “d”, de 0,1% (zero virgula um por cento) por dia de atraso injustificado sobre o valor da parcela inadimplida, até o limite de 30 (trinta) dias.

8.4.4.2. Moratória de 0,07% (sete centésimos por cento) por dia de atraso injustificado sobre o valor total do contrato, até o máximo de 2% (dois por cento), pela inobservância do prazo fixado para apresentação, suplementação ou reposição da garantia;

8.4.4.2.1. O atraso superior a 25 (vinte e cinco) dias para apresentação, suplementação ou reposição da garantia autoriza a Administração a promover a extinção do contrato por descumprimento ou cumprimento irregular de suas cláusulas, conforme dispõe o inciso I do art. 137 da Lei n. 14.133, de 2021.

8.4.4.3. Compensatória, para as infrações descritas acima alíneas “e” a “h” de 10% (dez por cento) a 30% (trinta por cento) do valor da contratação.

8.4.4.4. Compensatória, para a inexecução total do contrato prevista acima na alínea “c”, de 10% (dez por cento) a 30% (trinta por cento) do valor da contratação.

8.4.4.5. Compensatória, para a infração descrita acima na alínea “b”, de 5% (cinco por cento) até 15% (quinze por cento) do valor da contratação.

8.4.4.6. Compensatória, em substituição à multa moratória para a infração descrita acima na alínea “d”, de 2% (dois por cento) a 10% (dez por cento) do valor da contratação.

8.4.4.7. Compensatória, para a infração descrita acima na alínea “a”, de 0,5% (cinco décimos por cento) a 5% (cinco por cento) do valor da contratação.

8.5. A aplicação das sanções previstas neste Termo de Referência não exclui, em hipótese alguma, a obrigação de reparação integral do dano causado ao CONTRATANTE.

8.6. Todas as sanções previstas neste Termo de Referência poderão ser aplicadas cumulativamente com a multa.

8.7. Antes da aplicação da multa será facultada a defesa do interessado no prazo de 15 (quinze) dias úteis, contado da data de sua intimação.

8.8. Se a multa aplicada e as indenizações cabíveis forem superiores ao valor do pagamento eventualmente devido pelo CONTRATANTE ao Contratado, além da perda desse valor, a diferença será descontada da garantia prestada ou será cobrada judicialmente.

8.9. A multa poderá ser recolhida administrativamente no prazo máximo de 10 (dez) dias, a contar da data do recebimento da comunicação enviada pela autoridade competente.

8.10. 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 nº 14.133, de 2021, para as penalidades de impedimento de licitar e contratar e de declaração de inidoneidade para licitar ou contratar.

8.10.1. Para a garantia da ampla defesa e contraditório, as notificações serão enviadas eletronicamente para os endereços de e-mail informados na proposta comercial, bem como os cadastrados pela empresa no SICAF.

8.10.2. Os endereços de e-mail informados na proposta comercial e/ou cadastrados no SICAF serão considerados de uso contínuo da empresa, não cabendo alegação de desconhecimento das comunicações a eles comprovadamente enviadas.

8.11. Na aplicação das sanções serão considerados:

8.11.1. a natureza e a gravidade da infração cometida;

8.11.2. as peculiaridades do caso concreto;

8.11.3. as circunstâncias agravantes ou atenuantes;

8.11.4. os danos que dela provierem para o CONTRATANTE; e

8.11.5. a implantação ou o aperfeiçoamento de programa de integridade, conforme normas e orientações dos órgãos de controle.

8.12. Os atos previstos como infrações administrativas na Lei nº 14.133, de 2021, ou em outras leis de licitações e contratos da Administração Pública que também sejam tipificados como atos lesivos na Lei nº 12.846, de 2013, serão apurados e julgados conjuntamente, nos mesmos autos, observados o rito procedimental e autoridade competente definidos na referida Lei.

8.13. 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 Termo de Referência 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.

8.14. O CONTRATANTE deverá, no prazo máximo de 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.

8.14.1. As penalidades serão obrigatoriamente registradas no SICAF.

8.15. As sanções de impedimento de licitar e contratar e declaração de inidoneidade para licitar ou contratar são passíveis de reabilitação na forma do art. 163 da Lei nº 14.133, de 2021.

8.16. Os débitos do Contratado para com a Administração Contratante, resultantes de multa administrativa e/ou indenizações, não inscritos em dívida ativa, poderão ser compensados, total ou parcialmente, com os créditos devidos pelo referido órgão decorrentes deste mesmo contrato ou de outros contratos administrativos que o Contratado possua com o mesmo órgão ora Contratante, na forma da Instrução Normativa SEGES/ME nº 26, de 13 de abril de 2022.

9. CRITÉRIOS DE MEDIÇÃO E DE PAGAMENTO

9.1. RECEBIMENTO DO OBJETO

9.1.1. Os bens serão recebidos provisoriamente, de forma sumária, no ato da entrega, juntamente com a nota fiscal ou instrumento de cobrança equivalente, pelo(a) responsável pelo acompanhamento e fiscalização do contrato, para efeito de posterior verificação de sua conformidade com as especificações constantes no Termo de Referência e na proposta.

9.1.2. Os bens poderão ser rejeitados, no todo ou em parte, inclusive antes do recebimento provisório, quando em desacordo com as especificações constantes no Termo de Referência e na proposta, devendo ser substituídos no prazo de 10 (dez) dias, a contar da notificação da CONTRATADA, às suas custas, sem prejuízo da aplicação das penalidades.

9.1.3. O recebimento definitivo ocorrerá no prazo de 15 (quinze) dias úteis, a contar do recebimento da nota fiscal ou instrumento de cobrança equivalente pela Administração, após a verificação da qualidade e quantidade do material e consequente aceitação mediante termo detalhado.

9.1.4. Para as contratações decorrentes de despesas cujos valores não ultrapassem o limite de que trata o inciso II do art. 75 da Lei nº 14.133, de 2021, o prazo máximo para o recebimento definitivo será de até 5 (cinco) dias úteis.

9.1.5. O prazo para recebimento definitivo poderá ser excepcionalmente prorrogado, de forma justificada, por igual período, quando houver necessidade de diligências para a aferição do atendimento das exigências contratuais.

9.1.6. No caso de controvérsia sobre a execução do objeto, quanto à dimensão, qualidade e quantidade, deverá ser observado o teor do art. 143 da Lei nº 14.133, de 2021, comunicando-se à empresa para emissão de Nota Fiscal quanto à parcela incontroversa da execução do objeto, para efeito de liquidação e pagamento.

9.1.7. O prazo para a solução, pelo Contratado, de inconsistências na execução do objeto ou de saneamento da nota fiscal ou de instrumento de cobrança equivalente, verificadas pela Administração durante a análise prévia à liquidação de despesa, não será computado para os fins do recebimento definitivo.

9.1.8. O recebimento provisório ou definitivo não excluirá a responsabilidade civil pela solidez e pela segurança dos bens nem a responsabilidade ético-profissional pela perfeita execução do contrato.

9.1.9. As atividades de montagem, instalação e quaisquer outras necessárias para o funcionamento ou uso do bem correrão por conta do Contratado e são condição para o recebimento do objeto.

9.2. LIQUIDAÇÃO

9.2.1. Recebida a Nota Fiscal ou documento de cobrança equivalente, correrá o prazo de dez dias úteis para fins de liquidação, na forma desta seção, prorrogáveis por igual período, nos termos do art. 7º, §3º da Instrução Normativa SEGES/ME nº 77/2022.

9.2.2. O prazo de que trata o item anterior será reduzido à metade, mantendo-se a possibilidade de prorrogação, no caso de contratações decorrentes de despesas cujos valores não ultrapassem o limite de que trata o inciso II do art. 75 da Lei nº 14.133, de 2021.

9.2.3. Para fins de liquidação, o setor competente deverá verificar se a nota fiscal ou instrumento de cobrança equivalente apresentado expressa os elementos necessários e essenciais do documento, tais como:

9.2.3.1. o prazo de validade;

9.2.3.2. a data da emissão;

9.2.3.3. os dados do contrato e do órgão contratante;

9.2.3.4. o período respectivo de execução do contrato;

9.2.3.5. o valor a pagar; e

9.2.3.6. eventual destaque do valor de retenções tributárias cabíveis.

9.2.4. Havendo erro na apresentação da nota fiscal ou instrumento de cobrança equivalente, ou circunstância que impeça a liquidação da despesa, esta ficará sobrestada até que o Contratado providencie as medidas saneadoras, reiniciando-se o prazo após a comprovação da regularização da situação, sem ônus ao CONTRATANTE;

9.2.5. A nota fiscal ou instrumento de cobrança equivalente deverá ser obrigatoriamente acompanhado da comprovação da regularidade fiscal, constatada por meio de consulta on-line ao SICAF ou, na impossibilidade de acesso ao referido Sistema, mediante consulta aos sítios eletrônicos oficiais ou à documentação mencionada no art. 68 da Lei nº 14.133, de 2021.

9.2.6. A Administração deverá realizar consulta ao SICAF para:

9.2.6.1. verificar a manutenção das condições de habilitação exigidas;

9.2.6.2. identificar possível razão que impeça a participação em licitação/contratação no âmbito do órgão ou entidade, tais como a proibição de contratar com a Administração ou com o Poder Público, bem como ocorrências impeditivas indiretas.

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

9.2.8. Não havendo regularização ou sendo a defesa considerada improcedente, o CONTRATANTE deverá comunicar aos órgãos responsáveis pela fiscalização da regularidade fiscal quanto à inadimplência do Contratado, 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.

9.2.9. Persistindo a irregularidade, o CONTRATANTE deverá adotar as medidas necessárias à rescisão contratual nos autos do processo administrativo correspondente, assegurada ao Contratado a ampla defesa.

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

9.3. PRAZO DE PAGAMENTO

9.3.1. O pagamento será efetuado no prazo de até 10 (dez) dias úteis contados da finalização da liquidação da despesa, conforme seção anterior, nos termos da Instrução Normativa SEGES/ME nº 77, de 2022.

9.3.2. No caso de atraso pelo CONTRATANTE, os valores devidos ao Contratado serão atualizados monetariamente entre o termo final do prazo de pagamento até a data de sua efetiva realização, mediante aplicação do índice IPCA (Índice Nacional de Preços ao Consumidor Amplo) de correção monetária.

9.4. FORMA DE PAGAMENTO

9.4.1. O pagamento será realizado por meio de ordem bancária, para crédito em banco, agência e conta corrente indicados pelo Contratado.

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

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

9.4.4. Independentemente do percentual de tributo inserido na planilha, quando houver, serão retidos na fonte, quando da realização do pagamento, os percentuais estabelecidos na legislação vigente.

9.4.5. O Contratado regularmente optante pelo Simples Nacional, nos termos da Lei Complementar nº 123, de 2006, não sofrerá a retenção tributária quanto aos impostos e contribuições abrangidos por aquele regime. No entanto, o pagamento ficará condicionado à apresentação de comprovação, por meio de documento oficial, de que faz jus ao tratamento tributário favorecido previsto na referida Lei Complementar.

9.5. ANTECIPAÇÃO DE PAGAMENTO

9.5.1. Não será admitida a antecipação de pagamento.

9.6. CESSÃO DE CRÉDITO

9.6.1. As cessões de crédito dependerão de prévia aprovação do CONTRATANTE.

9.6.1.1. A eficácia da cessão de crédito, em relação à Administração, está condicionada à celebração de termo aditivo ao contrato administrativo.

9.6.1.2. Sem prejuízo do regular atendimento da obrigação contratual de cumprimento de todas as condições de habilitação por parte do Contratado (cedente), a celebração do aditamento de cessão de crédito e a realização dos pagamentos respectivos também se condicionam à regularidade fiscal e trabalhista do cessionário, bem como à certificação de que o cessionário não se encontra impedido de licitar e contratar com o Poder Público, conforme a legislação em vigor, ou de receber benefícios ou incentivos fiscais ou creditícios, direta ou indiretamente, conforme o art. 12 da Lei nº 8.429, de 1992, nos termos do Parecer JL-01, de 18 de maio de 2020.

9.6.1.3. O crédito a ser pago à cessionária é exatamente aquele que seria destinado à cedente (Contratado) pela execução do objeto contratual, restando absolutamente incólumes todas as defesas e exceções ao pagamento e todas as demais cláusulas exorbitantes ao direito comum aplicáveis no regime jurídico de direito público incidente sobre os contratos administrativos, incluindo a possibilidade de pagamento em conta vinculada ou de pagamento pela efetiva comprovação do fato gerador, quando for o caso, e o desconto de multas, glosas e prejuízos causados à Administração.

9.6.1.4. A cessão de crédito não afetará a execução do objeto contratado, que continuará sob a integral responsabilidade do Contratado.

9.6.2. O disposto nesta seção não afeta as operações de crédito de que trata a Instrução Normativa SEGES/MGI nº 82, de 21 de fevereiro de 2025, as quais ficam por esta regidas.

9.7. REAJUSTE

9.7.1. Os preços inicialmente contratados são fixos e irreajustáveis no prazo de um ano contado da data do orçamento estimado, em 19/08/2026**.**

9.7.2. Após o interregno de um ano, e independentemente de pedido do contratado, os preços iniciais serão reajustados, mediante a aplicação, pelo CONTRATANTE, do Índice de Custos de Tecnologia da Informação - ICTI, mantido pela Fundação Instituto de Pesquisa Econômica Aplicada - IPEA*,* exclusivamente para as obrigações iniciadas e concluídas após a ocorrência da anualidade

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

9.7.4. No caso de atraso ou não divulgação do(s) índice (s) de reajustamento, o CONTRATANTE pagará ao Contratado a importância calculada pela última variação conhecida, liquidando a diferença correspondente tão logo seja(m) divulgado(s) o(s) índice(s) definitivo(s).

9.7.5. Nas aferições finais, o(s) índice(s) utilizado(s) para reajuste será(ão), obrigatoriamente, o(s) definitivo(s).

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

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

9.7.8. O reajuste será realizado por apostilamento.

10. FORMA E CRITÉRIOS DE SELEÇÃO DO FORNECEDOR E FORMA DE FORNECIMENTO

10.1. FORMA DE SELEÇÃO E CRITÉRIO DE JULGAMENTO DA PROPOSTA

10.1.1. O fornecedor será selecionado por meio da realização de procedimento de LICITAÇÃO, na modalidade *PREGÃO* sob a forma ELETRÔNICA, com adoção do critério de julgamento pelo *MENOR PREÇO*.

10.2. FORMA DE FORNECIMENTO

10.2.1. O fornecimento do objeto será integral de acordo com a demanda solicitada pelo CONTRATANTE.

10.3. EXIGÊNCIAS DE HABILITAÇÃO

10.3.1. Para fins de habilitação, deverá o interessado comprovar os seguintes requisitos:

10.4. HABILITAÇÃO JURÍDICA

10.4.1. Pessoa física: cédula de identidade (RG) ou documento equivalente que, por força de lei, tenha validade para fins de identificação em todo o território nacional;

10.4.2. Empresário individual: inscrição no Registro Público de Empresas Mercantis, a cargo da Junta Comercial da respectiva sede;

10.4.3. Microempreendedor Individual - MEI: Certificado da Condição de Microempreendedor Individual - CCMEI, cuja aceitação ficará condicionada à verificação da autenticidade no sítio https://www.gov.br/empresas-e-negocios/pt-br/empreendedor;

10.4.4. Sociedade empresária, sociedade limitada unipessoal – SLU ou sociedade identificada como empresa individual de responsabilidade limitada - EIRELI: inscrição do ato constitutivo, estatuto ou contrato social no Registro Público de Empresas Mercantis, a cargo da Junta Comercial da respectiva sede, acompanhada de documento comprobatório de seus administradores;

10.4.5. Sociedade empresária estrangeira: portaria de autorização de funcionamento no Brasil, publicada no Diário Oficial da União e arquivada na Junta Comercial da unidade federativa onde se localizar a filial, agência, sucursal ou estabelecimento, a qual será considerada como sua sede, conforme Instrução Normativa DREI/ME n.º 77, de 18 de março de 2020;

10.4.6. Sociedade simples: inscrição do ato constitutivo no Registro Civil de Pessoas Jurídicas do local de sua sede, acompanhada de documento comprobatório de seus administradores;

10.4.7. Filial, sucursal ou agência de sociedade simples ou empresária: inscrição do ato constitutivo da filial, sucursal ou agência da sociedade simples ou empresária, respectivamente, no Registro Civil das Pessoas Jurídicas ou no Registro Público de Empresas Mercantis onde opera, com averbação no Registro onde tem sede a matriz;

10.4.8. Sociedade cooperativa: ata de fundação e estatuto social, com a ata da assembleia que o aprovou, devidamente arquivado na Junta Comercial ou inscrito no Registro Civil das Pessoas Jurídicas da respectiva sede, além do registro de que trata o art. 107 da Lei nº 5.764, de 16 de dezembro 1971.

10.4.9. Os documentos apresentados deverão estar acompanhados de todas as alterações ou da consolidação respectiva.

10.5. HABILITAÇÃO FISCAL, SOCIAL E TRABALHISTA

10.5.1. Prova de inscrição no Cadastro Nacional de Pessoas Jurídicas ou no Cadastro de Pessoas Físicas, conforme o caso;

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

10.5.3. Prova de regularidade com o Fundo de Garantia do Tempo de Serviço (FGTS);

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

10.5.5. Prova de inscrição no cadastro de contribuintes Estadual ou Distrital relativo ao domicílio ou sede do fornecedor, pertinente ao seu ramo de atividade e compatível com o objeto contratual;

10.5.6. Prova de regularidade com a Fazenda Estadual ou Distrital do domicílio ou sede do fornecedor, relativa à atividade em cujo exercício contrata ou concorre;

10.5.7. Caso o fornecedor seja considerado isento dos tributos relacionados ao objeto contratual, deverá comprovar tal condição mediante a apresentação de declaração da Fazenda respectiva do seu domicílio ou sede, ou outra equivalente, na forma da lei.

10.5.8. O fornecedor enquadrado como microempreendedor individual que pretenda auferir os benefícios do tratamento diferenciado previstos na Lei Complementar n. 123, de 2006, estará dispensado da prova de inscrição nos cadastros de contribuintes estadual e municipal.

10.6. QUALIFICAÇÃO ECONÔMICO-FINANCEIRA

10.6.1. certidão negativa de insolvência civil expedida pelo distribuidor do domicílio ou sede do interessado, caso se trate de pessoa física, desde que admitida a sua participação na licitação/contratação, ou de sociedade simples;

10.6.2. certidão negativa de falência expedida pelo distribuidor da sede do fornecedor;

10.6.3. balanço patrimonial, demonstração de resultado de exercício e demais demonstrações contábeis dos dois últimos exercícios sociais, já exigíveis e apresentados na forma da lei, comprovando, índices de Liquidez Geral (LG), Liquidez Corrente (LC), e Solvência Geral (SG) superiores a 1 (um), obtidos por meio da aplicação das seguintes fórmulas:

LG =	Ativo Circulante + Realizável a Longo Prazo
	Passivo Circulante + Passivo Não Circulante

SG =	Ativo Total
	Passivo Circulante + Passivo Não Circulante

LC =	Ativo Circulante
	Passivo Circulante

10.6.4. Caso a empresa apresente resultado inferior ou igual a 1 (um) em qualquer dos índices de Liquidez Geral (LG), Solvência Geral (SG) e Liquidez Corrente (LC), será exigido, para fins de habilitação, patrimônio líquido mínimo de 10% (dez por cento) do valor total estimado da contratação.

10.6.5. Os indicadores fixados acima deverão ser atingidos em cada um dos dois últimos exercícios sociais, sob pena de inabilitação.

10.6.6. 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.

10.6.7. Os documentos referidos acima deverão ser exigidos com base no limite definido pela Receita Federal do Brasil para transmissão da Escrituração Contábil Digital - ECD ao Sped.

10.6.8. As empresas criadas no exercício financeiro da licitação/contratação deverão atender a todas as exigências da habilitação e poderão substituir os demonstrativos contábeis pelo balanço de abertura.

10.6.9. O atendimento dos índices econômicos previstos neste termo de referência deverá ser atestado mediante declaração assinada por profissional habilitado da área contábil, apresentada pelo fornecedor.

10.7. QUALIFICAÇÃO TÉCNICA

10.7.1. Comprovação de aptidão para o fornecimento de bens e a prestação de serviços similares, de complexidade tecnológica e operacional equivalente ou superior à do objeto desta contratação, ou do item pertinente, por meio da apresentação de certidões ou atestados emitidos por pessoas jurídicas de direito público ou privado.

10.7.2. Para fins da comprovação de que trata o subitem anterior, os atestados deverão demonstrar a execução de contratos com as seguintes características mínimas:

10.7.2.1. Apresentação de atestado(s) de capacidade técnica, emitido(s) por pessoa jurídica de direito público ou privado, que comprove (m) o fornecimento, implantação e entrada em operação de solução corporativa de *Application Delivery Controller (ADC)* com funcionalidades integradas de *Web Application Firewall (WAF)*, em ambiente de produção, com complexidade tecnológica e operacional equivalente ou superior ao objeto desta contratação.

10.7.2.2. Para fins de comprovação da capacidade técnica, será(ão) considerado(s) pertinente(s) o(s) atestado(s) que demonstre(m), isolada ou cumulativamente:

10.7.2.2.1. fornecimento, implantação e entrada em operação de pelo menos uma solução de *Application Delivery Controller (ADC)* com funcionalidades de *Web Application Firewall (WAF)*, em ambiente de produção;

10.7.2.2.2. execução de serviços de instalação, configuração e entrada em operação da solução de *Application Delivery Controller (ADC)* com funcionalidades de *Web Application Firewall (WAF)*;

10.7.2.2.3. prestação de serviços de suporte técnico especializado em regime 24x7, pelo período mínimo de 12 (doze) meses;

10.7.2.2.4. execução de migração ou substituição de solução de *Application Delivery Controller (ADC)* em ambiente de produção, preservando a continuidade dos serviços;

10.7.2.2.5. execução dos serviços em ambiente de produção cuja indisponibilidade pudesse causar impacto à continuidade das atividades da organização contratante.

10.7.4. Será admitida a soma de atestados para fins de comprovação dos requisitos estabelecidos, desde que demonstrada a compatibilidade entre os objetos executados e o objeto desta contratação.

10.7.5. Os atestados deverão conter informações suficientes para a verificação de sua autenticidade e veracidade, incluindo, no mínimo:

10.7.5.1. identificação da pessoa jurídica emitente;

10.7.5.2. descrição do objeto contratado;

10.7.5.3. período de execução;

10.7.5.4. identificação do responsável pelas informações.

10.7.6. Serão admitidos, para fins de comprovação de quantitativo mínimo exigido, a apresentação e o somatório de diferentes atestados relativos a contratos executados de forma concomitante.

10.7.7. Os atestados de capacidade técnica poderão ser apresentados em nome da matriz ou da filial do fornecedor.

10.7.8. A licitante disponibilizará todas as informações necessárias à comprovação da legitimidade dos atestados, apresentando, quando solicitado pela Administração, cópia do contrato que deu suporte à contratação, endereço atual do CONTRATANTE e local em que foi executado o objeto Contratado, dentre outros documentos.

10.7.9. A Administração poderá, a qualquer tempo, realizar diligências junto aos emitentes dos atestados, com o objetivo de verificar a efetiva execução dos serviços declarados, podendo ser solicitadas informações adicionais ou documentos complementares que comprovem a experiência informada, nos termos da legislação vigente.

10.8. DISPOSIÇÕES GERAIS SOBRE HABILITAÇÃO

10.8.1. Quando permitida a participação de empresas estrangeiras que não funcionem no País, as exigências de habilitação serão atendidas mediante documentos equivalentes, inicialmente apresentados em tradução livre.

10.8.2. Na hipótese de o fornecedor ser empresa estrangeira que não funcione no País, para assinatura do contrato ou da ata de registro de preços ou do aceite do instrumento equivalente, os documentos exigidos para a habilitação serão traduzidos por tradutor juramentado no País e apostilados nos termos do disposto no Decreto nº 8.660, de 29 de janeiro de 2016, ou de outro que venha a substituí-lo, ou consularizados pelos respectivos consulados ou embaixadas.

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

10.8.4. Se o fornecedor for a matriz, todos os documentos deverão estar em nome da matriz, e se o fornecedor for a filial, todos os documentos deverão estar em nome da filial, exceto para atestados de capacidade técnica, e no caso daqueles documentos que, pela própria natureza, comprovadamente, forem emitidos somente em nome da matriz.

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

11. ESTIMATIVAS DO VALOR DA CONTRATAÇÃO

11.1. O custo estimado total da contratação, que corresponde ao valor máximo aceitável, é de **R$ 6.046.270,63 (seis milhões, quarenta e seis mil, duzentos e setenta reais e sessenta e três centavos)**, conforme custos unitários apostos na tabela contida no item 1.1 deste Termo de Referencia.

11.2. A estimativa de custo levou em consideração o risco envolvido na contratação e sua alocação entre CONTRATANTE e CONTRATADO, conforme especificado na matriz de risco constante do Contrato.

12. ADEQUAÇÃO ORÇAMENTÁRIA

12.1. As despesas decorrentes da presente contratação correrão à conta de recursos específicos consignados no Orçamento Geral da União.

12.2. A contratação será atendida pela seguinte dotação:

12.2.1. Ação: **2000**

12.2.1. Gestão/unidade: **364102**

12.2.2. Fonte de recursos: **1000000000**

12.2.3. Programa de trabalho: **173704**

12.2.4. Elemento de despesa: **339040**

12.2.5. Plano interno: **20000234006**

12.3. A dotação relativa aos exercícios financeiros subsequentes será indicada após aprovação da Lei Orçamentária respectiva e liberação dos créditos correspondentes, mediante apostilamento.

13. DISPOSIÇÕES FINAIS

13.1. As informações contidas neste Termo de Referência não são classificadas como sigilosas.

13.2. CRONOGRAMA FÍSICO FINANCEIRO

13.2.1. O pagamento dos itens previstos neste cronograma estará condicionado ao efetivo cumprimento das obrigações contratuais, à verificação dos critérios de aceitação e ao atendimento dos níveis mínimos de serviço definidos neste Termo de Referência.

ITEM	DESCRIÇÃO	PRAZO ESTIMADO DE ENTREGA/EXECUÇÃO	PRAZO ESTIMADO DE PAGAMENTO	PERIODICIDADE DO PAGAMENTO
1	*Appliance de Application Delivery Controller (ADC)* baseada na plataforma F5 BIG-IP, com funcionalidades integradas de *Web Application Firewall (WAF)*	Até 60 (sessenta) dias corridos, contados da emissão da Ordem de Fornecimento de Bens (OFB) ou instrumento equivalente.	Após o recebimento definitivo do objeto, condicionado à verificação da instalação física, do pleno funcionamento dos equipamentos, da conformidade com as especificações deste Termo de Referência, da integração ao ambiente da CONTRATANTE e da emissão do Termo de Recebimento Definitivo (TRD).	**Pagamento único**, correspondente a 100% do valor do item, após a entrega, instalação e recebimento definitivo do equipamento, mediante emissão do TRD.
2	Licenças de software F5 BIG-IP	Até 60 (sessenta) dias corridos, contados da emissão da Ordem de Serviços (OS) ou instrumento equivalente.	Após o recebimento definitivo do objeto, condicionado à comprovação da ativação, validade e pleno funcionamento das licenças, bem como à emissão do Termo de Recebimento Definitivo (TRD).	**Pagamento único**, correspondente a 100% do valor do item, após a disponibilização, ativação e recebimento definitivo das licenças, mediante emissão do TRD.
3	Garantia e suporte técnico oficial do fabricante para a solução F5 BIG-IP (60 meses)	Até 60 (sessenta) dias corridos, contados da emissão da Ordem de Serviços (OS) ou instrumento equivalente. Ativação da garantia e suporte oficial no início da execução contratual, com cobertura contínua durante 60 meses.	Pagamento anual, após o recebimento definitivo da cobertura correspondente ao respectivo período anual, condicionado à comprovação da manutenção da garantia e do suporte técnico oficial do fabricante, mediante emissão do Termo de Recebimento Definitivo (TRD).	**Pagamento anual**, em 5 (cinco) parcelas anuais iguais e sucessivas, condicionado ao recebimento definitivo da cobertura correspondente a cada período anual, mediante emissão do respectivo TRD.
4	Subscrições e assinaturas de segurança da plataforma F5 BIG-IP (60 meses)	Até 60 (sessenta) dias corridos, contados da emissão da Ordem de Serviços (OS) ou instrumento equivalente. Ativação das subscrições no início da execução contratual, com cobertura contínua durante 60 meses.	Pagamento anual, após o recebimento definitivo das subscrições e assinaturas de segurança correspondentes ao respectivo período anual, condicionado à comprovação de sua ativação, validade e funcionamento, mediante emissão do Termo de Recebimento Definitivo (TRD).	**Pagamento anual**, em 5 (cinco) parcelas anuais iguais e sucessivas, condicionado ao recebimento definitivo da cobertura correspondente a cada período anual, mediante emissão do respectivo Termo de Recebimento Definitivo (TRD).
			Após o recebimento definitivo dos serviços, condicionado à validação da	

5	Serviços especializados de instalação, configuração, implantação, migração, integração, testes e entrada em produção	Até 60 (sessenta) dias corridos, contados da conclusão da entrega dos itens 1 a 4, compreendendo instalação, configuração, implantação, migração, integração, testes e entrada em produção da solução	implantação completa da solução, incluindo migração, integração, testes de funcionamento, testes de alta disponibilidade, entrada em produção e aceite formal da CONTRATANTE, mediante emissão do Termo de Recebimento Definitivo (TRD).	**Pagamento único**, correspondente a 100% do valor do item, após a conclusão dos serviços de implantação e o recebimento definitivo, mediante emissão do TRD.
6	Serviços de consultoria técnica especializada (sob demanda)	Conforme Ordem de Serviço (OS), sob demanda da CONTRATANTE	Após o recebimento definitivo dos serviços executados em cada Ordem de Serviço, mediante emissão do Termo de Recebimento Definitivo (TRD).	Conforme cada Ordem de Serviço executada e recebida definitivamente.
7	Serviços de suporte técnico especializado da contratada em regime 24x7	Serviços prestados mensalmente, durante toda a vigência contratual, mediante Ordens de Serviço emitidas pela CONTRATANTE.	Mensalmente, após o recebimento definitivo dos serviços prestados no período, condicionado ao atendimento dos níveis mínimos de serviço (SLA), especialmente ao indicador ISA, e à emissão do correspondente Termo de Recebimento Definitivo (TRD).	**Pagamento mensal**, condicionado ao recebimento definitivo dos serviços prestados no período, ao atendimento dos níveis mínimos de serviço (SLA) estabelecidos neste Termo de Referência, e à emissão do respectivo Termo de Recebimento Definitivo (TRD).

13.2.2. Os itens 1, 2 e 5 serão pagos em parcela única, após o respectivo recebimento definitivo, condicionado ao cumprimento das obrigações contratuais e à verificação dos critérios de aceitação estabelecidos para cada item, mediante emissão do correspondente Termo de Recebimento Definitivo (TRD).

13.2.3. Os itens 3 e 4 terão seus valores divididos em 5 (cinco) parcelas anuais e sucessivas, permanecendo a garantia e o suporte técnico oficial do fabricante, bem como as subscrições e assinaturas de segurança, vigentes durante toda a vigência contratual de 60 (sessenta) meses. O pagamento de cada parcela ocorrerá anualmente, após a emissão do correspondente Termo de Recebimento Definitivo (TRD), condicionado à comprovação da manutenção da cobertura de garantia e suporte e da vigência das subscrições e assinaturas de segurança correspondentes ao respectivo período.

13.2.4. O item 6 será executado sob demanda, mediante solicitação da CONTRATANTE por meio de Ordem de Serviço (OS), sendo o pagamento realizado após o recebimento definitivo dos serviços efetivamente executados e a emissão do correspondente Termo de Recebimento Definitivo (TRD).

13.2.5. O item 7 será remunerado mensalmente, após o recebimento definitivo dos serviços prestados no respectivo período, condicionado ao atendimento dos níveis mínimos de serviço (SLA) estabelecidos neste Termo de Referência e à emissão do correspondente Termo de Recebimento Definitivo (TRD).

Item	Descrição	1º Ano	2º Ano	3º Ano	4º Ano	5º Ano
1	Custos da Aquisição dos *appliances ADC/WAF*	R$ 1.409.742,58	-	-	-	-
2	Custos do Licenciamento da solução F5 BIG-IP	R$ 1.044.792,90	-	-	-	-

3	Custos da Garantia e suporte técnico oficial do fabricante (60 meses)	R$ 308.332,99	R$ 308.332,99	R$ 308.332,99	R$ 308.332,99	R$ 308.333,02
4	Custos da Subscrições e assinaturas de segurança (60 meses)	R$ 187.243,02	R$ 187.243,02	R$ 187.243,02	R$ 187.243,02	R$ 187.243,04
5	Custos dos Serviços especializados de implantação	R$ 259.951,25	-	-	-	-
6	Custos dos Serviços de consultoria técnica especializada (sob demanda)	R$ 54.912,00	R$ 54.912,00	R$ 54.912,00	R$ 54.912,00	R$ 54.912,00
7	Custos dos Serviços de suporte técnico especializado da contratada (24x7)	R$ 115.868,76	R$ 115.868,76	R$ 115.868,76	R$ 115.868,76	R$ 115.868,76
Total anual estimado		**R$ 3.380.843,50**	**R$ 666.356,77**	**R$ 666.356,77**	**R$ 666.356,77**	**R$ 666.356,82**
Valor global estimado da contratação						**R$ 6.046.270,63**

13.2.6. Os valores apresentados na Tabela acima possuem caráter meramente estimativo e destinam-se ao planejamento da execução orçamentária da contratação, podendo sofrer alterações em razão dos valores efetivamente adjudicados na licitação e da efetiva execução dos serviços. No caso dos serviços de consultoria técnica especializada (item 6), a distribuição anual apresentada constitui apenas referência para fins de planejamento orçamentário, não limitando a quantidade de horas a ser executada em cada exercício, que observará a demanda efetiva da CONTRATANTE, as Ordens de Serviço emitidas e o saldo global contratado.

13.2.7. Para fins de faturamento, a CONTRATADA deverá apresentar a proposta comercial e emitir os respectivos documentos fiscais observando a estrutura dos itens desta contratação, discriminando individualmente os equipamentos, licenças de software, garantia e suporte técnico oficial do fabricante, subscrições e assinaturas de segurança, serviços especializados de implantação, serviços de consultoria técnica especializada e serviços de suporte técnico especializado, com seus respectivos valores unitários e totais, de forma a possibilitar a adequada identificação do objeto faturado e a correta liquidação da despesa.

14. Responsáveis

Todas as assinaturas eletrônicas seguem o horário oficial de Brasília e fundamentam-se no §3º do Art. 4º do Decreto nº 10.543, de 13 de novembro de 2020.

IRISLENISSON DE SOUZA OLIVEIRA

Integrante Requisitante

Assinou eletronicamente em 19/08/2026 às 14:25:49.

LEONARDO FABIANO SEGER

Integrante Técnico

Assinou eletronicamente em 19/08/2026 às 14:29:27.

JOAO PAULO DOS REIS JUNIOR

Integrante Administrativo

Assinou eletronicamente em 19/08/2026 às 15:06:57.

gov.br
Documento assinado digitalmente
GERALDO SORTE
Data: 21/08/2026 15:31:12-0300
Verifique em https://validar.iti.gov.br

GERALDO SORTE

Autoridade Máxima de TIC

gov.br
Documento assinado digitalmente
DEBORA PERES MENEZES
Data: 21/08/2026 16:17:18-0300
Verifique em https://validar.iti.gov.br

DEBORA PERES MENEZES

Autoridade competente

Lista de Anexos

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

- Anexo I - ESPECIFICACAO TECNICA MINIMA DA SOLUCAO.pdf (520.88 KB)
- Anexo II - MATRIZ DE COMPROVACAO DE ATENDIMENTO A ESPECIFICACAO TECNICA MINIMA DA. pdf (473.69 KB)
- Anexo III - TERMO DE COMPROMISSO DE MANUTENCAO DE SIGILO.pdf (249.18 KB)
- Anexo IV - TERMO DE CIENCIA.pdf (194.14 KB)
- Anexo V - MODELO DO TERMO DE VISTORIA TECNICA.pdf (178.52 KB)
- Anexo VI - MODELO DE RECUSA DE VISTORIA TECNICA.pdf (183.8 KB)
- Anexo VII - PLANILHA DE CUSTOS E FORMACAO DE PRECOS PARA CONTRATACAO DE SOFTWARE. pdf (248.51 KB)
- Anexo VIII - PLANILHA DE COMPOSICAO DE CUSTOS E FORMACAO DE PRECOS DE CONSULTORIA. pdf (246.03 KB)

CONSELHO NACIO DE DESEN. CIENT. E TECNOLÓGICO

Estudo Técnico Preliminar 51/2026

1. Informações Básicas

Número do processo: 01300.003396/2025-91

2. Descrição da necessidade

2.1. A presente contratação tem por objetivo modernizar a infraestrutura responsável pela entrega e proteção de aplicações institucionais do Conselho Nacional de Desenvolvimento Científico e Tecnológico - CNPq.

2.2. MOTIVAÇÃO/JUSTIFICATIVA

2.2.1. O ambiente de balanceamento de carga de aplicações do Conselho Nacional de Desenvolvimento Científico e Tecnológico – CNPq utiliza atualmente equipamentos da plataforma *F5 BIG-IP VIPRION*, operando na versão *10.2.4 Build 864.0 Hotfix HF11*, com licenciamento do tipo *Perpetual (Production)* datado de 08 de dezembro de 2011.

2.2.2. Trata-se de uma versão significativamente defasada da plataforma *F5 BIG-IP*, cuja manutenção e suporte técnico pelo fabricante encontram-se descontinuados.

2.2.3. A versão atualmente em uso foi lançada há mais de uma década e encontra-se oficialmente fora do ciclo de suporte do fabricante (*End of Technical Support - EoTS*), não recebendo atualizações de segurança, correções de falhas, melhorias de desempenho ou suporte técnico oficial.

2.2.4. Em razão dessa defasagem tecnológica, o ambiente atual apresenta riscos relevantes à segurança, estabilidade e disponibilidade dos serviços críticos hospedados na infraestrutura de aplicações do CNPq, além de dificultar o atendimento às boas práticas de governança e segurança da informação adotadas no âmbito da Administração Pública Federal.

2.2.5. A versão *BIG-IP 10.2.4* encontra-se substancialmente aquém das versões atualmente suportadas pelo fabricante (linhas 16.x e 17. x), apresentando incompatibilidades com padrões modernos de segurança, desempenho e automação.

2.2.6. Entre as principais limitações observadas, destacam-se:

2.2.6.1. ausência de suporte aos protocolos TLS 1.3 e HTTP/2, impactando a segurança e o desempenho das conexões criptografadas;

2.2.6.2. incompatibilidade com mecanismos modernos de automação, orquestração e integração baseados em APIs, utilizados em ambientes de infraestrutura programável, provisionamento automatizado e automação de serviços;

2.2.6.3. funcionalidades limitadas do módulo de *Firewall* de Aplicações Web (WAF - ASM), sem atualização de assinaturas para ameaças recentes e sem mecanismos avançados de mitigação comportamental;

2.2.6.4. limitações do módulo *APM (Access Policy Manager)*, com suporte restrito a mecanismos modernos de autenticação e federação de identidade, como *SAML 2.0, OAuth 2.0 e OpenID Connect*;

2.2.6.5. inexistência de correções para vulnerabilidades críticas divulgadas nos últimos anos, o que pode expor o ambiente a riscos de exploração remota.

2.2.7. Adicionalmente, a versão atualmente em uso apresenta incompatibilidade com plataformas modernas de *hardware* e versões mais recentes do sistema operacional TMOS, impossibilitando a atualização direta para versões suportadas.

2.2.8. A manutenção da infraestrutura baseada no *BIG-IP 10.2.4 HF11* implica na permanência de um ambiente em estado avançado de obsolescência tecnológica, com impactos diretos sobre a segurança, disponibilidade e conformidade da infraestrutura de aplicações.

2.2.9. Entre os principais riscos identificados, destacam-se:

CATEGORIA	RISCO	IMPACTO POTENCIAL
Segurança	Exploração de vulnerabilidades críticas conhecidas	Comprometimento da plataforma e das aplicações
Disponibilidade	Falhas não corrigidas no sistema operacional e componentes de rede	Interrupção de serviços críticos
Conformidade	Desalinhamento com políticas institucionais e *frameworks* de segurança	Riscos administrativos e reputacionais
Suporte Técnico	Ausência de suporte oficial do fabricante	Dificuldade de recuperação em incidentes críticos
Arquitetura	Topologia de rede inadequada	Ampliação da superfície de ataque

2.2.10. Ressalta-se que, por se tratar de solução fora do ciclo de suporte, não há possibilidade de obtenção de correções, atualizações de *firmware* ou suporte técnico oficial do fabricante, o que compromete a capacidade de resposta a incidentes de segurança e recuperação do ambiente em caso de falhas críticas.

2.2.11. Diante do exposto, verifica-se que o ambiente de balanceamento de carga e proteção de aplicações atualmente em operação encontra-se em estado avançado de obsolescência tecnológica, não atendendo aos níveis mínimos aceitáveis de segurança, disponibilidade e conformidade exigidos para a infraestrutura de TIC do CNPq.

2.2.12. A permanência desse cenário implica na aceitação formal de riscos institucionais, uma vez que eventuais incidentes decorrentes de vulnerabilidades conhecidas não poderão ser mitigados em razão da ausência de suporte técnico e atualizações do fabricante.

2.2.13. Nesse contexto, torna-se necessária a modernização da plataforma de balanceamento de carga e proteção de aplicações, contemplando:

2.2.13.1. atualização tecnológica da solução;

2.2.13.2. adoção de versões suportadas pelo fabricante;

2.2.13.3. implantação de recursos modernos de segurança e desempenho;

2.2.13.4. revisão da arquitetura da topologia de rede;

2.2.13.5. contratação de suporte técnico especializado.

2.2.14. A modernização da solução visa assegurar a continuidade operacional, a disponibilidade dos serviços digitais, a integridade das aplicações e a aderência às diretrizes de segurança da informação aplicáveis à Administração Pública Federal.

2.2.15. Adicionalmente, levantamento técnico detalhado do ambiente atual evidenciou elevado grau de criticidade e dependência da solução atualmente implantada, destacando-se:

2.2.15.1. existência de mais de 120 (cento e vinte) serviços de aplicações publicados por meio da plataforma de balanceamento;
2.2.15.2. utilização intensiva de regras customizadas (*iRules*), com mais de 100 (cem) implementações ativas, responsáveis por controle de acesso, segurança e tratamento de tráfego;
2.2.15.3. atuação da solução como elemento central de publicação e proteção de praticamente todos os sistemas institucionais;
2.2.15.4. dependência direta da solução para funcionamento de aplicações críticas, como Plataforma Lattes, sistemas de fomento, portais institucionais e serviços internos.

2.2.16. Tal cenário evidencia que a solução atualmente em operação desempenha papel estrutural na arquitetura de tecnologia da informação do CNPq, sendo responsável não apenas pelo balanceamento de carga, mas também por funções críticas de segurança, controle de acesso e observabilidade do tráfego de aplicações.

3. Área requisitante

Área Requisitante	Responsável
Coordenação de Infraestrutura de Tecnologia da Informação - COINT	Ana Paula Mendes Teixeira

4. Necessidades de Negócio

4.1. De maneira inicial e não exaustiva, podem ser identificadas as seguintes necessidades de negócio relacionadas à modernização do ambiente de balanceamento de carga e segurança de aplicações do CNPq:

4.1.1. Assegurar a continuidade operacional, a disponibilidade e a confiabilidade dos serviços de aplicações institucionais do CNPq, por meio da modernização da plataforma de balanceamento de carga e segurança de aplicações, eliminando riscos decorrentes da obsolescência tecnológica do ambiente atualmente em operação.

4.1.2. Garantir que a solução adotada esteja alinhada ao ciclo de suporte do fabricante, com acesso a suporte técnico oficial, atualizações regulares de software e correções de vulnerabilidades, de forma a reduzir riscos operacionais, de segurança e de indisponibilidade dos serviços institucionais.

4.1.3. Assegurar a disponibilidade contínua dos serviços, inclusive durante atividades de manutenção, atualização de *software*, substituição de componentes ou tratamento de falhas, de modo a não impactar o acesso dos usuários às funcionalidades críticas disponibilizadas pela instituição.

4.1.4. Atender às demandas atuais e futuras do negócio, suportando a evolução tecnológica dos sistemas institucionais, bem como a ampliação do volume de acessos, transações e integrações com outros órgãos e sistemas governamentais.

4.1.5. Promover a melhoria da experiência do usuário no acesso às aplicações institucionais, garantindo desempenho adequado, baixa latência e elevada taxa de disponibilidade, especialmente em períodos de maior utilização ou de demandas sazonais.

4.1.6. Assegurar o atendimento aos Acordos de Nível de Serviço estabelecidos pela instituição, com operação em regime contínuo de disponibilidade, 24 horas por dia e 7 dias por semana (24x7), suportando serviços essenciais ao funcionamento do CNPq.

4.1.7. Reduzir a exposição a riscos de segurança da informação, por meio da correção de falhas de segurança conhecidas, mitigação de vulnerabilidades críticas e adoção de mecanismos atualizados de proteção às aplicações e aos dados institucionais.

4.1.8. Garantir que a solução de balanceamento de carga possua capacidade adequada de processamento e desempenho, evitando gargalos que possam comprometer a prestação dos serviços institucionais, mesmo em cenários de aumento súbito de demanda.

4.1.9. Assegurar o correto dimensionamento da solução, considerando:

4.1.9.1. A carga atual de trabalho, de forma a garantir fluidez, estabilidade e desempenho no acesso às aplicações e sistemas em produção.

4.1.9.2. A carga futura estimada, assegurando escalabilidade, crescimento sustentável e longevidade da solução, evitando novas contratações emergenciais no curto ou médio prazo.

4.1.10. Garantir a manutenção evolutiva da solução, com acesso a atualizações regulares de software disponibilizadas pelo fabricante, incluindo melhorias de desempenho, compatibilidade com novas tecnologias e correções de falhas de segurança durante toda a vigência contratual.

4.1.11. Assegurar a proteção das aplicações web institucionais contra ataques cibernéticos direcionados à camada de aplicação, tais como injeção de código, *cross-site scripting (XSS)*, exploração de vulnerabilidades, ataques automatizados e outras ameaças descritas em boas práticas internacionais de segurança de aplicações.

4.1.12. Possibilitar a inspeção, análise e controle do tráfego de aplicações web por meio de mecanismos especializados de *firewall* de aplicações web (WAF), capazes de identificar, bloquear e mitigar atividades maliciosas antes que estas atinjam os servidores de aplicação.

4.1.13. Prover mecanismos de distribuição inteligente de tráfego entre múltiplos servidores ou instâncias de aplicação, permitindo a otimização do uso dos recursos computacionais disponíveis e evitando sobrecarga em componentes individuais da infraestrutura.

4.1.14. Permitir a implementação de arquiteturas de alta disponibilidade e recuperação de desastres, possibilitando o redirecionamento automático do tráfego para ambientes alternativos em caso de falhas ou indisponibilidade de serviços.

4.1.15. Assegurar compatibilidade com arquiteturas modernas de aplicações, incluindo ambientes virtualizados, plataformas de containers, microsserviços e interfaces de programação de aplicações (APIs), de modo a suportar a evolução tecnológica dos sistemas institucionais.

4.1.16. Possibilitar a integração com ferramentas de automação e gerenciamento de infraestrutura, permitindo a adoção de práticas modernas de operação de ambientes de tecnologia da informação, tais como automação de configurações, integração com pipelines de desenvolvimento e gerenciamento programático da infraestrutura.

4.1.17. Prover mecanismos de monitoramento, auditoria e geração de relatórios que permitam maior visibilidade sobre o tráfego das aplicações, identificação de comportamentos anômalos e suporte às atividades de governança e gestão da segurança da informação.

4.1.18. Reduzir a complexidade operacional da infraestrutura de entrega e proteção de aplicações, consolidando funcionalidades de balanceamento de carga, segurança de aplicações e otimização de tráfego em uma plataforma integrada, contribuindo para maior eficiência operacional e melhor aproveitamento dos recursos tecnológicos disponíveis.

4.2. A continuidade operacional depende da substituição por solução compatível com a arquitetura atual.

5. Necessidades Tecnológicas

5.1. As necessidades tecnológicas, também denominadas requisitos da solução de tecnologia, descrevem as características que a solução deverá possuir para atender às necessidades institucionais do CNPq, considerando aspectos de segurança, desempenho, disponibilidade e evolução da infraestrutura.

5.2. No contexto do CNPq, tais requisitos orientam a definição de soluções capazes de sustentar serviços digitais críticos, em especial a Plataforma Lattes, incluindo o Currículo Lattes, a Plataforma Integrada Carlos Chagas - PICC e demais sistemas institucionais do CNPq, que desempenham papel estruturante para a ciência, tecnologia e inovação no Brasil.

5.3. A Plataforma Lattes e os demais sistemas institucionais do CNPq processam e armazenam elevado volume de dados pessoais, acadêmicos e profissionais sensíveis, incluindo informações de pesquisadores, bolsistas, instituições de pesquisa e produção científica nacional.

5.4. A indisponibilidade ou degradação dos sistemas institucionais do CNPq pode impactar diretamente a execução de políticas públicas, a concessão de bolsas e auxílios e a avaliação da produção científica nacional, configurando risco institucional relevante.

5.5. Nesse contexto, as soluções tecnológicas adotadas devem garantir não apenas o funcionamento operacional, mas também a continuidade dos serviços, a resiliência da infraestrutura e a mitigação de riscos associados a falhas, indisponibilidades e incidentes de segurança.

5.6. Os requisitos tecnológicos são classificados em:

5.6.1. Requisitos funcionais: Correspondem às capacidades que a solução deve prover em termos de comportamento, processamento e resposta.

5.6.2. Requisitos não funcionais: Relacionam-se a atributos de qualidade, como desempenho, escalabilidade, disponibilidade, segurança e capacidade.

5.6.3. Requisitos de transição: Migração controlada de configurações, a preservação da continuidade dos serviços e a minimização de impactos durante o processo de substituição ou evolução da infraestrutura atual.

5.7. A definição dos requisitos considera as diretrizes estabelecidas no Guia de Requisitos Mínimos de Privacidade e Segurança da Informação para Aplicações Web do Governo Federal (versão 2.0), bem como normativos relacionados à proteção de dados e segurança da informação.

5.8. Dentre os principais aspectos a serem atendidos, destacam-se:

5.8.1. Garantia da confidencialidade, integridade e disponibilidade das informações;

5.8.2. Implementação de mecanismos de controle de acesso e auditoria;

5.8.3. Proteção contra vulnerabilidades exploradas em aplicações web;

5.8.4. Uso de criptografia para proteção de dados em trânsito e, quando aplicável, em repouso;

5.8.5. Registro e monitoramento de eventos de segurança;

5.8.6. Adoção de práticas de hardening e atualização contínua dos sistemas.

5.9. A definição dos requisitos tecnológicos considera, ainda, a necessidade de adoção de abordagens modernas de segurança, incluindo o princípio de "Zero Trust", no qual nenhuma comunicação é automaticamente confiável, sendo exigidos mecanismos contínuos de verificação, inspeção e controle do tráfego de dados.

5.10. NECESSIDADES TECNOLÓGICAS DA SOLUÇÃO

5.10.1. Prover balanceamento de carga de aplicações em múltiplas camadas (L4 - L7), garantindo alta disponibilidade e distribuição eficiente do tráfego.

5.10.2. Prover publicação segura das aplicações institucionais.

5.10.3. Proteger aplicações contra ameaças da camada de aplicação, incluindo ataques baseados em vulnerabilidades conhecidas.

5.10.4. Prover mecanismos de *Web Application Firewall (WAF)* para proteção contra ataques como injeção de código, *cross-site scripting* e outras ameaças descritas no OWASP Top 10.

5.10.5. Permitir inspeção e controle de tráfego criptografado (SSL/TLS), garantindo visibilidade e aplicação de políticas de segurança.

5.10.6. Implementar mecanismos de proteção contra ataques de negação de serviço (DoS/DDoS).

5.10.7. Permitir definição de políticas granulares de controle de tráfego, baseadas em aplicações, usuários ou contexto.

5.10.8. Prover monitoramento contínuo do estado de saúde das aplicações e serviços.

5.10.9. Disponibilizar geração de relatórios operacionais e de segurança.

5.10.10. Permitir gerenciamento centralizado da solução.

5.10.11. Permitir integração com diretórios corporativos, ferramentas de monitoramento e sistemas existentes.

5.10.12. Permitir integração com ambientes modernos, incluindo containers e microsserviços.

5.10.13. Prover proteção contra bots e automações maliciosas.

5.10.14. Permitir proteção e inspeção de APIs.

5.10.15. Prover balanceamento global baseado em DNS (GSLB).

5.10.16. Disponibilizar métricas e visibilidade sobre o tráfego e desempenho.

5.10.17. Permitir visibilidade abrangente do tráfego e do comportamento das aplicações, possibilitando a identificação proativa de anomalias, degradações de desempenho e potenciais incidentes de segurança.

5.10.18. Ser capaz de suportar ambientes com elevado grau de customização, incluindo a implementação de regras avançadas de tratamento de tráfego, controle de acesso e segurança, por meio de mecanismos programáveis e políticas definidas em nível de aplicação.

5.10.19. Permitir a migração controlada dessas regras, assegurando a continuidade das políticas de segurança, controle de acesso e comportamento das aplicações, de forma a preservar as funcionalidades existentes.

5.11. As necessidades tecnológicas associadas à solução pretendida decorrem da análise do ambiente atual, das demandas institucionais e dos requisitos de segurança, desempenho e disponibilidade necessários para suportar os sistemas críticos do CNPq.

5.12. Uma plataforma de *Application Delivery Controller (ADC)* com funcionalidades integradas de segurança de aplicações constitui solução adequada para atender às necessidades descritas, por possibilitar a entrega otimizada, segura e altamente disponível de aplicações institucionais.

5.13. A solução deverá ser capaz de operar de forma modular, permitindo a adoção das funcionalidades necessárias ao ambiente institucional, de forma escalável e evolutiva.

5.14. Em síntese, a solução deverá contemplar, de forma integrada, funcionalidades de balanceamento de carga, inspeção de tráfego criptografado, distribuição global de tráfego, proteção de aplicações web e APIs e mitigação de ataques de negação de serviço.

5.15. A solução deverá permitir a implementação de arquiteturas de alta disponibilidade, assegurando a continuidade dos serviços mesmo em cenários de falha.

5.16. A solução deverá possibilitar a definição de indicadores de desempenho, tais como:

5.16.1. tempo de resposta das aplicações;
5.16.2. taxa de erro nas requisições;
5.16.3. volume de tráfego processado;
5.16.4. disponibilidade dos serviços;
5.16.5. eventos de segurança detectados.

5.17. Esses indicadores deverão apoiar o monitoramento contínuo do ambiente e a tomada de decisão estratégica sobre a evolução da infraestrutura.

5.18. A modernização da infraestrutura permitirá ao CNPq elevar os níveis de segurança, desempenho e disponibilidade dos sistemas institucionais, além de possibilitar maior controle e visibilidade sobre o ambiente tecnológico.

5.19. A solução deverá suportar evolução tecnológica ao longo de seu ciclo de vida, permitindo a atualização de funcionalidades, mecanismos de segurança e componentes de *software*, bem como a expansão dos recursos disponíveis por meio de licenciamento ou atualização tecnológica, quando aplicável, preservada a compatibilidade da plataforma ofertada.

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

6.1. REQUISITOS LEGAIS

6.1.1. O presente processo de contratação deve estar aderente à:

6.1.1.1. Constituição Federal;

6.1.1.2. Lei nº 14.133, de 1º de abril de 2021 (Lei de Licitações e Contratos Administrativos);

6.1.1.3. Instrução Normativa SGD/ME nº 94, de 23 de dezembro de 2022, que dispõe sobre o processo de contratação de soluções de Tecnologia da Informação e Comunicação - TIC pelos órgãos e entidades integrantes do Sistema de Administração dos Recursos de Tecnologia da Informação - SISP do Poder Executivo Federal;

6.1.1.4. Portaria SGD/MGI nº 5.950, de 26 de outubro de 2023, que estabelece modelo de contratação de software e de serviços de computação em nuvem, no âmbito dos órgãos e entidades integrantes do Sistema de Administração dos Recursos de Tecnologia da Informação - SISP do Poder Executivo Federal;

6.1.1.5. Instrução Normativa SEGES/ME nº 65, de 7 de julho de 2021, que dispõe sobre o procedimento administrativo para a realização de pesquisa de preços para aquisição de bens e contratação de serviços em geral, no âmbito da administração pública federal direta, autárquica e fundacional;

6.1.1.6. Lei nº 13.709, de 14 de agosto de 2018 (Lei Geral de Proteção de Dados Pessoais – LGPD);

6.1.1.7. Decreto nº 10.947, de 25 de janeiro de 2022, que regulamenta o plano de contratações anual e institui o Sistema de Planejamento e Gerenciamento de Contratações no âmbito da administração pública federal direta, autárquica e fundacional;

6.1.1.8. Decreto nº 12.122, de 30 de julho de 2024, que institui o Programa Federal de Prevenção e Enfrentamento do Assédio e da Discriminação;

6.1.1.9. Plano Diretor de Logística Sustentável do CNPq 2026/2028 (CPLS/CNPq);

6.1.1.10. Resolução CGD/CNPq nº 2, de 3 de novembro de 2025, que dispõe sobre a estratégia de uso de software e de serviços de computação em nuvem, no âmbito do CNPq;

6.1.1.11. Decreto nº 12.572, de 24 de agosto de 2025, que institui a Política Nacional de Segurança da Informação e dispõe sobre a governança da segurança da informação no âmbito da administração pública federal;

6.1.1.12. Decreto nº 7.174, de 12 de maio de 2010, que regulamenta a contratação de bens e serviços de informática e automação pela administração pública federal, assegurando as preferências e certificações adequadas;
6.1.1.13. Instrução Normativa SLTI/MP nº 01, de 19 de janeiro de 2010, que dispõe sobre os critérios de sustentabilidade ambiental na aquisição de bens e contratação de serviços;
6.1.1.14. Lei nº 12.305, de 2 de agosto de 2010, que institui a Política Nacional de Resíduos Sólidos (PNRS), aplicada especificamente à logística reversa e desfazimento ambientalmente adequado dos equipamentos substituídos;
6.1.1.15. Portaria SGD/MGI nº 1.070, de 1º de junho de 2023, que estabelece o Modelo de Contratação de Serviços de Operação de Infraestrutura e Atendimento a Usuários de Tecnologia da Informação e Comunicação;
6.1.1.16. Padrões de Governo Eletrônico, especificamente os Padrões de Interoperabilidade (e-PING), o Modelo de Acessibilidade (e-MAG) e os Padrões Web (e-PWG) , que devem ser observados nas soluções de TIC do Poder Executivo;
6.1.1.17. Lei nº 12.527, de 18 de novembro de 2011, Lei de Acesso à Informação (LAI), em atendimento à garantia de transparência, tratamento e segurança das informações no âmbito dos serviços prestados;
6.1.1.18. Instrução Normativa GSI/PR nº 5, de 30 de agosto de 2021, que dispõe sobre os requisitos mínimos de segurança da informação para utilização de soluções de computação em nuvem.

6.1.1.19. Demais normas legais, regulamentares e orientações dos órgãos de controle aplicáveis à contratação, execução e fiscalização de soluções de TIC.

6.2. REQUISITOS MANUTENÇÃO E SUPORTE TÉCNICO

6.2.1. Considerando a criticidade da infraestrutura de balanceamento de carga e proteção de aplicações do CNPq, a solução de TIC a ser contratada deverá contemplar serviços de manutenção, atualização e suporte técnico especializados durante toda a vigência contratual.

6.2.2. Esses serviços deverão assegurar o funcionamento contínuo da solução implantada, bem como a atualização tecnológica e a correção de eventuais falhas identificadas durante sua operação.

6.2.3. Os serviços de manutenção e suporte técnico deverão ser prestados pela futura contratada e/ou pelo fabricante da solução, a partir da emissão do Termo de Recebimento Definitivo da solução implantada no ambiente tecnológico do CNPq.

6.2.4. Deverão ser contempladas, no mínimo, as seguintes requisitos:

6.2.4.1. disponibilização de atualizações de *software*, *firmware* e assinaturas de segurança, sempre que novas versões forem disponibilizadas pelo fabricante;

6.2.4.2. correção de falhas de *software* identificadas durante o período de vigência contratual, sem custos adicionais para o CNPq;

6.2.4.3. acesso à documentação técnica, base de conhecimento e demais recursos disponibilizados pelo fabricante;

6.2.4.4. disponibilização de canais oficiais de suporte técnico para abertura e acompanhamento de chamados;

6.2.4.5. execução de procedimentos necessários para restabelecimento do funcionamento normal da solução em caso de falhas ou incidentes;

6.2.4.6. disponibilização de atualizações tecnológicas necessárias para manter a solução aderente às boas práticas de segurança da informação e desempenho.

6.2.5. O suporte técnico deverá ser disponibilizado por meio de Central de Atendimento que permita a abertura e acompanhamento de chamados técnicos por meio de sistema web, correio eletrônico ou telefone.

6.2.6. O atendimento deverá estar disponível em regime 24 (vinte e quatro) horas por dia, 7 (sete) dias por semana, durante toda a vigência contratual.

6.2.7. Os atendimentos poderão ser realizados de forma remota ou presencial, conforme a natureza do incidente ou demanda técnica.

6.2.8. Quando necessário, poderá ser realizado atendimento presencial nas dependências do CNPq.

6.2.9. Os serviços de manutenção deverão contemplar, no mínimo, as seguintes modalidades:

6.2.9.1. Manutenção preventiva: A manutenção preventiva consiste na execução planejada de verificações periódicas do funcionamento da solução, com o objetivo de identificar possíveis falhas ou degradações de desempenho antes que causem indisponibilidade dos serviços. Essas atividades poderão incluir:

6.2.9.1.1. verificação da saúde da solução;

6.2.9.1.2. análise de desempenho e utilização de recursos;

6.2.9.1.3. revisão de configurações relevantes;

6.2.9.1.4. verificação de atualizações recomendadas pelo fabricante.

6.2.9.1.5. Quando aplicável, deverá ser emitido relatório técnico contendo as atividades realizadas e eventuais recomendações de melhoria.

6.2.9.2. Manutenção corretiva: A manutenção corretiva consiste na execução de procedimentos destinados a restabelecer o funcionamento normal da solução em caso de falhas, defeitos ou degradação de desempenho. Essas atividades poderão incluir:

6.2.9.2.1. diagnóstico de incidentes;

6.2.9.2.2. correção de falhas de *software*;

6.2.9.2.3. substituição de componentes defeituosos;

6.2.9.2.4. reinstalação ou reconfiguração de *softwares* e serviços.

6.2.9.2.2. Caso seja necessária substituição de componentes defeituosos, a contratada deverá providenciar a reposição por componentes equivalentes ou superiores, sem custos adicionais para o CNPq.

6.2.9.3. Manutenção evolutiva: A manutenção evolutiva consiste na disponibilização e implantação de novas versões de *software* ou *firmware* que venham a ser disponibilizadas pelo fabricante durante a vigência contratual. Essas atualizações poderão incluir:

6.2.9.3.1. melhorias de desempenho;

6.2.9.3.2. correções de segurança;

6.2.9.3.3. inclusão de novas funcionalidades;

6.2.9.3.4. adequações tecnológicas recomendadas pelo fabricante.

6.2.10. Os incidentes e solicitações de suporte técnico deverão ser registrados por meio de sistema de chamados, permitindo o acompanhamento de todas as etapas do atendimento.

6.2.10.1. Cada chamado deverá possuir identificação única e conter, no mínimo:

6.2.10.1.1. data e hora de abertura;

6.2.10.1.2. descrição do incidente ou solicitação;

6.2.10.1.3. nível de severidade;

6.2.10.1.4. registro das ações executadas;

6.2.10.1.5. data e hora de encerramento.

6.2.10.1.6. O chamado somente poderá ser considerado encerrado após validação da solução aplicada pelo responsável técnico do CNPq.

6.2.11. Os incidentes registrados deverão ser classificados conforme o nível de severidade, considerando o impacto causado ao ambiente tecnológico e às aplicações institucionais.

6.2.11.1. Os níveis de severidade deverão considerar, entre outros fatores:

6.2.11.1.1. indisponibilidade total da solução;

6.2.11.1.2. degradação significativa de desempenho;

6.2.11.1.3. falhas parciais ou intermitentes;

6.2.11.1.4. solicitações de configuração ou esclarecimentos técnicos.

6.2.12. Durante toda a vigência contratual, a contratada deverá disponibilizar relatórios periódicos contendo informações sobre os atendimentos realizados.

6.2.12.1. Esses relatórios deverão incluir, no mínimo:

6.2.12.1.1. quantidade de chamados registrados no período;

6.2.12.1.2. classificação por nível de severidade;

6.2.12.1.3. tempo médio de atendimento e resolução;

6.2.12.1.4. descrição dos incidentes e soluções aplicadas.

6.2.12.1.5. Os relatórios servirão como instrumento de acompanhamento dos níveis de serviço contratados e de avaliação da qualidade do suporte prestado.

6.2.13. A solução fornecida deverá contar com garantia e suporte técnico válidos no território nacional durante toda a vigência contratual.

6.2.13.1. A garantia deverá abranger tanto os componentes de *hardware* quanto os componentes de *software* que integram a solução.

6.2.13.2. Durante o período de garantia e suporte técnico deverão estar disponíveis, sem custos adicionais para o CNPq:

6.2.13.2.1. atualizações de *software* e *firmware*;

6.2.13.2.2. correções de segurança;

6.2.13.2.3. suporte técnico especializado;

6.2.13.2.4. substituição de componentes defeituosos, quando aplicável.

6.3. REQUISITOS TEMPORAIS

6.3.1. Os requisitos temporais da presente contratação estabelecem os prazos estimados para formalização contratual, implantação da solução e início da prestação dos serviços de suporte técnico, considerando a criticidade da infraestrutura de balanceamento de carga e segurança de aplicações do CNPq.

6.3.2. Após a assinatura do contrato, deverá ser realizada reunião inicial de alinhamento entre a equipe técnica do CNPq e a contratada, com o objetivo de apresentar o ambiente tecnológico do órgão, alinhar as etapas de implantação da solução, definir os responsáveis técnicos e estabelecer os procedimentos operacionais iniciais.

6.3.3. Essa reunião deverá ocorrer no prazo máximo de 10 (dez) dias corridos, contados da assinatura do contrato, observando as boas práticas de planejamento e gestão contratual previstas na Instrução Normativa SGD/ME nº 94/2022, que dispõe sobre o processo de contratação de soluções de tecnologia da informação e comunicação no âmbito da Administração Pública Federal.

6.3.4. O prazo máximo para execução das atividades relacionadas ao fornecimento, entrega e disponibilização dos equipamentos, licenças, garantias, subscrições, *softwares*, acessórios e demais recursos necessários à solução será de até 60 (sessenta) dias corridos, contados a partir da emissão da Ordem de Fornecimento de Bens (OFB) ou instrumento equivalente.

6.3.5. O prazo máximo para execução das atividades relacionadas à instalação, configuração, implantação, integração, testes, validação técnica e disponibilização da solução para entrada em operação será de até 60 (sessenta) dias corridos, contados a partir da emissão da Ordem de Serviço (OS).

6.3.6. Os prazos previstos nos itens 6.3.4 e 6.3.5 poderão ser prorrogados, uma única vez e por igual período, mediante justificativa formal da contratada e aprovação da Administração.

6.3.7. Após a conclusão da implantação da solução e a emissão do Termo de Recebimento Definitivo, terão início os serviços de garantia, manutenção e suporte técnico da solução.

6.3.8. O período de garantia e suporte técnico deverá ser de 60 (sessenta) meses, contados a partir da data de emissão do Termo de Recebimento Definitivo.

6.3.9. Após a implantação da solução, poderão ser executadas atividades de apoio técnico especializado destinadas à estabilização do ambiente, ajustes de configuração e otimização de desempenho.

6.3.10. Essas atividades poderão ocorrer durante todo o período contratual, conforme necessidade identificada pelo órgão.

6.3.11. O cronograma de execução deverá contemplar as principais etapas relacionadas à implantação da solução, incluindo planejamento, fornecimento dos equipamentos, instalação, configuração, testes e entrada em produção.

6.3.12. A tabela abaixo apresenta um cronograma indicativo das etapas previstas.

ETAPA	DESCRIÇÃO	PRAZO ESTIMADO
1	Assinatura do contrato	Contagem Inicial
2	Reunião inicial de alinhamento	até 10 dias corridos após assinatura do contrato
3	Fornecimento dos equipamentos, licenças, garantias e subscrições.	conforme planejamento da implantação
4	Instalação e configuração da solução	durante o período de implantação
5	Testes e validação técnica	antes da entrada em produção
6	Emissão do Termo de Recebimento Definitivo	após validação da solução
7	Início dos serviços de garantia e suporte técnico	após recebimento definitivo

6.3.12. Os prazos estabelecidos buscam assegurar a implantação adequada da solução sem comprometer a continuidade dos serviços institucionais atualmente suportados pela infraestrutura de balanceamento de carga do CNPq.

6.3.13. A definição desses prazos considera a complexidade da solução a ser implantada, a necessidade de integração com o ambiente tecnológico existente e a criticidade das aplicações institucionais suportadas pela plataforma.

6.4. REQUISITOS DE SEGURANÇA DA INFORMAÇÃO E PRIVACIDADE

6.4.1. A solução a ser contratada deverá observar integralmente as diretrizes, normas e políticas de segurança da informação adotadas pelo Conselho Nacional de Desenvolvimento Científico e Tecnológico - CNPq, bem como a legislação vigente aplicável à proteção de dados e segurança da informação.

6.4.2. A solução e os serviços associados deverão observar as diretrizes estabelecidas na Política de Segurança da Informação e Comunicações do CNPq (POSIC), bem como a legislação aplicável à proteção de dados pessoais e segurança da informação, especialmente a Lei nº 13.709/2018 (Lei Geral de Proteção de Dados Pessoais – LGPD), além das normas e boas práticas aplicáveis à Administração Pública Federal.

6.4.3. A contratada deverá manter absoluto sigilo sobre todas as informações, dados, configurações, documentos e comunicações a que tiver acesso em razão da execução contratual. Tais informações não poderão ser divulgadas, reproduzidas ou utilizadas para finalidade diversa da execução do objeto contratado, salvo mediante autorização formal do CNPq.

6.4.4. A obrigação de confidencialidade deverá ser estendida a todos os empregados, prepostos e eventuais subcontratados envolvidos na execução do contrato e permanecerá vigente mesmo após o término ou rescisão da contratação.

6.4.4.1. Todos os profissionais designados pela Contratada deverão assinar Termo de Responsabilidade e Confidencialidade, previamente ao início das atividades, a ser fornecido pela Contratante.

6.4.5. A contratada deverá observar integralmente o disposto na Lei nº 13.709/2018 (Lei Geral de Proteção de Dados Pessoais – LGPD), adotando medidas técnicas e administrativas adequadas para proteger dados pessoais eventualmente acessados durante a execução contratual. Essas medidas deverão ser suficientes para prevenir acessos não autorizados, perda acidental ou ilícita, destruição, alteração, comunicação ou qualquer forma de tratamento inadequado ou ilícito de dados pessoais.

6.4.6. A contratada deverá adotar controles adequados de acesso físico e lógico aos recursos tecnológicos do CNPq sob sua responsabilidade, garantindo que o acesso aos sistemas, equipamentos e informações institucionais seja restrito exclusivamente às atividades necessárias à execução do contrato.

6.4.7. Os acessos concedidos deverão permanecer sob controle do CNPq e poderão ser alterados, suspensos ou revogados a qualquer tempo.

6.4.8. Ao término do contrato, ou quando solicitado pela contratante, todos os perfis de acesso, contas e credenciais concedidos deverão ser imediatamente revogados.

6.4.9. A contratada deverá informar ao CNPq todas as credenciais administrativas eventualmente criadas ou utilizadas durante a execução contratual.

6.4.10. As senhas e demais credenciais poderão ser alteradas pela contratante a qualquer momento, especialmente ao término do contrato ou quando identificado risco à segurança da informação.

6.4.11. Os recursos de tecnologia da informação disponibilizados pelo CNPq para execução das atividades contratuais deverão ser utilizados exclusivamente para os fins relacionados à execução do objeto contratado, sendo vedada sua utilização para quaisquer outras finalidades que não estejam diretamente relacionadas às atividades previstas no contrato.

6.4.12. A contratada poderá manter registros técnicos estritamente necessários à execução contratual, desde que tais registros sejam armazenados em ambiente seguro e controlado e utilizados exclusivamente para fins relacionados ao contrato. Esses registros deverão ser protegidos contra acesso não autorizado e, ao término da contratação, deverão ser eliminados ou transferidos ao CNPq, quando aplicável.

6.4.13. A contratada deverá assegurar que a solução permaneça atualizada com versões oficialmente suportadas pelo fabricante, incluindo atualizações de software, correções de vulnerabilidades e demais melhorias de segurança disponibilizadas durante a vigência contratual.

6.4.14. Todos os documentos, relatórios técnicos, configurações e procedimentos produzidos no âmbito da contratação serão considerados propriedade do CNPq.

6.5. REQUISITOS SOCIAIS, AMBIENTAIS E CULTURAIS

6.5.1. Os serviços devem estar aderentes às seguintes diretrizes sociais, ambientais e culturais:

6.5.1.1. Requisitos Sociais:

6.5.1.1.1. Todos os profissionais da Contratada que desempenharão as atividades em contato direto (físico ou virtual) com a Contratante deverão cumprir os seguintes requisitos:

6.5.1.1.2. Apresentar-se vestidos de forma adequada ao ambiente de trabalho físico ou virtual, evitando-se o vestuário que caracterize o comprometimento da boa imagem institucional da Contratante.

6.5.1.1.3. Respeitar todos os servidores, funcionários e colaboradores, em qualquer posição hierárquica, preservando a comunicação e o relacionamento interpessoal construtivo.

6.5.1.1.4. Quando da execução de tarefas no ambiente do CNPq os funcionários da contratada deverão observar, no trato com os servidores e o público em geral, a urbanidade e os bons costumes de comportamento, tais como: asseio, pontualidade, cooperação, respeito mútuo, discrição e zelo com o patrimônio público. Deverão ainda portar identificação pessoal, conforme as normas internas da Instituição.

6.5.1.1.5. A execução contratual deverá observar, no que couber, as diretrizes estabelecidas pelo Decreto nº 12.122, de 30 de julho de 2024, que institui o Programa Federal de Prevenção e Enfrentamento do Assédio e da Discriminação, devendo a contratada promover ambiente de trabalho pautado pelo respeito, ética, integridade, urbanidade e não discriminação no relacionamento com servidores, colaboradores, terceirizados e demais usuários envolvidos na execução contratual.

6.5.1.2. Requisitos Ambientais:

6.5.1.2.1. A contratada deverá seguir, no que couber, os requisitos definidos no Guia Nacional de Contratações Sustentáveis da Advocacia Geral da União (AGU) — 8ª Edição, Outubro/2025, disponível em: https://www.gov.br/agu/pt-br/assuntos-1/agu-na-cop30/central-de-conteudos/edicao_2025_do_guia_final_para_cop30.pdf/

6.5.1.2.2. Igualmente, a contratada deverá adotar práticas de sustentabilidade ambiental na execução do objeto, no que couber, conforme disposto na Instrução Normativa SLTI/MP nº 01/2010, que dispõe sobre os critérios de sustentabilidade ambiental na aquisição de bens, contratação de serviços ou obras pela Administração Pública Federal direta, autárquica e fundacional e dá outras providências.

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

6.5.1.2.4. As soluções deverão observar práticas de eficiência operacional e uso racional dos recursos computacionais e energéticos, buscando maximizar desempenho, disponibilidade e capacidade de processamento com o menor impacto possível sobre a infraestrutura tecnológica da Contratante.

6.5.1.2.5. As configurações de hardware e software deverão ser realizadas visando alto desempenho com a utilização racional de energia, evitando-se a sobrecarga de equipamentos ou dispositivos elétricos e eletrônicos.

6.5.1.2.6. Fornecer aos empregados os equipamentos de segurança que se fizerem necessários, para a execução de serviços.

6.5.1.2.7. Respeitar as Normas Brasileiras – NBR publicadas pela Associação Brasileira de Normas Técnicas sobre resíduos sólidos.

6.5.1.2.8. Que os bens devam ser, preferencialmente, acondicionados em embalagem individual adequado, com menor volume possível, que utilize materiais recicláveis, de forma a garantir a máxima proteção durante o transporte e o armazenamento.

6.5.1.2.9. Que os bens não contenham substâncias perigosas em concentração acima da recomendada na diretiva RoHS (*Restriction of Certain Hazardous Substances*), tais como mercúrio (Hg), chumbo (Pb), cromo hexavalente (Cr(VI)), cádmio (Cd), bifenil-polibromados (PBBs), éteres difenil-polibromados (PBDEs).

6.5.1.2.10. Deverá entregar os documentos solicitados na forma digital, com vistas a evitar ou reduzir o uso de papel e impressão, em atendimento ao Art. 9º da Política de Nacional de Resíduos Sólidos (Lei n.º 12.305/ 2010).

6.5.1.2.11. Considerando que a presente contratação poderá contemplar o fornecimento de equipamentos, componentes, acessórios ou outros ativos tecnológicos, deverão ser observadas práticas relacionadas à gestão ambiental durante todo o ciclo de vida dos bens, incluindo reutilização, logística reversa, reciclagem, desfazimento e descarte ambientalmente adequado de equipamentos, componentes e resíduos eletroeletrônicos eventualmente gerados.

6.5.1.2.12. Deverá ser observado planejamento para destinação ambientalmente adequada dos ativos atualmente instalados que venham a ser substituídos, descontinuados ou impactados pela solução objeto da contratação.

6.5.1.2.13. Considerando a eventual substituição ou descontinuidade dos equipamentos atualmente instalados no ambiente do CNPq, após a migração e validação da nova solução, os ativos desativados deverão ser submetidos às seguintes etapas, quando aplicável:

6.5.1.2.13.1. desligamento controlado e retirada do ambiente produtivo;

6.5.1.2.13.2. inventário e avaliação patrimonial dos ativos;

6.5.1.2.13.3. sanitização segura das informações eventualmente armazenadas, incluindo arquivos de configuração, credenciais, certificados digitais, chaves criptográficas, logs e demais dados operacionais;

6.5.1.2.13.4. definição da destinação administrativa aplicável, podendo contemplar remanejamento interno, reaproveitamento, desfazimento, logística reversa, reciclagem ou descarte ambientalmente adequado;

6.5.1.2.13.5. observância da legislação aplicável ao gerenciamento de resíduos eletroeletrônicos e das normas internas do CNPq relativas ao desfazimento patrimonial.

6.5.1.2.14. Previamente ao desfazimento, remanejamento, descarte ou destinação dos ativos substituídos, deverá ser realizada sanitização segura das informações eventualmente armazenadas, visando impedir recuperação indevida ou vazamento de informações institucionais.

6.5.1.3. Requisitos Culturais:

6.5.1.3.1. Toda a documentação produzida e/ou fornecida pela contratada referente ao objeto deverá estar preferencialmente no idioma Português - BR, de forma clara e objetiva.

6.6. REQUISITOS DE ARQUITETURA TECNOLÓGICA

6.6.2. Todos os equipamentos fornecidos deverão ser novos, de primeiro uso, estar em linha de produção do fabricante e disponíveis comercialmente no mercado. Não serão aceitas funcionalidades previstas apenas em *roadmap* ou em estágio experimental (beta).

6.6.3. A solução deverá ser composta por plataforma especializada de balanceamento de aplicações, baseada em instâncias, nós ou componentes dedicados, não sendo aceitas soluções baseadas em servidores de uso geral, estações de trabalho ou equipamentos genéricos adaptados para execução das funções de balanceamento de carga e segurança de aplicações.

6.6.4. Toda a solução deverá ser fornecida por um único fabricante, incluindo *hardware* e *software*, garantindo total integração entre os componentes da plataforma. Tal exigência visa assegurar a plena interoperabilidade entre os componentes da solução, reduzir a complexidade de integração e mitigar riscos operacionais associados à gestão de múltiplos fabricantes em ambiente de missão crítica.

6.6.5. A arquitetura da solução deverá permitir operação em *cluster* de alta disponibilidade, garantindo continuidade dos serviços em caso de falha de um dos equipamentos e permitindo sincronização de configurações entre as instâncias, nós ou componentes.

6.6.6. A contratada deverá fornecer todos os recursos necessários para a implantação da solução, incluindo equipamentos, licenciamento, *softwares*, subscrições, garantia, acessórios, cabeamentos e demais componentes necessários ao pleno funcionamento da solução no ambiente tecnológico do CNPq.

6.6.7. Nenhum dos componentes da solução poderá possuir anúncio de *End of Sale (EoS) ou End of Life (EoL)* no momento do aceite definitivo da solução. Caso tal situação seja identificada, o fornecedor deverá substituir o equipamento por modelo equivalente ou superior, sem custos adicionais para o CNPq.

6.6.8. Caso, durante a vigência contratual, qualquer componente da solução venha a ser descontinuado pelo fabricante ou tenha anúncio de *End of Sale (EoSale), End of Support (EoSup), End of Life (EoL)* ou condição equivalente que comprometa a continuidade do suporte técnico, garantia, atualizações, disponibilidade de peças de reposição ou manutenção da solução, a CONTRATADA deverá providenciar, sem ônus adicional para o CNPq, a substituição por outro componente novo e de primeiro uso, com características técnicas iguais ou superiores, plenamente compatível com a arquitetura da solução e que possua suporte técnico oficial vigente do fabricante durante todo o período remanescente da contratação.

6.6.9. Todos os componentes da solução deverão ser fornecidos com as licenças necessárias para seu pleno funcionamento, incluindo as funcionalidades requeridas para operação da plataforma de balanceamento de carga e segurança de aplicações.

6.6.10. As licenças fornecidas deverão permitir que a solução permaneça plenamente operacional após o término do período de vigência da garantia e das subscrições contratadas, assegurando a continuidade do funcionamento da plataforma, ainda que sem direito a novas atualizações de *software*, suporte técnico do fabricante, assinaturas de segurança ou demais benefícios associados às subscrições expiradas.

6.6.11. As instâncias, nós ou componentes que compõem a solução deverão possuir fontes de alimentação redundantes e *hot-swappable* , compatíveis com a infraestrutura elétrica do data center do CNPq.

6.6.12. Os equipamentos deverão ser compatíveis com racks padrão de 19 polegadas, devendo ser fornecidos com todos os acessórios necessários para sua instalação física.

6.6.13. Os equipamentos fornecidos deverão possuir certificações de homologação aplicáveis no Brasil, emitidas por órgãos competentes, quando exigido pela legislação.

6.6.14. Durante a implantação da solução, a contratada deverá realizar as atividades necessárias para sua entrada em operação, incluindo instalação de *software*, configuração inicial, integração com o ambiente existente, migração de configurações quando aplicável e execução de testes de funcionamento.

6.6.15. A definição dos requisitos arquiteturais da solução busca assegurar a padronização tecnológica do ambiente de entrega de aplicações do CNPq, de forma a garantir interoperabilidade entre os componentes da infraestrutura, simplificação da administração da plataforma e redução da complexidade operacional. Em ambientes de missão crítica, a adoção de soluções integradas e baseadas em plataformas especializadas contribui para a redução de riscos associados à operação, manutenção e evolução tecnológica do ambiente.

6.6.16. Nesse contexto, a definição de requisitos arquiteturais baseados em instâncias, nós ou componentes dedicados e plataformas integradas visa assegurar maior estabilidade operacional, maior previsibilidade na gestão da infraestrutura e melhor aproveitamento do conhecimento técnico acumulado pela equipe responsável pela operação do ambiente tecnológico do órgão.

6.7. REQUISITOS DE PROJETO E DE IMPLEMENTAÇÃO

6.7.1. A implementação da solução deverá contemplar todas as atividades necessárias para que a plataforma de balanceamento de aplicações e *firewall* de aplicações web seja plenamente operacional no ambiente tecnológico do CNPq.

6.7.2. Durante a fase de implantação, a contratada deverá elaborar e apresentar projeto executivo de implantação, contendo o detalhamento das etapas de implementação da solução, cronograma de execução e descrição das atividades técnicas necessárias para a plena operacionalização do ambiente.

6.7.3. O Projeto Executivo deverá ser submetido à análise e aprovação da equipe técnica do CNPq antes do início das atividades de implantação.

6.7.4. O Projeto Executivo deverá contemplar, no mínimo:

6.7.4.1. levantamento da infraestrutura tecnológica relacionada à solução, incluindo equipamentos, *softwares*, licenças, conectividade e demais componentes envolvidos;

6.7.4.2. definição do escopo da solução a ser implantada e dos componentes que a integram;

6.7.4.3. identificação dos ativos que compõem a arquitetura da solução, incluindo interconexões físicas e lógicas, interfaces de rede e integrações necessárias;

6.7.4.4. definição dos parâmetros de configuração da solução, incluindo endereçamento IP, segmentação de rede, políticas de balanceamento de carga, políticas de segurança, parâmetros de roteamento e demais elementos necessários ao funcionamento da plataforma;

6.7.4.5. elaboração da arquitetura lógica da solução, com representação da topologia proposta e das integrações com a infraestrutura existente;

6.7.4.6. elaboração da arquitetura física da solução, incluindo o mapeamento das conexões físicas necessárias entre os equipamentos da solução e os dispositivos de rede do ambiente do CNPq;

6.7.4.7. definição de procedimentos de contingência e plano de *rollback*, descrevendo as ações necessárias para restabelecimento do ambiente em caso de falhas durante o processo de implantação.

6.7.4.8. elaboração e execução de plano de migração das configurações existentes, incluindo políticas de balanceamento, certificados digitais, regras de publicação, mecanismos de segurança, *iRules* ou funcionalidades equivalentes, assegurando sua correta implementação na nova solução.

6.7.5. A instalação e configuração da solução deverão ser planejadas e executadas de forma a assegurar a interoperabilidade com a infraestrutura tecnológica existente no CNPq, evitando impactos nos serviços em produção.

6.7.6. Durante a execução das atividades de implantação, a contratada deverá atuar sob supervisão da equipe técnica do CNPq, garantindo que as mudanças no ambiente sejam realizadas de forma controlada e documentada.

6.7.7. Caso sejam identificadas necessidades de ajustes no projeto durante a execução das atividades de implantação, a contratada deverá submeter as alterações propostas à avaliação e aprovação do fiscal técnico do contrato antes de sua implementação.

6.8. REQUISITOS DE IMPLANTAÇÃO

6.8.1. A contratada será responsável pela execução integral das atividades necessárias para implantação da solução de balanceamento de aplicações e *firewall* de aplicações web no ambiente tecnológico do CNPq.

6.8.2. A implantação deverá contemplar todas as etapas necessárias para que a solução seja plenamente operacional, incluindo o fornecimento dos equipamentos, licenças, garantias, subscrições, instalação física, configuração lógica, integração com a infraestrutura existente, realização de testes e entrada em produção.

6.8.3. Compete à contratada, no mínimo:

6.8.3.1. responsabilizar-se pela completa implantação da solução, incluindo todos os custos necessários à operacionalização dos equipamentos e *softwares* fornecidos;

6.8.3.2. disponibilizar todos os instrumentos, ferramentas e recursos técnicos necessários para execução das atividades de instalação, configuração e testes da solução;

6.8.3.3. realizar a entrega dos equipamentos e demais componentes da solução nos locais de instalação definidos pelo CNPq, responsabilizando-se pelas atividades de transporte, embalagem, desembalagem e demais procedimentos logísticos necessários;

6.8.3.4. realizar a instalação física e lógica dos equipamentos e componentes da solução, de acordo com o Projeto Executivo previamente aprovado;

6.8.3.5. executar as atividades necessárias de configuração e adequação dos equipamentos, *softwares*, licenças e componentes fornecidos, garantindo sua correta integração com o ambiente tecnológico do CNPq;

6.8.3.6. realizar a migração controlada das configurações e serviços existentes para a nova solução, incluindo políticas de balanceamento, regras de segurança, certificados digitais e demais parâmetros necessários ao funcionamento do ambiente;

6.8.3.7. planejar e executar as atividades de integração da solução com a infraestrutura de rede existente, de modo a evitar impactos nos serviços em produção;

6.8.3.8. elaborar e apresentar Plano de Homologação e Testes, contendo a descrição dos procedimentos e critérios de validação da solução implantada;

6.8.3.9. executar os testes funcionais e operacionais previstos no Plano de Homologação e Testes, de forma a verificar o correto funcionamento de todos os componentes de *hardware* e *software* envolvidos;

6.8.3.10. elaborar e entregar a documentação técnica final da solução implantada, incluindo registros de configuração, arquitetura implementada e demais informações necessárias para operação e manutenção do ambiente.

6.8.4. Durante a implantação da solução poderão ser executadas atividades como instalação de *softwares*, migração de regras e políticas de segurança, elaboração e execução de scripts, ajustes de configuração, análise de desempenho, otimização de parâmetros de funcionamento e resolução de eventuais incidentes técnicos.

6.8.5. Quando necessário, determinadas atividades poderão ser executadas em janelas de manutenção previamente acordadas com o CNPq, inclusive em horários noturnos ou fins de semana, de forma a minimizar impactos nos serviços institucionais.

6.8.6. Compete ao CNPq acompanhar as atividades de implantação, fornecer informações necessárias sobre a infraestrutura existente e definir, quando necessário, as janelas de intervenção para execução das atividades técnicas.

6.8.7. Ao término das atividades de implantação deverá ser realizado processo formal de validação da solução implantada, com verificação do atendimento aos requisitos técnicos definidos.

6.9. REQUISITOS DE GARANTIA

6.9.1. A solução fornecida deverá possuir garantia técnica integral do fabricante, pelo período mínimo de 60 (sessenta) meses, contados a partir da emissão do Termo de Recebimento Definitivo da solução implantada no ambiente tecnológico do CNPq.

6.9.2. O prazo de garantia estabelecido considera a natureza da solução a ser contratada, composta por ativos de rede, segurança e entrega de aplicações de missão crítica, cuja vida útil estimada é de, no mínimo, 5 (cinco) anos, sendo a contratação da garantia durante todo esse período medida tecnicamente adequada e economicamente mais vantajosa para a Administração.

6.9.3. A garantia deverá abranger todos os componentes da solução fornecida, incluindo, no mínimo:

6.9.3.1. *hardware*;

6.9.3.2. *software*;

6.9.3.3. licenças;

6.9.3.4. módulos e funcionalidades contratadas;

6.9.3.5. *firmwares*;

6.9.3.6. assinaturas, bases de proteção e demais mecanismos associados à segurança da solução, quando aplicável.

6.9.4. Durante o período de garantia deverão estar contemplados, sem ônus adicional para o CNPq:

6.9.4.1. correção de falhas e defeitos de *hardware* e *software*;

6.9.4.2. atualização de versões do sistema operacional da plataforma;

6.9.4.3. atualização de módulos de *software* e funcionalidades da solução;

6.9.4.4. atualização de *firmwares* e componentes embarcados;

6.9.4.5. disponibilização de correções de segurança, patches e *hotfixes* publicados pelo fabricante;

6.9.4.6. atualização de assinaturas, mecanismos de proteção e demais recursos de segurança associados às funcionalidades contratadas, quando aplicável;

6.9.4.7. direito ao recebimento e utilização de novas versões, correções, melhorias e evoluções disponibilizadas pelo fabricante para a solução fornecida.

6.9.5. A garantia técnica deverá assegurar a plena operacionalidade da solução em todas as funcionalidades contratadas, abrangendo tanto aquelas descritas nas especificações do objeto quanto as previstas nos manuais, catálogos e demais documentos técnicos oficiais do fabricante.

6.9.6. A garantia deverá cobrir a resolução de falhas, erros, defeitos, instabilidades, vulnerabilidades, degradação de desempenho ou quaisquer ocorrências que venham a afetar os componentes físicos ou lógicos da solução fornecida.

6.9.7. Sempre que necessário, a garantia deverá incluir a substituição total ou parcial de equipamentos, módulos, licenças ou componentes que apresentem defeito ou falha de funcionamento, sem ônus adicional para o CNPq.

6.9.8. Os equipamentos, peças, módulos ou componentes substituídos deverão ser novos, originais, de primeiro uso e possuir características técnicas equivalentes ou superiores às dos itens substituídos.

6.9.9. Os componentes substituídos durante o período de garantia deverão manter, no mínimo, o mesmo prazo de garantia originalmente contratado, observando-se a solução como um todo e suas funcionalidades associadas.

6.9.10. A contratada deverá assegurar que a solução permaneça plenamente suportada pelo fabricante durante todo o período de garantia, incluindo a disponibilidade de peças de reposição, atualizações, correções de software e demais recursos necessários à manutenção da solução em operação.

6.9.11. As atualizações, correções e novas versões disponibilizadas pelo fabricante deverão ser instaladas pela contratada sempre que necessário, mediante planejamento conjunto com a equipe técnica do CNPq, de forma a preservar a estabilidade do ambiente e minimizar impactos aos serviços em produção.

6.9.12. A garantia deverá ser prestada pelo fabricante, permanecendo, em qualquer hipótese, a contratada integralmente responsável pelo cumprimento das condições estabelecidas no contrato.

6.9.13. Correrão por conta exclusiva da contratada todas as despesas relacionadas ao deslocamento de pessoal técnico, transporte, retirada, entrega, frete, reposição, substituição e demais providências necessárias à execução dos serviços de garantia.

6.9.14. Os componentes eventualmente removidos ou substituídos durante atividades de manutenção não ficarão sob responsabilidade do CNPq, cabendo à contratada providenciar sua retirada e destinação final ambientalmente adequada, em conformidade com a legislação aplicável, especialmente a Lei nº 12.305/2010, que institui a Política Nacional de Resíduos Sólidos.

6.9.14.1. Quando aplicável, deverão ser observadas práticas de reutilização, reaproveitamento, logística reversa, reciclagem e descarte ambientalmente adequado dos equipamentos, peças, componentes e resíduos eletroeletrônicos decorrentes das atividades de garantia e substituição da solução.

6.9.14.2. Os ativos eventualmente substituídos ou descontinuados em decorrência da contratação deverão observar procedimento de desligamento controlado, sanitização segura das informações eventualmente armazenadas e destinação final ambientalmente adequada, observadas o art. 18, §1º, inciso XII da Lei nº 14.133/2021, normas internas do CNPq e legislações aplicáveis.

6.9.15. Caso, durante a vigência contratual, qualquer componente da solução venha a ser descontinuado pelo fabricante ou deixe de possuir suporte técnico oficial *(End of Support - EoS ou End of Life - EoL)*, a Contratada deverá providenciar, sem ônus adicional para o CNPq, a substituição por outro componente novo, de primeiro uso, com características técnicas iguais ou superiores, plenamente compatível com a arquitetura da solução e com suporte vigente durante todo o período remanescente do contrato.

6.9.16. A substituição deverá garantir a continuidade da operação da solução, sem prejuízo às funcionalidades existentes, níveis de desempenho, integração com o ambiente atual e políticas de segurança previamente estabelecidas.

6.9.17. O detalhamento dos procedimentos, prazos, níveis de atendimento e demais condições relativas à garantia, suporte e assistência técnica será estabelecido no Termo de Referência e em seus anexos.

6.10. REQUISITOS DE EXPERIÊNCIA PROFISSIONAL

6.10.1. Considerando a criticidade da solução de balanceamento de aplicações e *firewall* de aplicações web para a continuidade dos serviços institucionais do CNPq, torna-se necessário que a empresa contratada possua experiência comprovada na implantação de soluções de natureza e complexidade compatíveis com o objeto da contratação.

6.10.2. Para fins de qualificação técnica, deverá ser exigida da licitante a comprovação de aptidão para execução de serviços similares ao objeto da contratação, mediante apresentação de atestado(s) de capacidade técnica emitido(s) por pessoa jurídica de direito público ou privado.

6.10.3. Os atestados deverão comprovar que a licitante possui experiência na implantação de solução de balanceamento de carga de aplicações, incluindo fornecimento, instalação, configuração ou suporte técnico associado.

6.10.4. Para fins de comprovação da capacidade técnico-operacional, poderá ser exigida a apresentação de, no mínimo, 1 (um) atestado de capacidade técnica que demonstre a execução de contrato compatível em características com o objeto desta contratação.

6.10.5. Os atestados apresentados deverão conter informações que permitam a verificação da experiência da licitante, incluindo, sempre que possível:

6.10.5.1. identificação da entidade contratante;

6.10.5.2. descrição do objeto contratado;

6.10.5.3. período de execução do contrato;

6.10.5.4. avaliação quanto à qualidade ou regularidade dos serviços prestados.

6.10.6. Poderá ser admitida a apresentação de mais de um atestado de capacidade técnica para fins de comprovação da experiência exigida, desde que os serviços descritos sejam compatíveis com o objeto da contratação.

6.10.7. A Administração poderá realizar diligências para verificar a veracidade das informações constantes nos atestados apresentados, nos termos da legislação vigente.

6.10.8. A definição detalhada dos critérios de habilitação técnica e dos requisitos formais para apresentação dos atestados será estabelecida no Termo de Referência e no edital da licitação, em conformidade com a Lei nº 14.133/2021.

6.11. REQUISITOS DE FORMAÇÃO DA EQUIPE

6.11.1. Considerando a natureza e a complexidade técnica da solução, a contratada deverá dispor de equipe técnica em quantidade e qualificação suficientes para execução integral das atividades previstas no objeto da contratação.

6.11.2. O dimensionamento da equipe técnica necessária à execução do objeto será de responsabilidade exclusiva da contratada, devendo ser compatível com o escopo contratado e suficiente para assegurar o cumprimento integral dos requisitos, prazos, níveis de serviço e demais obrigações estabelecidas no Termo de Referência.

6.11.3. Caberá à contratada definir a composição, quantidade e distribuição dos profissionais necessários à execução das atividades de fornecimento, instalação, configuração, implantação, migração, suporte técnico, garantia e demais serviços associados à solução.

6.11.4. A equipe disponibilizada deverá possuir capacitação técnica compatível com as atividades executadas, observadas as tecnologias, níveis de criticidade e requisitos operacionais envolvidos na contratação.

6.12. REQUISITOS DE METODOLOGIA DE TRABALHO

6.12.1. A execução dos serviços estará condicionada ao recebimento, pela contratada, de Ordem de Serviço (OS) / Ordem de Fornecimento de Bens (OFB) emitida pela contratante.

6.12.2. A Ordem de Serviço/ Ordem de Fornecimento de Bens indicará o tipo de serviço a ser executado, a quantidade, o local de execução e demais informações necessárias para a realização das atividades.

6.12.3. A contratada deverá disponibilizar meios adequados para abertura e acompanhamento de chamados técnicos e registro de ocorrências, preferencialmente por meio eletrônico e atendimento telefônico.

6.12.4. A execução dos serviços deverá ser acompanhada pela contratada, que deverá comunicar à contratante quaisquer ocorrências que possam impactar a execução das atividades ou a disponibilidade da solução.

6.12.5. A metodologia de trabalho adotada deverá observar o princípio da delegação de responsabilidades, cabendo à contratante a gestão e fiscalização do contrato e à contratada a execução dos serviços e a gestão de seus recursos técnicos.

6.12.6. A contratada deverá executar os serviços em conformidade com as boas práticas de mercado, recomendações do fabricante da solução e diretrizes técnicas estabelecidas pelo CNPq para o ambiente de infraestrutura do Data Center.

6.12.7. Sempre que aplicável, a contratada deverá registrar e documentar as atividades realizadas, incluindo atendimentos de suporte técnico, manutenções, atualizações de software, substituição de componentes e demais intervenções efetuadas no ambiente.

6.12.8. A contratada deverá indicar formalmente um preposto responsável pela interlocução com a contratante e pelo acompanhamento da execução contratual.

6.12.9. Os serviços prestados estarão sujeitos à avaliação técnica da contratante, considerando o atendimento aos requisitos técnicos, aos níveis de serviço estabelecidos e às condições previstas no contrato.

7. Estimativa da demanda - quantidade de bens e serviços

7.1. SITUAÇÃO ATUAL DO AMBIENTE DO CNPq

7.1.1. O ambiente atual de balanceamento de carga e entrega de aplicações do Conselho Nacional de Desenvolvimento Científico e Tecnológico - CNPq é composto por equipamentos modulares *F5 BIG-IP VIPRION*, operando em arquitetura de *cluster*. O sistema encontra-se na versão *BIG-IP 10.2.4 Build 864.0 Hotfix HF11*, configurado com 16 CPUs ativas.

7.1.2. A solução atualmente em operação é composta por dois *appliances* dedicados de *Application Delivery Controller (ADC)*, atualmente representados pela plataforma *F5 BIG-IP VIPRION C2400*, responsáveis pelo balanceamento de carga, entrega e proteção das aplicações institucionais.

7.1.3. A Tabela abaixo apresenta os principais componentes que integram a arquitetura tecnológica atualmente utilizada.

QUANTIDADE	COMPONENTE	FINALIDADE PRINCIPAL
2	Chassis VIPRION C2400	Infraestrutura modular para blades de processamento
2	Blades de processamento	Execução de serviços de balanceamento de carga e WAF
2	Licenças de software BIG-IP	Recursos de ADC, WAF, SSL Offloading e segurança
2	Módulos de rede	Interfaces de alta performance (10GbE/40GbE)
2	Fontes redundantes	Garantia de operação contínua

7.2. LICENCIAMENTO E MÓDULOS ATIVOS

7.2.1. Os equipamentos utilizam licenças *Perpetual (Production)*, datadas de 08 de dezembro de 2011, com os seguintes módulos habilitados:

7.2.1.1. ***LTM (Local Traffic Manager) – Base C2400***

- *IPv6 Gateway*
- *Rate Shaping*
- *Compressão (50 Mbps)*
- *RAM Cache*
- *SSL (500 TPS por núcleo)*
- *Cluster Multi-Processing*

7.2.1.2. ***ASM (Application Security Manager) – Licença Unlimited (VIPRION)***

7.2.1.3. APM (Access Policy Manager) – Licença Limited (VIPRION), incluindo:

- *App Tunnel*
- *Endpoint Security Checks*
- *Protected Workspace*
- *Secure Virtual Keyboard*
- *Remote Desktop / App Tunnel*

7.2.2. Verifica-se, contudo, que nem todos os módulos licenciados encontram-se efetivamente provisionados no ambiente atual, sendo a utilização concentrada predominantemente nos módulos LTM e ASM.

7.3. LIMITAÇÕES DO AMBIENTE ATUAL

7.3.1. Embora os equipamentos ainda cumpram parcialmente seu propósito original, o ambiente apresenta limitações relevantes decorrentes do tempo de uso e da obsolescência tecnológica, destacando-se:

7.3.1.1. Obsolescência de hardware: os componentes físicos não possuem mais reposição garantida por contrato vigente, dificultando ou inviabilizando a manutenção corretiva em caso de falhas.

7.3.1.2. Fim do suporte de software: a versão do sistema operacional *BIG-IP* em uso encontra-se fora do ciclo de suporte do fabricante, impedindo a aplicação de correções de segurança e atualizações.

7.3.1.3. Exposição a ameaças cibernéticas: a ausência de atualizações regulares amplia o risco de exploração de vulnerabilidades conhecidas, especialmente no contexto de proteção de aplicações web e APIs.

7.3.1.4. Limitações de escalabilidade e modernização: a arquitetura atual não está preparada para ambientes *cloud-native*, integração com pipelines *DevOps* ou uso de microserviços, dificultando a evolução tecnológica do CNPq.

7.3.1.5. Custo de oportunidade: a manutenção de uma infraestrutura legada pode resultar em custos operacionais elevados quando comparada a soluções modernas mais eficientes e com menor complexidade de gestão.

7.3.1.6. Incompatibilidade criptográfica: a versão atual suporta apenas TLS 1.0, protocolo obsoleto e inseguro. Sistemas institucionais como o *Keycloak* exigem, no mínimo, TLS 1.2, o que compromete a autenticação segura, a rastreabilidade de acessos e a conformidade com boas práticas de segurança da informação.

7.4. CICLO DE VIDA E SUPORTE DO FABRICANTE

7.4.1. Componentes que atingem o fim de seu ciclo de vida (*End of Life - EoL*) passam a ser considerados obsoletos, deixando de receber suporte técnico, atualizações de *software*, correções de segurança e reposição de peças pelo fabricante.

7.4.2. O fabricante anunciou o fim do suporte para a versão do sistema operacional BIG-IP atualmente utilizada pelo CNPq (versão 10.2.4), encerrado em 31 de dezembro de 2016, conforme apresentado na Tabela 07.

VERSÃO DO SOFTWARE	FIM DO DESENVOLVIMENTO	FIM DO SUPORTE TÉCNICO
10.2.1 10.2.2 10.2.3 10.2.4	December 31, 2015 (31/12/2015)	December 31, 2016 (31/12/2016)

7.4.3. Ainda que fosse excepcionalmente considerada a atualização do *software*, a plataforma de *hardware* atingiu, em abril de 2026, o limite de suporte para atualizações de *software* pelo fabricante, não sendo mais elegível para novas versões ou correções evolutivas, conforme demonstrado na Tabela 08.

SKU	DESCRIÇÃO	END OF SALE (EoS)	END OF SOFTWARE SUPPORT (EoSS)	END OF TECHNICAL SUPPORT (EoTS), END OF RMA (EoRMA)
F5-VPR-LTM-B2150	**VIPRION Blade:** BIG-IP LTM B2150 Blade	1-Apr-2023 (01/04/2023)	1-Apr-2026 (01/04/2026)	1-Apr-2030 (01/04/2030)
F5-VPR-LTM-C2400-AC	**VIPRION Chassis:** BIG-IP LTM C2400 4-Slot Chassis AC Power	1-Apr-2023 (01/04/2023)	1-Apr-2026 (01/04/2026)	1-Apr-2030 (01/04/2030)

End of Sale Announcement for VIPRION B2150, B2250, C2200-AC, C2200-DC, C2400-AC, and C2400-DC - https://my.f5.com/manage/s/article/K95877400

BIG-IP software support policy - https://my.f5.com/manage/s/article/K5903

7.4.4. Considerando que os equipamentos operam em regime contínuo 24x7, a existência de garantia vigente e suporte técnico especializado é essencial para assegurar a disponibilidade dos serviços e a mitigação de falhas decorrentes do desgaste natural do *hardware* e de vulnerabilidades de *software*.

7.5. RISCOS PARA O ÓRGÃO

7.5.1. Conforme exposto anteriormente neste Estudo, embora os equipamentos atualmente em uso ainda atendam parcialmente ao propósito para o qual foram originalmente implantados, trata-se de uma solução em operação há longo período, baseada em componentes de *hardware* sem reposição garantida por contrato vigente e em *software* fora do ciclo de suporte do fabricante. Esse cenário expõe o CNPq a riscos relevantes, os quais são apresentados a seguir.

ID	CAUSA	RISCO	CONSEQUÊNCIA
1	Falhas elétricas ou envelhecimento do hardware	Falha de Hardware	Indisponibilidade das aplicações
2	Bugs em software legado	Falha de Software	Parada do equipamento e reincidência
3	Descoberta de novas vulnerabilidades	Vulnerabilidade de segurança	Exposição do balanceador e das aplicações
4	Ataques direcionados às aplicações	Exploração de vulnerabilidade	Indisponibilidade, vazamento ou adulteração de dados
5	Erros de configuração	Falha operacional	Interrupção dos serviços institucionais

7.5.2. Ressalta-se que o ambiente de *Application Delivery Controller* constitui ponto único de entrada e publicação das aplicações institucionais, sendo responsável pela intermediação de praticamente todo o tráfego entre usuários externos e os sistemas do CNPq.

7.5.3. O uso contínuo da versão *10.2.4 HF11* implica risco elevado de:

7.5.3.1. exploração remota e comprometimento total do sistema;

7.5.3.2. indisponibilidade de serviços críticos;

7.5.3.3. vazamento ou adulteração de dados sensíveis;

7.5.3.4. inviabilidade de integração segura com plataformas modernas e serviços em nuvem.

7.6. ESTIMATIVA DE DEMANDA DE BENS E SERVIÇOS

7.6.1. A presente seção tem por finalidade apresentar a estimativa preliminar de demanda de bens e serviços de TIC necessária ao atendimento da necessidade identificada neste Estudo Técnico Preliminar, considerando o ambiente de balanceamento de carga e segurança de aplicações do CNPq e sua criticidade para a continuidade operacional dos serviços institucionais.

7.6.2. A estimativa aqui descrita não configura definição antecipada de marca, modelo ou tecnologia específica, tampouco vincula a Administração a um formato único de fornecimento. Trata-se de projeção indicativa baseada em cenários plausíveis de atendimento da necessidade, a ser refinada após a etapa de análise de alternativas de solução.

7.6.3. Para fins de dimensionamento, adotam-se as seguintes premissas mínimas:

7.6.3.1. a solução deverá operar em alta disponibilidade, suportando falhas de componente sem interrupção perceptível dos serviços críticos;
7.6.3.2. o ambiente é de missão crítica, com operação contínua 24x7;
7.6.3.3. deverão ser atendidas, de forma integrada, as funcionalidades de balanceamento local (L4/L7), segurança de aplicações (WAF), *offload*/inspeção SSL/TLS e balanceamento global por DNS (GSLB), conforme requisitos técnicos levantados;
7.6.3.4. deverá ser prevista capacidade de evolução e execução de ajustes, melhorias, migrações e integrações ao longo da vigência.

7.6.4. A técnica de estimativa de demanda utilizada considerou, de forma não exaustiva, os seguintes parâmetros:

7.6.4.1. necessidade de arquitetura em cluster/alta disponibilidade, no mínimo com dois nós, suportando modos ativo-passivo e/ou ativo-ativo, conforme projeto;
7.6.4.2. necessidade de continuidade operacional durante janelas de manutenção, atualização e resposta a incidentes;
7.6.4.3. levantamento das interfaces necessárias para integração com a rede do Data Center, considerando conectividade de dados e gerenciamento;
7.6.4.4. necessidade de gestão centralizada, registro de logs, integração com NMS/SIEM e integração com ambientes de containers/orquestração via API;
7.6.4.5. necessidade de serviços especializados de implantação e operação assistida, considerando migração controlada e plano de *rollback*;
7.6.4.6. referência de práticas observadas em contratações similares na Administração Pública, especialmente quanto a prazo de garantia/suporte e previsão de horas técnicas para sustentação e evolução.

7.6.5. Considerando o requisito de alta disponibilidade e a criticidade dos serviços institucionais, estima-se a demanda mínima de 02 (duas) instâncias, nós ou componentes da solução, operando em arquitetura redundante, de forma a compor ambiente em alta disponibilidade. Justifica-se o quantitativo mínimo pelos seguintes fatores:

7.6.5.1. necessidade de redundância para tolerância a falhas de *hardware, software* ou componentes da solução;
7.6.5.2. necessidade de manter serviços em operação durante atividades de atualização, manutenção ou substituição de componentes;
7.6.5.3. necessidade de garantir continuidade de sessão e preservação de experiência do usuário;
7.6.5.4. aderência ao requisito de alta disponibilidade e mitigação de risco de indisponibilidade dos serviços institucionais.

7.6.6. A solução deverá ser fornecida com os elementos necessários ao seu pleno funcionamento, incluindo: *hardware*, licenciamento, garantia, subscrições, transceptores, cabos e acessórios de instalação em rack e demais componentes previstos nas especificações técnicas.

7.6.7. Para assegurar a implantação controlada e o início da operação em conformidade com os requisitos técnicos e de segurança, estima-se a demanda mínima dos seguintes serviços associados:

7.6.7.1. serviços especializados de instalação, configuração e implantação, incluindo plano de implantação, plano de *rollback*, testes e entrada em produção.;
7.6.7.2. garantia e suporte técnico oficial do fabricante durante todo o período contratual;

7.6.7.3. subscrições de segurança necessárias à atualização contínua dos mecanismos de proteção da solução;
7.6.7.4. suporte técnico especializado complementar, destinado ao atendimento preventivo, corretivo e evolutivo;

7.6.7.5. banco de horas técnicas destinado à execução de ajustes, integrações, migrações, otimizações e apoio técnico especializado.

7.6.8. Considerando a natureza dinâmica do ambiente de entrega e segurança de aplicações (aplicações novas, mudanças em políticas, evolução de TLS, atualização de assinaturas de WAF, tuning de performance, integrações com orquestradores, ajustes de DNS/GSLB e mitigação de incidentes), estima-se necessário prever banco de horas técnicas sob demanda.

7.6.9. A estimativa considera a natureza dinâmica e imprevisível das demandas associadas à operação de ambientes de entrega e segurança de aplicações. Para fins de planejamento, estima-se a necessidade de até 48 (quarenta e oito) horas técnicas por semestre, totalizando até 480 (quatrocentas e oitenta) horas em um horizonte de 60 (sessenta) meses, contemplando:

7.6.9.1. avaliação e diagnóstico de ambiente;
7.6.9.2. planejamento e execução de mudanças;
7.6.9.3. acompanhamento pós-mudança e operação assistida;
7.6.9.4. janelas de manutenção fora do horário comercial, quando necessário;
7.6.9.5. atividades evolutivas de segurança e performance.

7.6.10. O quantitativo poderá ser ajustado após a definição da alternativa de solução e do desenho final da arquitetura.

7.6.11. O dimensionamento preliminar da solução considera requisitos mínimos de desempenho e capacidade compatíveis com o ambiente institucional, incluindo processamento de tráfego de aplicações em camada 7 (L7), offload de SSL/TLS, inspeção de aplicações web (WAF), proteção contra ataques de negação de serviço e suporte a múltiplas aplicações institucionais. Esses requisitos são compatíveis com plataformas de *Application Delivery Controller* de classe corporativa utilizadas em ambientes de data center de missão crítica. Com base nessas premissas, a estimativa preliminar de bens e serviços necessários ao atendimento da demanda institucional encontra-se apresentada na tabela a seguir.

ITEM	DESCRIÇÃO	QUANTIDADE	MÉTRICA
1	*Appliance de Application Delivery Controller (ADC)* com funcionalidades integradas de *Web Application Firewall (WAF)*	2	Unidade
2	Licenciamento da solução de *ADC/WAF*	2	Unidade
3	Garantia e suporte técnico oficial do fabricante da solução (60 meses)	2	Unidade
4	Subscrições e assinaturas de segurança da solução (60 meses)	2	Unidade
5	Serviços especializados de instalação, configuração e implantação	1	Serviço
6	Serviços de consultoria técnica especializada sob demanda	480	Hora
7	Serviços de suporte técnico especializado da solução em regime 24x7	60	Mês

7.6.12. A estimativa de demanda apresentada contempla todos os bens e serviços necessários para implantação, operação, sustentação e evolução da solução de entrega e proteção de aplicações do CNPq, abrangendo equipamentos, licenciamento, garantia e suporte oficial do fabricante, subscrições de segurança e serviços técnicos especializados.

7.6.13. O quantitativo de 02 (duas) instâncias, nós ou componentes decorre da necessidade de implementação da solução em arquitetura de alta disponibilidade, garantindo redundância operacional, continuidade de serviço e tolerância a falhas.

7.6.14. O item referente aos serviços especializados de instalação, configuração e implantação contempla todas as atividades necessárias para disponibilização da solução em ambiente de produção, incluindo elaboração do projeto executivo, instalação física, configuração lógica, migração de políticas e regras existentes, integração com a infraestrutura do CNPq, execução de testes e entrada assistida em operação.

7.6.15. O apoio técnico especializado pós-implantação, estimado em até 480 (quatrocentas e oitenta) horas, destina-se à execução de atividades sob demanda relacionadas à evolução da solução, incluindo ajustes de configuração, revisões arquiteturais, implementação de novas funcionalidades, apoio a mudanças planejadas, otimização de desempenho e suporte especializado à equipe técnica do CNPq.

7.6.16. Os serviços de suporte técnico especializado previstos para 60 (sessenta) meses possuem natureza complementar ao suporte oficial do fabricante, destinando-se ao atendimento de demandas operacionais do CNPq, apoio à resolução de incidentes, acompanhamento de mudanças, orientações técnicas, análise de desempenho e apoio à evolução da solução.

7.6.17. Os quantitativos apresentados possuem caráter estimativo, podendo sofrer ajustes na etapa de definição final da solução e da elaboração do Termo de Referência.

7.6.18. A vigência contratual estimada de 60 (sessenta) meses para os serviços associados à solução de balanceamento de aplicações e firewall de aplicações web está alinhada às boas práticas de contratação de infraestrutura crítica de tecnologia da informação.

7.6.19. Esse período permite garantir continuidade operacional, estabilidade tecnológica e previsibilidade orçamentária, fatores especialmente relevantes em ambientes de missão crítica que suportam aplicações institucionais essenciais.

7.6.20. A adoção de horizonte contratual mais amplo também se justifica pelas seguintes razões:

7.6.20.1. o ciclo de vida típico de equipamentos e soluções de infraestrutura de rede e segurança costuma variar entre 5 (cinco) e 7 (sete) anos, sendo prática comum associar contratos de suporte e garantia a períodos de até 60 meses;

7.6.20.2. a vigência estendida reduz a necessidade de processos licitatórios frequentes para manutenção de infraestrutura essencial;

7.6.20.3. permite melhor aproveitamento do investimento público, garantindo que a solução permaneça suportada pelo fabricante durante período adequado;

7.6.20.4. assegura disponibilidade contínua de atualizações de *software*, correções de segurança e suporte técnico especializado.

7.6.21. Dessa forma, a previsão de vigência contratual de até 60 (sessenta) meses busca garantir equilíbrio entre economicidade, eficiência administrativa e segurança operacional, assegurando que a solução permaneça plenamente suportada durante todo o período de utilização previsto.

8. Levantamento de soluções

8.1. O principal objetivo deste Estudo Técnico Preliminar (ETP) é orientar a seleção da solução mais adequada, pautada em critérios de eficácia, efetividade, eficiência e viabilidade econômica, de modo a satisfazer plenamente às necessidades de negócio deste Conselho.

8.2. Portanto, para alcançar este objetivo, é crucial que a equipe de planejamento da contratação elabore critérios que viabilizem a comparação entre diversas soluções, tanto em termos de qualidade quanto de viabilidade econômica, ao mesmo tempo em que visa estabelecer uma base sólida para a tomada de decisões alinhadas aos objetivos estratégicos da instituição e em conformidade com as diretrizes do artigo 11, inciso II da IN SGD/ME nº 94/2022, de forma a proporcionar a escolha da melhor solução.

8.3. Foram identificadas 3 (três) possíveis cenários para a segurança da informação, conforme descrição da tabela a seguir:

CENÁRIO	DESCRIÇÃO
1	Utilização de solução baseada em software livre
2	Solução em nuvem (SaaS ou serviço gerenciado)
3	Solução de *Application Delivery Controller* (ADC), com instalação on-premise

8.4. Verificou-se que não há solução que atenda à necessidade deste processo de contratação no Catálogo de Soluções de TIC com condições padronizadas para licenciamento de software. Desta forma, não há de se considerar o PMC-TIC.

9. Análise comparativa de soluções

9.1. A análise comparativa de soluções, nos termos do inciso II do art. 11 da Instrução Normativa SGD/ME nº 94, de 23 de dezembro de 2022, tem por objetivo identificar e avaliar as alternativas disponíveis para atendimento da necessidade identificada neste Estudo Técnico Preliminar.

9.2. Essa análise considera não apenas o aspecto econômico, mas também aspectos qualitativos relacionados à segurança, desempenho, governança, continuidade operacional e aderência à arquitetura tecnológica institucional.

9.3. Com base nessas premissas, foram avaliados os seguintes cenários possíveis de atendimento à necessidade de modernização da solução de balanceamento de aplicações e proteção de aplicações web do CNPq.

9.4. CENÁRIO 1 - UTILIZAÇÃO DE SOLUÇÃO BASEADA EM SOFTWARE LIVRE

9.4.1. O modelo de Application Delivery Controller (ADC) baseado em software livre apresenta limitações relevantes para sua adoção em um ambiente corporativo como o do CNPq. Esse tipo de solução, em geral, não possui suporte técnico oficial estruturado, dependendo de atualizações disponibilizadas pela comunidade, as quais podem demandar períodos mais longos para testes consistentes e disponibilização em versões estáveis. Além disso, a capacidade de tratar e inspecionar grandes volumes de tráfego pode ser limitada, uma vez que tais soluções normalmente não dispõem de hardware desenvolvido especificamente para essa finalidade.

9.4.2. De forma complementar, esse tipo de solução geralmente requer a utilização de servidores de propósito geral para execução das funções de balanceamento de carga e inspeção de tráfego, não contando com hardware especializado projetado especificamente para processamento intensivo de aplicações, criptografia e inspeção de tráfego em larga escala. Em ambientes que demandam processamento avançado em camada 7 (L7), offload de SSL/TLS, inspeção de aplicações web (WAF) e mitigação de ataques de negação de serviço, a ausência de aceleração por hardware e de arquitetura otimizada pode resultar em limitações de desempenho, aumento de latência e maior complexidade operacional.

9.4.3. Outro aspecto relevante refere-se à ausência de funcionalidades integradas típicas de plataformas ADC corporativas, tais como gerenciamento centralizado, mecanismos robustos de alta disponibilidade com sincronização de estado entre equipamentos, recursos avançados de proteção a aplicações web, ferramentas de análise e visibilidade de tráfego, integração nativa com serviços de identidade e automação por meio de APIs estruturadas. A implementação dessas funcionalidades em soluções baseadas em software livre geralmente depende da integração de múltiplos componentes independentes, o que aumenta significativamente a complexidade de implantação, manutenção e operação.

9.4.4. Adicionalmente, a adoção de soluções baseadas exclusivamente em software livre implicaria maior dependência da equipe técnica interna para configuração, manutenção, atualização e resolução de problemas, elevando o risco operacional e a necessidade de especialização contínua. Tal cenário pode impactar negativamente a capacidade institucional de manter níveis adequados de disponibilidade, segurança e governança das aplicações críticas hospedadas no ambiente do CNPq.

9.5. CENÁRIO 2 - SOLUÇÃO EM NUVEM (SAAS OU SERVIÇO GERENCIADO)

9.5.1. Uma solução de *Application Delivery Controller* (ADC) e *Web Application Firewall* (WAF) baseada em nuvem consiste na disponibilização das funcionalidades de balanceamento de carga, aceleração de aplicações, inspeção de tráfego e proteção de aplicações web por meio de infraestrutura hospedada e operada por fornecedor especializado. Nesse modelo, os componentes responsáveis pelo processamento e proteção do tráfego não são instalados diretamente no datacenter do órgão, sendo acessados como serviço, normalmente por meio da internet ou de conexões dedicadas. A solução pode ser ofertada no formato *Software as a Service* (SaaS) ou como serviço gerenciado.

9.5.2. No modelo SaaS, o fornecedor disponibiliza uma plataforma compartilhada ou dedicada, acessível remotamente, na qual são executadas as funcionalidades de ADC e WAF. O tráfego destinado às aplicações institucionais é direcionado para a infraestrutura do provedor, que passa a realizar atividades como balanceamento de carga, inspeção de requisições HTTP/HTTPS, mitigação de ataques, aplicação de políticas de segurança, cache, aceleração e controle de sessões. O gerenciamento da infraestrutura subjacente, bem como atualizações, correções de segurança e escalabilidade da plataforma, permanecem sob responsabilidade do prestador do serviço.

9.5.3. Já no modelo de serviço gerenciado, além da disponibilização da tecnologia, o fornecedor também assume atividades operacionais relacionadas à administração da solução, tais como configuração de políticas, monitoramento contínuo, resposta a incidentes, ajustes de desempenho, atualização de assinaturas de segurança e suporte técnico especializado. Nesse formato, o órgão contratante reduz significativamente a necessidade de atuação direta da equipe interna na operação cotidiana da plataforma, transferindo parte da responsabilidade operacional ao contratado.

9.5.4. Entre as principais vantagens desse modelo destacam-se a elevada escalabilidade, a redução da necessidade de aquisição de infraestrutura própria, a simplificação das atividades de atualização tecnológica e a possibilidade de rápida expansão da capacidade de atendimento conforme a demanda. Além disso, soluções em nuvem frequentemente oferecem recursos avançados de proteção contra ataques distribuídos (*DDoS*), inteligência global de ameaças e presença geograficamente distribuída, o que pode contribuir para maior disponibilidade e resiliência dos serviços publicados.

9.5.5. Por outro lado, a adoção desse modelo exige avaliação criteriosa de aspectos relacionados à segurança da informação, governança e conformidade normativa. Como o tráfego das aplicações passa a ser processado parcial ou integralmente em ambiente externo ao órgão, devem ser analisados requisitos de soberania dos dados, aderência à Lei Geral de Proteção de Dados (LGPD), requisitos de sigilo institucional, dependência de conectividade externa e eventuais impactos de latência. Também devem ser considerados aspectos relacionados à integração com sistemas legados, autenticação corporativa e interoperabilidade com a infraestrutura atualmente existente.

9.5.6. Adicionalmente, a contratação de soluções ADC/WAF em nuvem demanda análise do modelo financeiro envolvido, uma vez que normalmente se baseia em cobrança recorrente, vinculada a métricas como volume de tráfego, quantidade de aplicações protegidas, largura de banda, número de usuários ou consumo de recursos. Dessa forma, embora possa reduzir investimentos iniciais em infraestrutura física, o modelo pode representar custos operacionais contínuos ao longo do tempo, devendo ser avaliado sob a perspectiva de custo total de propriedade (*Total Cost of Ownership – TCO*) e aderência às necessidades institucionais de médio e longo prazo.

9.6. CENÁRIO 3 - SOLUÇÃO APPLICATION DELIVERY CONTROLLER (ADC), COM INSTALAÇÃO ON-PREMISE

9.6.1. A adoção de solução ADC corporativa no modelo *on-premise* consiste na implantação de plataforma especializada composta por equipamentos dedicados, licenciamento, subscrições de segurança e serviços associados, instalada fisicamente no ambiente de data center do CNPq.

9.6.2. Esse modelo apresenta diversas vantagens relevantes para ambientes institucionais de missão crítica, destacando-se:

9.6.2.1. Controle e governança: permite controle completo sobre dados, tráfego, políticas de segurança e configurações da solução, garantindo maior aderência às políticas institucionais de segurança da informação.

9.6.2.2. Segurança e conformidade: a instalação local possibilita que todo o processamento de tráfego de aplicações ocorra dentro do perímetro de segurança institucional, facilitando o atendimento a requisitos de segurança, auditoria e conformidade.

9.6.2.3. Personalização profunda: as soluções on-premise geralmente podem ser altamente personalizadas para atender às necessidades específicas do negócio. Isso pode incluir a integração com outros sistemas internos, adaptando funcionalidades e modificando fluxos de trabalho.

9.6.2.4. Independência do fornecedor: ao gerenciar sistemas internamente, uma organização não depende completamente de um fornecedor externo para tarefas de configuração, disponibilidade ou atualizações. Isso auxilia a reduzir os riscos associados à dependência de terceiros.

9.6.2.5. Desempenho e baixa latência: soluções on-premise operam diretamente no ambiente de data center da instituição, reduzindo latência e proporcionando melhor desempenho para aplicações críticas.

9.6.2.6. Custos de longo prazo: embora a implantação de soluções on-premise possa demandar investimento inicial superior, esse modelo tende a apresentar maior previsibilidade de custos ao longo do ciclo de vida da solução, especialmente em ambientes institucionais que já dispõem de infraestrutura de data center consolidada;

9.6.2.7. Alta disponibilidade: plataformas ADC corporativas permitem a implementação de arquiteturas em cluster com alta disponibilidade, garantindo continuidade operacional mesmo em cenários de falha de hardware ou software.

9.6.2.8. Integração com a infraestrutura existente: a solução pode ser integrada de forma direta com a arquitetura de rede existente, incluindo firewalls, sistemas de monitoramento, ferramentas de gestão e plataformas de autenticação.

9.6.3. Dessa forma, a adoção de solução ADC corporativa on-premise apresenta elevado grau de aderência às necessidades técnicas, operacionais e de segurança do ambiente tecnológico do CNPq.

9.6.4. Critérios de comparação das alternativas

9.6.4.1. Para fins de comparação entre as alternativas avaliadas, foram considerados critérios técnicos e operacionais alinhados aos requisitos levantados neste Estudo Técnico Preliminar. Os principais critérios considerados foram:

ID	REQUISITOS	CARACTERÍSTICAS
1	Continuidade e alta disponibilidade	suporte a arquitetura em cluster com failover automático;
		operação em regime contínuo 24x7;
		possibilidade de manutenção e atualização com impacto mínimo nos serviços.
2	Entrega de aplicações e desempenho	suporte a balanceamento de carga em camadas 4 e 7;
		mecanismos de persistência e health checks;
		aceleração criptográfica e offload de SSL/TLS.

3	Segurança de aplicações	suporte a Web Application Firewall (WAF);
		capacidade de mitigação de ataques comuns a aplicações web;
		suporte à evolução contínua de políticas de segurança.
4	Operação e governança	capacidade de integração com ferramentas de monitoramento e SIEM;
		mecanismos de auditoria e rastreabilidade de ações administrativas.
5	Migração e risco operacional	capacidade de migração controlada do ambiente existente;
		redução de risco de indisponibilidade durante a transição;
		aproveitamento do conhecimento técnico já existente na equipe institucional.
6	Adequação a ambiente de missão crítica	aderência ao ambiente tecnológico existente;
		controle operacional;
		requisitos de segurança e governança institucional.

9.6.5. Quadro comparativo entre as alternativas

ID	CRITÉRIO	CENÁRIO 1 - SOFTWARE LIVRE	CENÁRIO 2 - SOLUÇÃO EM NUVEM	CENÁRIO C - ADC ON-PREMISE
1	**Continuidade e alta disponibilidade (cluster, failover, operação 24x7)**	Limitado	Atende parcialmente	Atende plenamente
2	**Entrega de aplicações e desempenho (L4/L7, persistência, SSL offload)**	Dependente da infraestrutura	Atende plenamente	Atende plenamente
3	**Segurança de aplicações (WAF, mitigação de ataques web)**	Limitado	Atende plenamente	Atende plenamente

4	**Operação e governança (logs, auditoria, integração SIEM/NMS)**	Limitado	Atende parcialmente	Atende plenamente
5	**Migração e risco operacional**	Alto risco	Risco moderado	Risco moderado
6	**Adequação a ambiente de missão crítica**	Baixa	Moderada	Alta

9.6.6. Levantamento de contratações similares na administração pública

9.6.6.1. Com o objetivo de verificar a aderência da solução proposta às práticas adotadas na Administração Pública, foi realizado levantamento complementar sobre contratações relacionadas a soluções de entrega, balanceamento e proteção de aplicações, incluindo plataformas ADC corporativas e soluções WAF utilizadas em ambientes institucionais críticos.

9.6.6.2. O levantamento identificou predominância da adoção de soluções ADC corporativas instaladas localmente (on-premise) em órgãos e entidades responsáveis pela operação de ambientes de missão crítica, especialmente quando há necessidade de maior controle operacional, integração com infraestrutura existente, processamento local do tráfego e requisitos elevados de disponibilidade e segurança.

9.6.6.3. As informações foram obtidas a partir de consultas a sistemas oficiais de compras públicas, contratos administrativos e registros de pregões eletrônicos, conforme demonstrado a seguir.

ÓRGÃO	PREGÃO / CONTRATO	OBJETO / SOLUÇÃO
Superior Tribunal de Justiça - STJ	PE n°110 /2023	Contratação de empresa especializada para fornecimento de solução de Web Application Firewall (WAF) com serviços de instalação, configuração, suporte técnico e treinamento, conforme especificação do objeto constante do Termo de Referência, edital.
Conselho da Justiça Federal - CJF	PE n° 90008/2025	Contratação de empresa especializada, por meio de Registro de Preços – SRP, para o fornecimento de solução tecnológica de Controlador de Entrega de Aplicações (Application Delivery Controller – ADC), incluindo os serviços de instalação, configuração, suporte técnico mensal e transferência de conhecimento, bem como serviços técnicos especializados, sob demanda, para implementação e customização da solução, com vistas a atender às necessidades do Conselho da Justiça Federal e demais órgãos partícipes.
Coordenação de Aperfeiçoamento de Pessoal de Nível Superior - CAPES	PE n° 16/2023	contratação de Solução de Segurança de Balanceador de Cargas com funcionalidades de WAF (Web Application Firewall), incluindo garantia e suporte técnico de 60 (sessenta) meses, bem como a prestação de serviços agregados de instalação, migração, configuração, transferência de conhecimento e apoio técnico especializado pós-implantação sob demanda, conforme condições, quantidades e exigências estabelecidas neste Edital e seus anexos.
Tribunal Regional Federal da 3ª Região - TRF3	CONTRATO nº 07.006.10.2025	O objeto deste contrato consiste no fornecimento de solução tecnológica de Controlador de Entrega de Aplicações (Application Delivery Controller – ADC), incluindo os serviços de instalação, configuração, suporte técnico mensal e transferência de conhecimento, bem como serviços técnicos especializados, sob demanda, para implementação e customização da solução, conforme especificações técnicas contidas no Termo de Referência

		e seus anexos, com vistas a atender às necessidades do Tribunal Regional Federal da 3ª Região e da Justiça Federal de Primeiro Grau em São Paulo.
Banco do Nordeste do Brasil	CONTRATO nº 2023/153	O presente Contrato tem por objeto a aquisição de equipamentos balanceadores de carga, aceleradores e firewall de aplicação, com seus respectivos serviços de implantação, treinamento, suporte e assistência técnica, em conformidade com as especificações constantes deste Instrumento, do Edital e de seus Anexos.
Companhia de Tecnologia da Informação e Comunicação do Paraná - CELEPAR	CONTRATO GMS nº 1335/2026	Contratação de empresa para fornecimento de solução de Application Delivery Controller (ADC) para balanceamento, otimização e controle de entrega de serviços de aplicações, incluindo equipamentos (hardware e software), garantia e suporte técnico por 60 (sessenta) meses, de forma a atender plenamente as características descritas neste edital e seus anexos.
Companhia de Processamento de Dados do Estado de São Paulo PRODESP	PE n° 90061/2024	Fornecimento de 2 (dois) Balanceadores de Carga (ADC) do tipo “Appliance” em alta disponibilidade, instalação, configuração, treinamento, Serviço de Consultoria, serviços de garantia e manutenção especializada on site pelo período de 60 (sessenta) meses.
Serviço Federal de Processamento de Dados - SERPRO	PE n° 91107/2024	Contratação de appliances e componentes adicionais com garantia técnica, para a Solução de Balanceamento de Aplicações com funcionalidades de segurança e WAF (Web Application Firewall) para Data Centers do Serpro. Devem incluir seus dispositivos, softwares, e as licenças para recursos de segurança e gerenciamento integrado, mediante criação de Ata de Registro de Preços cujo órgão gerenciador é o Serpro.
Tribunal Regional Federal da Primeira Região - TRF 1	PE nº 56/2023	A presente licitação tem por objeto a contratação de empresa especializada para o fornecimento de solução de balanceadores de carga, com garantia de 60 (sessenta) meses, serviço de instalação, implantação, integração dos produtos, operação assistida e treinamento, de acordo com condições, especificações, quantidades constantes deste Edital e seus Anexos.
Secretaria de Estado de Desenvolvimento e Inovação Estado de Goiás	CONTRATO n° 26/2022 - SEDI	Aquisição de Solução de Applica on Delivery Controller (ADC), com funções de balanceador de carga e aceleração web com módulos de Loading Balance, Global Server Loading Balance, Web Application Firewall, SSL offload e inspection, incluindo garantia, Suporte técnico e subscrições e treinamentos, conforme quantitativos, especificações e condições estabelecidos no Termo de Referência
Advocacia Geral da União - AGU	PE n° 90002/2026	Aquisição de Solução de Segurança de Balanceamento de Carga com suporte, instalação, licenciamento e garantia, conforme condições e exigências estabelecidas no Termo de Referência.

9.6.6.4. A análise das contratações identificadas demonstra que soluções de Application Delivery Controller (ADC) constituem tecnologia amplamente utilizada na Administração Pública para suporte a ambientes responsáveis pela disponibilização de sistemas institucionais, serviços digitais e aplicações críticas.

9.6.6.5. Observa-se que essas soluções são empregadas, de forma recorrente, para:

9.6.6.5.1. distribuição inteligente de carga entre servidores de aplicação;

9.6.6.5.2. aumento da disponibilidade e resiliência de sistemas institucionais;

9.6.6.5.3. otimização do desempenho de aplicações web;

9.6.6.5.4. implementação de mecanismos de segurança, incluindo proteção contra ataques a aplicações (WAF);

9.6.6.5.5. controle e inspeção do tráfego entre usuários e sistemas corporativos.

9.6.6.6. Verifica-se, ainda, predominância da adoção de arquiteturas especializadas baseadas em plataformas dedicadas instaladas localmente (*on-premise*), especialmente em ambientes de missão crítica que demandam elevado nível de integração, governança e controle operacional.

9.6.6.7. Também se observa recorrência na continuidade tecnológica de plataformas previamente implantadas, com o objetivo de reduzir riscos operacionais, preservar conhecimento técnico acumulado, simplificar a administração do ambiente e minimizar impactos decorrentes de processos de migração.

9.6.6.8. O levantamento evidencia que a utilização de soluções ADC corporativas instaladas localmente constitui prática consolidada na Administração Pública para atendimento dos requisitos de disponibilidade, desempenho, segurança e continuidade operacional.

9.6.6.9. Nesse contexto, a solução proposta neste Estudo Técnico Preliminar mostra-se aderente às práticas observadas em outros órgãos e entidades públicas, reforçando sua adequação técnica e operacional para atendimento das necessidades do CNPq.

9.6.7. Observância das alternativas às políticas, premissas e especificações técnicas vigentes

REQUISITO	CENÁRIOS	SIM	NÃO	NÃO SE APLICA
A Solução encontra-se implantada em outro órgão ou entidade da Administração Pública Federal?	1		X	
	2	X		
	3	X		
A Solução está disponível no Portal do Software Público Brasileiro?	1		X	
	2			X
	3		X	
A Solução é um software livre ou software público?	1	X		
	2			X
	3		X	
A Solução é aderente às políticas, premissas e especificações técnicas definidas pelos Padrões e-PING, e-MAG?	1			X
	2			X
	3			X

A Solução é aderente às regulamentações da ICP-Brasil? (quando houver necessidade de certificação digital)	1			X
	2			X
	3			X
A Solução é aderente às orientações, premissas e especificações técnicas e funcionais do e-ARQ Brasil? (quando o objetivo da solução abranger documentos arquivísticos)	1			X
	2			X
	3			X

10. Registro de soluções consideradas inviáveis

10.1. Com base nas análises apresentadas na seção anterior deste Estudo Técnico Preliminar, e nos termos do §1º do art. 11 da Instrução Normativa SGD/ME nº 94/2022, registram-se as alternativas de solução avaliadas que foram consideradas **i**nviáveis para atendimento da necessidade institucional.

10.2. CENÁRIO 1 – UTILIZAÇÃO DE SOLUÇÃO BASEADA EM SOFTWARE LIVRE

10.2.1. A alternativa baseada em software livre foi considerada tecnicamente inviável para o contexto do ambiente institucional do CNPq, especialmente considerando os requisitos de disponibilidade, segurança, governança, desempenho e suporte exigidos para a infraestrutura de entrega e proteção de aplicações.

10.2.2. Embora existam soluções de balanceamento de carga baseadas em software livre amplamente utilizadas em determinados contextos, essas soluções normalmente não contam com suporte oficial estruturado de fabricante com níveis de serviço, atualizações coordenadas e suporte especializado compatíveis com ambientes corporativos de missão crítica.

10.2.3. Nesse cenário, a responsabilidade pela implantação, manutenção, atualização de segurança, correção de vulnerabilidades e resolução de incidentes recairia majoritariamente sobre a equipe técnica interna, elevando significativamente o esforço operacional necessário para sustentação da solução.

10.2.4. Adicionalmente, soluções dessa natureza normalmente requerem infraestrutura baseada em servidores de propósito geral e integração de múltiplos componentes independentes para prover funcionalidades equivalentes às plataformas corporativas de ADC/WAF, aumentando a complexidade de implantação, manutenção e operação do ambiente.

10.2.5. Verificou-se ainda que plataformas baseadas exclusivamente em software livre normalmente não disponibilizam, de forma nativa e integrada, diversas funcionalidades presentes em plataformas ADC corporativas, tais como:

10.2.5.1. mecanismos avançados de inspeção, transformação e tratamento de tráfego;

10.2.5.2. gerenciamento centralizado e visão integrada do ambiente;

10.2.5.3. sincronização de estado e mecanismos avançados de alta disponibilidade;

10.2.5.4. aceleração criptográfica e processamento otimizado para SSL/TLS;

10.2.5.5. integração estruturada com APIs, automação e mecanismos de gerenciamento;

10.2.5.6. funcionalidades avançadas de proteção e segurança de aplicações.

10.2.6. No contexto do ambiente atualmente existente no CNPq, verificou-se ainda que a adoção de solução baseada exclusivamente em software livre demandaria atividades adicionais de migração e adaptação da infraestrutura atualmente implantada. O ambiente em

operação possui regras e configurações específicas associadas ao tratamento do tráfego das aplicações institucionais, incluindo mecanismos de balanceamento, redirecionamentos condicionais, tratamento diferenciado de requisições, políticas customizadas e regras baseadas em expressões regulares.

10.2.7. Foram identificadas implementações equivalentes a mecanismos de inspeção e tratamento avançado de tráfego, atualmente utilizados para atendimento de regras específicas de publicação e operação das aplicações institucionais.

10.2.8. A eventual migração dessas configurações para plataformas baseadas em software livre demandaria reimplementação, adaptação e validação individualizada das regras existentes, ampliando a complexidade da transição tecnológica, o esforço de implantação e o risco operacional associado.

10.2.9. A existência de aplicações com regras específicas de tratamento de tráfego, controle de acesso, redirecionamentos, tratamento de sessões e lógica operacional customizada exigiria ciclos adicionais de testes, homologação e validação, aumentando o tempo e a complexidade do processo de migração.

10.2.10. Observou-se ainda que o ambiente institucional já possui conhecimento técnico acumulado relacionado à operação de plataformas ADC corporativas, abrangendo procedimentos operacionais, configurações específicas, integrações e tratamento das aplicações atualmente publicadas. A adoção de solução baseada exclusivamente em software livre demandaria processo adicional de adaptação operacional, capacitação e revisão de procedimentos internos.

10.2.11. Considerando os requisitos de disponibilidade, continuidade operacional, suporte especializado, integração com a infraestrutura existente, preservação do conhecimento técnico institucional e redução de riscos de migração, concluiu-se que a adoção de solução baseada exclusivamente em software livre não atende plenamente às necessidades identificadas para o ambiente de entrega e proteção de aplicações do CNPq, sendo considerada tecnicamente inviável.

10.3. CENÁRIO 2 – SOLUÇÃO EM NUVEM (SAAS OU SERVIÇO GERENCIADO)

10.3.1. A adoção de solução de Application Delivery Controller (ADC) e Web Application Firewall (WAF) baseada exclusivamente em nuvem, no modelo Software as a Service (SaaS) ou serviço gerenciado, apresenta limitações relevantes frente às necessidades operacionais, arquiteturais e de segurança do ambiente institucional. Considerando a criticidade dos serviços disponibilizados pelo órgão, bem como a necessidade de elevado nível de controle sobre o tráfego de aplicações e integrações internas, a utilização de infraestrutura externa para processamento e inspeção das comunicações pode introduzir riscos operacionais e de governança incompatíveis com os requisitos institucionais identificados.

10.3.2. Um dos principais fatores de inviabilidade relaciona-se à dependência de conectividade externa para funcionamento da solução. Nesse modelo, o tráfego destinado às aplicações institucionais precisaria ser direcionado para infraestrutura mantida por terceiros, localizada fora do ambiente computacional do órgão. Dessa forma, eventuais indisponibilidades de links de comunicação, degradações de conectividade ou falhas em provedores externos poderiam impactar diretamente a disponibilidade dos sistemas institucionais, inclusive em situações nas quais os serviços internos permanecessem operacionalmente disponíveis no datacenter local.

10.3.3. Outro aspecto relevante refere-se aos requisitos de segurança da informação, sigilo institucional e governança sobre os dados trafegados. Soluções em nuvem exigem que parte significativa do tráfego das aplicações seja processada em ambiente externo ao domínio administrativo do órgão, incluindo requisições autenticadas, sessões de usuários e, em determinados cenários, conteúdo inspecionado por mecanismos de proteção HTTPS/TLS. Tal característica pode gerar restrições relacionadas ao controle operacional, rastreabilidade, gestão de registros de tráfego e aderência às políticas institucionais de segurança e proteção de dados.

10.3.4. Adicionalmente, observam-se limitações quanto à integração com a infraestrutura atualmente existente. O ambiente institucional do CNPq possui arquitetura consolidada baseada em serviços publicados localmente, integrações específicas, mecanismos de autenticação, roteamento, segmentação de rede e regras de balanceamento desenvolvidas ao longo dos anos de operação da plataforma atualmente utilizada.

10.3.5. Parte relevante dessas implementações contempla regras específicas de publicação e tratamento das aplicações, incluindo redirecionamentos, reescritas, controle de acesso, regras condicionais, expressões regulares e mecanismos customizados aplicados ao tráfego institucional. A migração dessas funcionalidades para modelo baseado exclusivamente em nuvem demandaria atividades adicionais de adaptação, reconfiguração, validação e testes.

10.3.6. Adicionalmente, a adoção de solução SaaS ou totalmente gerenciada poderia demandar alterações significativas na topologia de publicação dos serviços, mecanismos de encaminhamento de tráfego, políticas de segurança e integração com componentes atualmente instalados no ambiente tecnológico do CNPq, aumentando a complexidade da transição e os riscos associados ao processo de migração.

10.3.7. Observou-se ainda que o ambiente institucional já possui conhecimento técnico acumulado relacionado à operação de plataformas ADC instaladas localmente, abrangendo procedimentos operacionais, configurações específicas, integrações e tratamento das aplicações atualmente publicadas. A adoção de solução integralmente baseada em nuvem demandaria processo adicional de capacitação, adaptação operacional e revisão de procedimentos internos.

10.3.8. Sob a perspectiva econômica e contratual, também foram identificados fatores desfavoráveis. Soluções em nuvem normalmente utilizam modelos de cobrança recorrente baseados em volume de tráfego, largura de banda, quantidade de aplicações protegidas ou consumo de recursos computacionais. Em ambientes institucionais com crescimento contínuo de utilização e elevado volume de acessos, esse modelo pode resultar em aumento progressivo de custos ao longo do período contratual, reduzindo previsibilidade orçamentária e potencialmente tornando o custo total de propriedade superior ao de soluções implantadas localmente.

10.3.9. Considerando os requisitos de integração com a infraestrutura existente, a necessidade de elevado nível de controle operacional, a preservação do conhecimento técnico institucional, a continuidade tecnológica do ambiente e a redução dos riscos associados à migração, conclui-se que a alternativa baseada exclusivamente em solução em nuvem apresenta menor aderência às necessidades identificadas para o ambiente de entrega e proteção de aplicações do CNPq, sendo considerada tecnicamente inviável para a presente contratação.

10.4. CONCLUSÃO DA ANÁLISE COMPARATIVA DAS ALTERNATIVAS

10.4.1. A análise comparativa demonstra que as alternativas baseadas em software livre e em solução em nuvem apresentam limitações relevantes frente às necessidades identificadas para o ambiente institucional do CNPq.

10.4.2. No caso das soluções baseadas em software livre, foram observadas limitações relacionadas à ausência de funcionalidades corporativas integradas, maior dependência de atuação da equipe técnica interna, necessidade de adaptação e migração das configurações atualmente existentes, maior complexidade operacional e riscos associados à transição tecnológica.

10.4.3. Quanto às soluções baseadas em nuvem, verificaram-se limitações relacionadas ao modelo operacional, governança do ambiente, dependência de infraestrutura externa, integração com o ambiente tecnológico existente, controle institucional sobre o processamento do tráfego das aplicações e necessidade de adequações decorrentes da migração para arquitetura externa.

10.4.4. Considerando as características do ambiente tecnológico do CNPq, a necessidade de integração com a infraestrutura existente, os requisitos de continuidade operacional, governança, controle do ambiente, processamento local do tráfego das aplicações, preservação do conhecimento técnico institucional e redução dos riscos de migração, verifica-se que a alternativa baseada em solução ADC corporativa com instalação on-premise apresenta maior aderência aos requisitos técnicos e operacionais identificados neste Estudo Técnico Preliminar.

11. Análise comparativa de custos (TCO)

11.1. Considera-se que um dos objetivos das contratações públicas é assegurar igualdade de condições entre os licitantes, observando-se que a finalidade do processo licitatório é selecionar a proposta mais vantajosa para a Administração Pública, considerando aspectos técnicos, operacionais e econômicos.

11.2. Com base na análise comparativa realizada entre as alternativas levantadas neste Estudo Técnico Preliminar, a alternativa tecnicamente mais adequada para atendimento da necessidade institucional do CNPq é a adoção de solução corporativa de *Application Delivery Controller (ADC)* no modelo on-premise, em arquitetura de alta disponibilidade.

11.3. Essa alternativa apresenta maior aderência aos requisitos técnicos, operacionais e de segurança definidos neste Estudo Técnico Preliminar, garantindo, entre outros aspectos:

- **11.3.1.** maior controle sobre a infraestrutura e o tráfego de aplicações;
- **11.3.2.** melhor desempenho e menor latência para as aplicações institucionais;
- **11.3.3.** integração direta com a arquitetura de segurança existente;
- **11.3.4.** suporte técnico estruturado e atualizações contínuas do fabricante.

11.4. A solução selecionada também apresenta maior aderência à arquitetura tecnológica atualmente utilizada, especialmente quanto à compatibilidade com configurações, políticas e integrações já implementadas. A continuidade tecnológica favorece a padronização da infraestrutura, reduz a curva de aprendizado da equipe técnica e contribui para maior eficiência na operação e manutenção da solução ao longo de seu ciclo de vida.

11.5. Ademais, o ambiente atualmente em operação já possui configurações, políticas, objetos e mecanismos de customização específicos, inclusive por meio de scripts e lógicas de tratamento de tráfego, cuja migração tende a ser substancialmente mais simples e segura quando realizada para solução compatível com a plataforma já utilizada no ambiente institucional.

11.6. Dessa forma, a contratação de solução ADC corporativa no modelo *on-premise*, em arquitetura de alta disponibilidade e com suporte técnico especializado, constitui a alternativa mais adequada para assegurar a continuidade, segurança e desempenho dos serviços digitais disponibilizados pelo CNPq.

11.7. CONTINUIDADE TECNOLÓGICA E PADRONIZAÇÃO DO AMBIENTE

11.7.1. O ambiente atual de entrega e proteção de aplicações do CNPq utiliza solução de ADC da fabricante F5 Networks, atualmente em operação há longo período na infraestrutura tecnológica da instituição. Mesmo após vários anos de utilização, a solução atualmente implantada continua desempenhando suas funções de balanceamento de aplicações e proteção de serviços web, evidenciando a robustez, confiabilidade e maturidade da tecnologia adotada.

11.7.2. Esse histórico de operação demonstra que a plataforma apresenta elevado grau de estabilidade operacional e aderência às necessidades institucionais do CNPq, constituindo importante referência para a definição da solução de atualização tecnológica.

11.7.3. Nesse contexto, a continuidade tecnológica da plataforma atualmente utilizada apresenta vantagens relevantes para a Administração Pública, dentre as quais se destacam:

11.7.3.1. preservação da padronização da infraestrutura tecnológica do ambiente de data center;
11.7.3.2. maior interoperabilidade entre componentes e serviços já existentes;
11.7.3.3. simplificação das atividades de administração, operação e monitoramento da solução;
11.7.3.4. redução de riscos operacionais associados à adoção de tecnologias distintas.

11.7.4. A adoção de plataforma tecnológica compatível com a atualmente utilizada permite manter padrões operacionais já consolidados ao longo dos anos de utilização da solução, garantindo maior estabilidade e previsibilidade na operação do ambiente.

11.8. COMPLEXIDADE DO AMBIENTE ATUAL E RISCOS DE MIGRAÇÃO

11.8.1. Soluções de *Application Delivery Controller* (ADC) possuem elevado grau de complexidade técnica, sendo responsáveis pela entrega de aplicações institucionais críticas, bem como pela proteção contra ameaças direcionadas às aplicações web expostas à internet.

11.8.2. Ao longo dos anos de operação da solução atualmente utilizada no ambiente do CNPq, foram implementadas diversas configurações, objetos de infraestrutura, políticas de balanceamento de carga, regras de segurança e integrações com sistemas institucionais, que compõem a lógica operacional responsável pelo funcionamento das aplicações hospedadas no ambiente institucional.

11.8.3. Entre os principais componentes normalmente presentes em ambientes dessa natureza destacam-se estruturas como servidores virtuais responsáveis pela publicação das aplicações, pools de servidores de aplicação, nós de infraestrutura, políticas de segurança associadas ao firewall de aplicações web, perfis de tráfego, regras de persistência de sessão e mecanismos de customização utilizados para tratamento específico de conexões e requisições.

11.8.4. Esses elementos constituem a base operacional da infraestrutura de entrega de aplicações, sendo responsáveis pela distribuição de tráfego entre os servidores de aplicação, pela inspeção de requisições HTTP/HTTPS e pela aplicação de políticas de segurança voltadas à proteção das aplicações institucionais.

11.8.5. Em ambientes corporativos que operam soluções de ADC/WAF há vários anos, é comum que essas estruturas sejam progressivamente ajustadas e aprimoradas ao longo do tempo, à medida que novas aplicações são disponibilizadas, políticas de segurança são implementadas e requisitos operacionais são incorporados ao ambiente.

11.8.6. A solução atualmente em operação baseia-se na versão TMOS 10.2.4, classificada como *End of Life (EoL)*, não recebendo atualizações ou correções de segurança desde 2015, com suporte do fabricante encerrado em dezembro de 2014.
11.8.7. Essa condição expõe o ambiente a vulnerabilidades conhecidas (CVEs) amplamente documentadas e potencialmente exploráveis, comprometendo a segurança das aplicações institucionais.
11.8.8. O ambiente atual apresenta alto grau de complexidade operacional, composto por aproximadamente:

11.8.8.1. 125 (cento e vinte e cinco) Virtual Servers;

11.8.8.2. 122 (cento e vinte e dois) Pools de aplicação;

11.8.8.3. 111 (cento e onze) regras avançadas de tratamento de tráfego (*iRules*).

11.8.9. Tal volume de configurações evidencia um ambiente significativamente customizado, cuja lógica operacional foi construída e refinada ao longo dos anos.

11.8.10. A eventual substituição por solução de fabricante distinto implicaria elevado esforço de migração, especialmente em razão da necessidade de reimplementação das regras, políticas e mecanismos de customização atualmente existentes no ambiente.

11.8.11. Tal cenário se torna ainda mais crítico considerando que essas customizações foram desenvolvidas ao longo dos anos para atender requisitos específicos das aplicações institucionais, exigindo validação técnica detalhada em caso de reescrita ou adaptação.
11.8.12. A solução de ADC atualmente implantada constitui ponto central de publicação das aplicações institucionais para a internet, sendo responsável pela disponibilização de diversos sistemas críticos do CNPq.
11.8.13. Dessa forma, eventuais falhas, indisponibilidades ou inconsistências na solução impactariam simultaneamente múltiplos serviços institucionais essenciais, ampliando significativamente o risco operacional.

11.8.14. Nesse contexto, a substituição completa da plataforma atualmente utilizada por solução de fabricante distinto implicaria a necessidade de reimplementação integral dessas estruturas e configurações, incluindo:

11.8.14.1. recriação das estruturas de publicação de aplicações;
11.8.14.2. reimplementação das políticas de balanceamento de carga;
11.8.14.3. reconfiguração das políticas de segurança de aplicações web (WAF);
11.8.14.4. adaptação de integrações existentes com a infraestrutura institucional;
11.8.14.5. validação completa do funcionamento das aplicações após a migração.

11.8.15. Esse processo demandaria etapas adicionais de planejamento, testes, validações e ajustes operacionais, podendo introduzir riscos de indisponibilidade temporária de aplicações institucionais ou inconsistências operacionais durante o período de estabilização da nova plataforma.

11.8.16. Considerando que a infraestrutura de balanceamento de aplicações do CNPq suporta serviços institucionais utilizados por servidores, pesquisadores e usuários externos, eventuais interrupções decorrentes de processos de migração tecnológica poderiam impactar diretamente a disponibilidade desses serviços, podendo resultar em comprometimento da confidencialidade, integridade e disponibilidade das informações institucionais.

11.8.17. Dessa forma, a adoção de solução compatível com a plataforma atualmente utilizada permite realizar a modernização da infraestrutura de forma mais controlada e com menor impacto operacional, reduzindo significativamente os riscos associados à migração tecnológica do ambiente.

11.8.18. Assim, a continuidade tecnológica da plataforma atualmente empregada no ambiente institucional mostra-se adequada para preservar a estabilidade operacional da infraestrutura de aplicações, ao mesmo tempo em que possibilita a atualização tecnológica da solução de forma planejada e segura.

11.9. CURVA DE APRENDIZADO E CONHECIMENTO TÉCNICO ACUMULADO

11.9.1. A equipe técnica do CNPq responsável pela administração da infraestrutura de aplicações possui experiência consolidada na operação da plataforma atualmente utilizada.

11.9.2. Esse conhecimento acumulado ao longo dos anos permite maior agilidade na identificação e resolução de incidentes, bem como na implementação de ajustes operacionais necessários para garantir a estabilidade do ambiente.

11.9.3. A adoção de solução tecnológica distinta implicaria na necessidade de novos processos de capacitação, adaptação operacional e estabilização do ambiente, o que poderia impactar negativamente a capacidade de resposta a incidentes e a continuidade operacional dos serviços.

11.9.4. Nesse contexto, a continuidade tecnológica também contribui para a redução da curva de aprendizado e para maior eficiência operacional.

11.10. PROVA DE CONCEITO (PoC) - POC

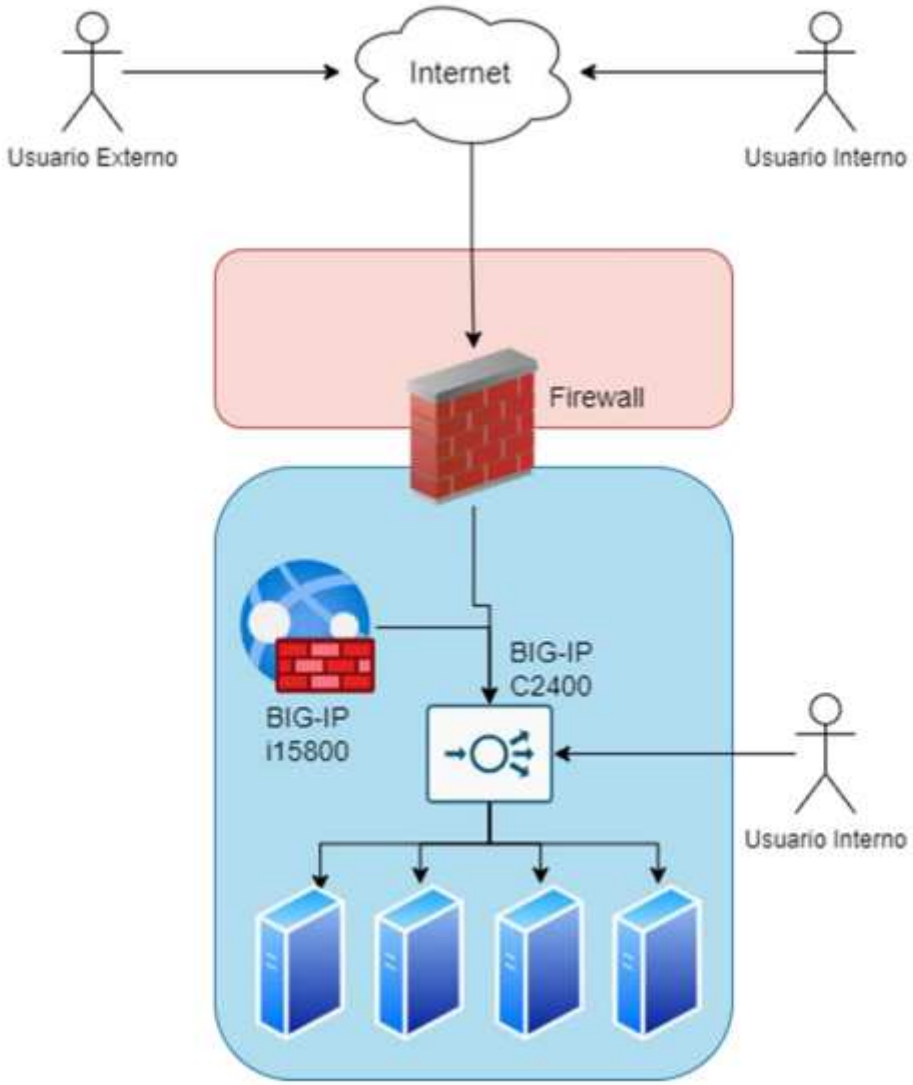
11.10.1. Com o objetivo de validar, em ambiente controlado, a aderência técnica da solução proposta às necessidades institucionais do CNPq, foi realizada Prova de Conceito (PoC) com a utilização de appliance da plataforma F5 BIG-IP, modelo i5800.

11.10.2. A PoC foi conduzida no período de 08/01/2026 a 23/03/2026, contemplando a instalação on-site do equipamento, configuração da solução e execução de testes com aplicações reais do ambiente institucional.

11.10.3. Para viabilizar a execução dos testes sem impacto à operação do ambiente produtivo, o appliance BIG-IP i5800 foi implantado em arquitetura One-Arm, posicionado na VLAN interna do data center institucional.

11.10.4. Nessa topologia, o equipamento existente (VIPRION C2400) permaneceu responsável pelas funções atuais de balanceamento de carga e publicação de aplicações, enquanto o appliance da PoC foi utilizado especificamente para inspeção e proteção das aplicações selecionadas.

11.10.5. O fluxo de tráfego foi estruturado de forma que as requisições destinadas às aplicações em teste fossem encaminhadas ao módulo de segurança (WAF) da solução avaliada, retornando posteriormente ao ambiente produtivo, conforme ilustrado na topologia definida para a PoC.



11.10.6. Foram selecionadas 4 (quatro) aplicações institucionais para participação na PoC:

11.10.6.1. buscatextual.cnpq.br

11.10.6.2. sei.cnpq.br

11.10.6.3. powerbi.cnpq.br

11.10.6.4. glpi.cnpq.br

11.10.7. A aplicação Currículo Lattes, por sua criticidade, foi deliberadamente excluída do escopo da PoC, a fim de mitigar riscos operacionais.

11.10.8. Para cada aplicação, foi realizada a criação de:

11.10.8.1. 01 (um) Virtual Server (VS);

11.10.8.2. 01 (uma) política dedicada de Web Application Firewall (WAF).

11.10.9. As políticas de segurança foram inicialmente configuradas em modo Transparent, permitindo o aprendizado automático do comportamento das aplicações e reduzindo a incidência de falsos positivos.

11.10.10. Após período de aproximadamente uma semana de aprendizagem, as políticas foram ajustadas para o modo Blocking, mediante execução controlada em janela de mudança.

11.10.11. Durante a configuração das políticas, foram habilitados mecanismos de:

11.10.11.1. aprendizado (Learn);

11.10.11.2. alerta (Alarm);

11.10.11.3. bloqueio (Block), para assinaturas de ataque.

11.10.12. Para outros parâmetros de segurança (CSRF Protection, Headers, Cookies, File Types e Content Profiles), optou-se majoritariamente por modos de aprendizado e alerta, com o objetivo de maximizar a visibilidade sobre o comportamento das requisições.

11.10.13. Adicionalmente, foram adaptadas regras de tratamento de tráfego (*iRules*) para viabilizar redirecionamentos e ajustes de fluxo, sendo contabilizadas:

11.10.13.1. 8 (oito) regras no ambiente de PoC;

11.10.13.2. 72 (setenta e duas) regras no ambiente produtivo existente.

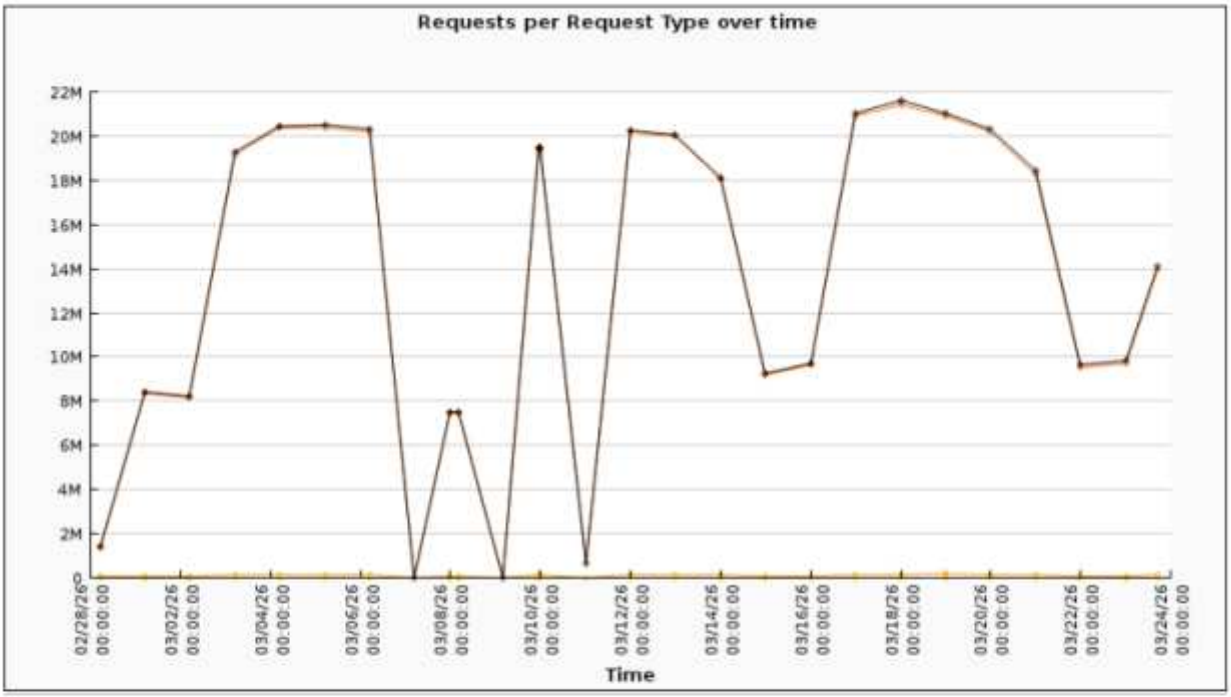
11.10.14. Durante o período de execução da PoC, foi observado volume significativo de tráfego, mesmo sem a inclusão da aplicação mais crítica do ambiente institucional. Destaca-se que, das 4 aplicações avaliadas 2 estavam expostas à internet e 2 eram de uso interno.

11.10.15. Ainda assim, foi registrada quantidade relevante de requisições e eventos de segurança, evidenciando o nível de exposição das aplicações institucionais.

11.10.16. Os gráficos a seguir apresentam análises complementares da telemetria coletada pelo módulo de segurança da solução, permitindo avaliação estruturada do comportamento do tráfego e dos eventos de segurança.

Gráfico 1 - Quantidade de Requests por Tipo

Viewing statistics from 02/27/26 22:00 to 03/23/26 17:07



Request Type	Legal Requests	Illegal Requests	▼ Requests
Legal	364095119	0	364095119
Alarmed	0	2522903	2522903
Blocked	0	5116	5116
Overall	364095119	2528019	366623138

Total Entries: **3**

11.10.17. Este relatório apresenta a distribuição do tráfego com base na classificação das requisições:

11.10.17.1. Legal: requisições válidas conforme políticas;

11.10.17.2. Illegal: requisições que violam políticas de segurança.

11.10.18. As requisições ilegais foram classificadas em:

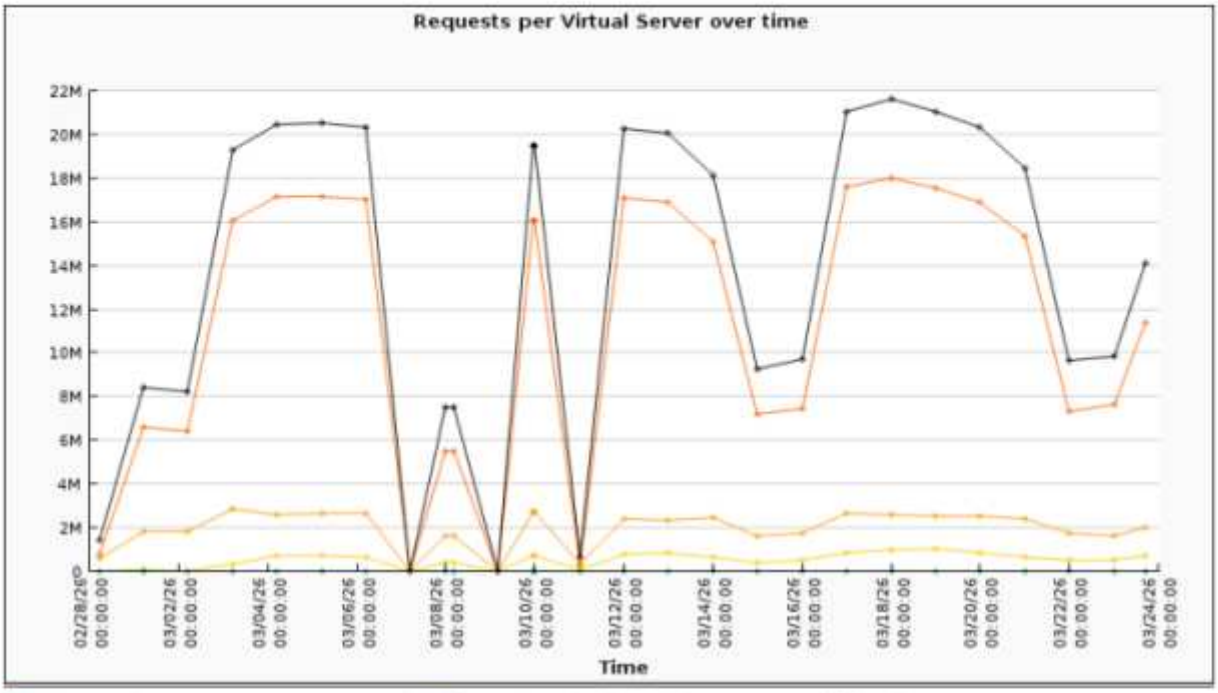
11.10.18.1. bloqueadas (Blocked);

11.10.18.2. apenas alertadas (Alarmed), conforme estratégia adotada na PoC.

11.10.19. A análise permite identificar padrões de comportamento anômalo e avaliar a efetividade das políticas de segurança.

Gráfico 2 - Quantidade de Requests por Virtual Server

Viewing statistics from 02/27/26 22:00 to 03/23/26 17:07



Virtual Server	Legal Requests	Illegal Requests	▼ Requests
Aggregated	299213854	722576	299936430
/Common/vs_buscatextual.cnpq.br_https	50606077	1785596	52391673
/Common/vs_buscatextual.cnpq.br_redirect	14137721	11692	14149413
/Common/vs_webmail.cnpq.br_https	130838	8023	138861
/Common/vs_glpi.cnpq.br_https	5068	132	5200
/Common/vs_powerbi.cnpq.br_https	1561	0	1561
Overall	364095119	2528019	366623138

Total Entries: **6**

11.10.20. Este relatório segmenta o tráfego por aplicação, permitindo identificar:

11.10.20.1. volume de requisições por serviço;

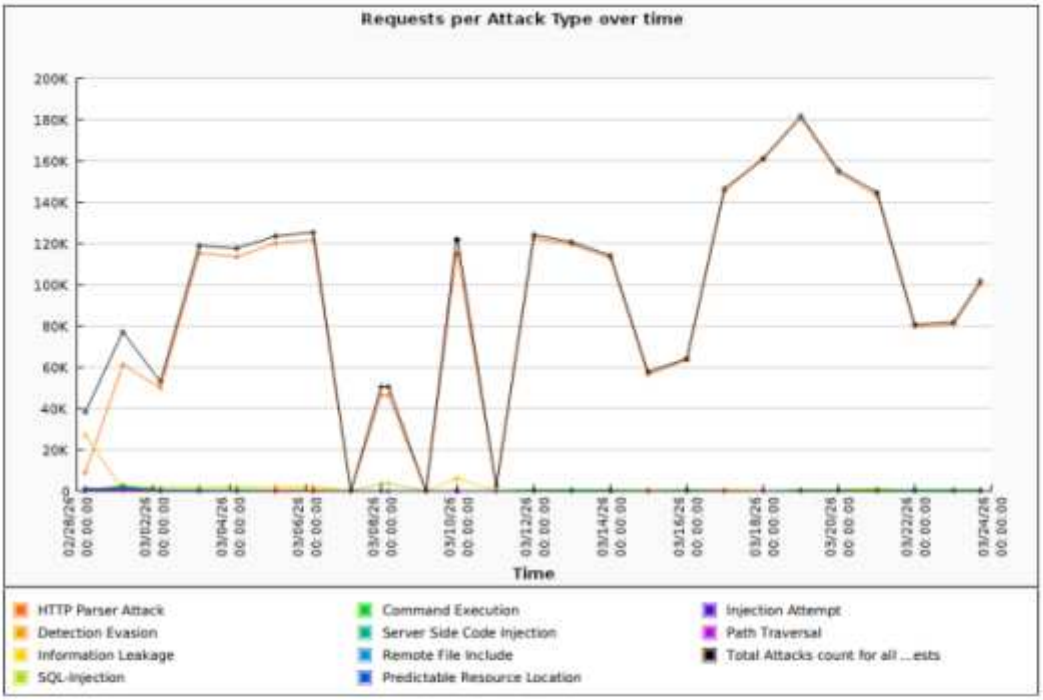
11.10.20.2. nível de exposição a tentativas de ataque.

11.10.21. Observou-se que a aplicação Busca Textual apresentou maior volume de requisições ilegais, indicando maior exposição a tentativas de exploração.

11.10.22. Destaca-se também a ocorrência de requisições maliciosas em aplicações internas, evidenciando risco mesmo em ambientes não expostos diretamente à internet.

Gráfico 3 - Quantidade de Requests por Tipo de Ataque

Viewing statistics from 02/27/26 22:00 to 03/23/26 17:07



Attack Type	▼ Requests
HTTP Parser Attack	2435124
Detection Evasion	31100
Information Leakage	30121
SQL-Injection	11019
Command Execution	8743
Server Side Code Injection	5001
Remote File Include	2079
Predictable Resource Location	2013
Injection Attempt	2004
Path Traversal	1986
Total Attacks count for all requests	2534093

Displaying **10** out of total **25** entries

11.10.23. Este relatório categoriza os eventos de segurança por tipo de ataque detectado.

11.10.24. Foram identificados, entre outros:

11.10.24.1. HTTP Parser Attacks (scanners e bots automatizados);

11.10.24.2. Detection Evasion;

11.10.24.3. Information Leakage;

11.10.24.4. SQL Injection;

11.10.24.5. Command Execution.

11.10.25. O volume de ataques evidencia não apenas atividades de reconhecimento, mas também tentativas efetivas de exploração de vulnerabilidades.

11.10.26. Durante a PoC, foram registrados diversos eventos de segurança, incluindo tentativas reais de exploração.

11.10.27. Entre os principais achados, destacam-se:

11.10.27.1. Tentativas de Information Leakage, utilizando métodos HTTP como OPTIONS e PROPFIND, evidenciando exposição de superfície de ataque;

11.10.27.2. Tentativas de SQL Injection, com uso de técnicas de evasão (mixed case, encoding e comentários inline), devidamente bloqueadas pela solução;

11.10.27.3. Tentativas de Command Execution e Path Traversal, com indicativos de malware e comunicação com servidores externos de comando e controle.

11.10.28. Em cenários sem proteção adequada, tais requisições poderiam resultar em comprometimento total dos servidores de aplicação.

11.10.29. A PoC demonstrou, de forma prática, a capacidade da solução em:

11.10.29.1. proteger aplicações contra ataques reais;

11.10.29.2. identificar e classificar eventos de segurança com alto nível de granularidade;

11.10.29.3. permitir monitoramento detalhado por aplicação;

11.10.29.4. aplicar políticas de segurança com diferentes níveis de atuação (permitir, alertar, bloquear).

11.10.30. Foram plenamente atendidos os critérios de sucesso definidos para a validação da solução, incluindo:

11.10.30.1. implementação de políticas de WAF por aplicação;

11.10.30.2. capacidade de monitoramento de tráfego e eventos;

11.10.30.3. geração de alertas e visibilidade operacional;

11.10.30.4. identificação precisa de vetores de ataque.

11.10.31. Os resultados obtidos evidenciam a aderência técnica da solução às necessidades institucionais, bem como sua capacidade de operar em ambiente real com aplicações críticas.

11.10.32. A inclusão da Prova de Conceito neste Estudo Técnico Preliminar reforça a fundamentação técnica da solução, reduz incertezas quanto à sua adoção e contribui para maior segurança na tomada de decisão administrativa.

11.11. POSICIONAMENTO DA SOLUÇÃO NO MERCADO DE TECNOLOGIA

11.11.1. Diversas empresas independentes de pesquisa e consultoria em tecnologia da informação publicam relatórios periódicos analisando fornecedores e soluções voltadas à entrega e segurança de aplicações. Esses estudos são amplamente utilizados por organizações públicas e privadas como referência para avaliação de maturidade tecnológica e posicionamento de mercado.

11.11.2. Nesse contexto, destacam-se os seguintes estudos e relatórios de mercado:

11.11.2.1. A empresa Enterprise Management Associates (EMA), líder em pesquisa e consultoria de tecnologia da informação e gerenciamento de dados, apresentou durante o evento RSA Conference 2023 o relatório denominado *Vendor Vision Report*. Nesse estudo são destacados fabricantes considerados visionários no segmento de cibersegurança e segurança de aplicações. Entre os fornecedores destacados encontra-se a tecnologia de segurança de aplicações desenvolvida pela F5, evidenciando sua relevância e capacidade de inovação no setor.

11.11.2.2. A empresa Gartner, uma das principais organizações globais de análise e consultoria em tecnologia da informação, publica periodicamente relatórios e estudos destinados a orientar organizações na escolha de tecnologias e fornecedores estratégicos. Em análises voltadas ao segmento de segurança de aplicações, a Gartner destaca a importância de tecnologias como *Web Application Firewall* (WAF) e *Application Delivery Controllers* (ADC) para proteção e otimização de aplicações corporativas. Essas tecnologias são consideradas componentes essenciais para a proteção de aplicações web e APIs, sendo amplamente adotadas em ambientes corporativos de missão crítica.

11.11.2.3. Adicionalmente, relatórios do tipo Magic Quadrant elaborados pela Gartner avaliam fornecedores com base em critérios como capacidade de execução e visão estratégica. Nesse contexto, soluções da fabricante F5 têm sido posicionadas ao longo dos anos no quadrante de líderes no segmento de *Application Delivery Controllers* e *Web Application Firewalls*, evidenciando sua maturidade tecnológica e ampla adoção em ambientes corporativos.

11.11.2.4. A empresa *Forrester Research*, organização internacional de pesquisa de mercado e consultoria em tecnologia, publicou o relatório *The Forrester Wave™: Web Application Firewalls, Q3 2022*, no qual foram avaliados diversos fornecedores de soluções de firewall de aplicações web com base em 24 critérios técnicos e estratégicos, incluindo funcionalidades, estratégia de produto e presença de mercado. Nesse relatório, a solução F5 BIG-IP Advanced WAF foi classificada entre as principais do

mercado, sendo reconhecida por sua estratégia tecnológica, robustez funcional e presença consolidada no mercado de segurança de aplicações.

11.11.2.5. Estudos de mercado e análises comparativas adicionais sobre soluções de proteção de aplicações indicam que a plataforma F5 BIG-IP oferece funcionalidades avançadas de gerenciamento de tráfego em camadas L4 e L7, aceleração criptográfica, balanceamento inteligente de aplicações e integração com mecanismos de segurança voltados à proteção contra ameaças direcionadas às aplicações e APIs.

11.11.3. Diante dos estudos e análises apresentados por organizações independentes de pesquisa e consultoria em tecnologia, observa-se que as soluções da fabricante F5 figuram entre as plataformas mais consolidadas e reconhecidas no segmento de entrega e proteção de aplicações corporativas, sendo amplamente utilizadas por organizações públicas e privadas em ambientes de missão crítica.

11.11.4. Esse posicionamento reforça a adequação da tecnologia para atendimento aos requisitos institucionais do CNPq, especialmente no que se refere a:

11.11.4.1. proteção de aplicações web e APIs;
11.11.4.2. otimização de desempenho e entrega de aplicações;
11.11.4.3. alta disponibilidade e resiliência da infraestrutura de serviços digitais;
11.11.4.4. maturidade tecnológica e evolução contínua da plataforma.

11.11.5. Dessa forma, os estudos de mercado analisados corroboram a escolha da solução baseada na plataforma F5 BIG-IP, evidenciando tratar-se de tecnologia amplamente consolidada e reconhecida no mercado de segurança e entrega de aplicações.



Figura 1 - Quadrante Mágico do Gartner

11.12. COMPETITIVIDADE DO MERCADO E AUSÊNCIA DE RESTRIÇÃO À CONCORRÊNCIA

11.12.1. Ressalta-se que a escolha da tecnologia não implica restrição à competitividade do processo licitatório.

11.12.2. O mercado nacional possui diversas empresas integradoras e revendedoras autorizadas aptas a fornecer equipamentos e serviços associados à tecnologia escolhida.

11.12.3. Conforme verificado no portal de parceiros da própria fabricante F5, existem diversos parceiros autorizados no Brasil capazes de comercializar, implantar e prestar suporte às soluções da plataforma, garantindo ampla competitividade no processo de contratação.

11.12.4. A relação de parceiros autorizados pode ser consultada no portal oficial do fabricante F5 através do link: *https://www.f5.com/pt_br/partners/find-a-partner?partnerLocation=Brazil&partnerPage=1*

11.12.5. Dessa forma, a definição da solução tecnológica baseia-se em critérios técnicos relacionados à continuidade do ambiente, padronização tecnológica e redução de riscos operacionais, sem prejuízo à ampla concorrência entre os potenciais fornecedores da solução.

11.13. COMPARATIVO TÉCNICO ENTRE FABRICANTES

11.13.1. Para subsidiar a análise técnica apresentada neste Estudo Técnico Preliminar, foi realizada avaliação comparativa entre soluções corporativas de Application Delivery Controller (ADC) com funcionalidades de balanceamento de carga e Web Application Firewall (WAF) disponíveis no mercado.

11.13.2. Foram consideradas plataformas amplamente presentes em contratações públicas e ambientes corporativos, incluindo soluções dos fabricantes F5 Networks, Citrix, A10 Networks, Fortinet e Radware, identificados a partir de consultas a contratações públicas, documentação técnica e estudos de mercado.

11.13.3. A análise comparativa considerou critérios técnicos e operacionais relevantes para o contexto do ambiente tecnológico do CNPq, incluindo:

11.13.3.1. balanceamento de carga L4/L7;
11.13.3.2. operação em cluster e alta disponibilidade;
11.13.3.3. offload de SSL/TLS;
11.13.3.4. WAF integrado à solução;
11.13.3.5. suporte corporativo e atualizações;
11.13.3.6. compatibilidade com a arquitetura atual do CNPq;
11.13.3.7. reaproveitamento de políticas e configurações existentes;
11.13.3.8. impacto de substituição tecnológica;
11.13.3.9. risco operacional durante migração;
11.13.3.10. curva de aprendizado da equipe técnica.

CRITÉRIO TÉCNICO	F5 BIG-IP	Citrix ADC	A10 Thunder ADC	Fortinet ADC	Radware
Balanceamento de carga L4/L7 corporativo	Atende	Atende	Atende	Atende	Atende
WAF integrado à solução	Atende	Atende	Atende	Atende	Atende
Operação em cluster / alta disponibilidade	Atende	Atende	Atende	Atende	Atende
Suporte corporativo e atualizações de software	Atende	Atende	Atende	Atende	Atende

Compatibilidade com a arquitetura atual do CNPq	Alta	Parcial	Parcial	Parcial	Parcial
Reaproveitamento de políticas de balanceamento existentes	Alto	Baixo	Baixo	Baixo	Baixo
Reaproveitamento de políticas de segurança/WAF existentes	Alto	Baixo	Baixo	Baixo	Baixo
Impacto de substituição tecnológica no ambiente atual	Menor	Maior	Maior	Maior	Maior
Risco operacional durante migração	Menor	Maior	Maior	Maior	Maior
Curva de aprendizado da equipe técnica	Menor	Maior	Maior	Maior	Maior
Tempo estimado de estabilização pós-implantação	Menor	Maior	Maior	Maior	Maior

11.13.4. A análise demonstra que as plataformas avaliadas possuem capacidade técnica para atender às funcionalidades básicas de balanceamento de carga e proteção de aplicações web.

11.13.5. Entretanto, quando considerado o contexto específico do ambiente tecnológico do CNPq, a plataforma atualmente utilizada apresenta vantagens relevantes nos seguintes aspectos:

11.13.5.1. Padronização tecnológica: A manutenção da plataforma atualmente utilizada preserva o padrão tecnológico existente no ambiente institucional, facilitando atividades de gestão, operação e monitoramento da infraestrutura.

11.13.5.2. Redução de riscos operacionais: A continuidade da tecnologia utilizada evita a necessidade de migração completa das políticas de balanceamento, regras de segurança, objetos e scripts atualmente implementados, reduzindo riscos de indisponibilidade durante o processo de atualização tecnológica.

11.13.5.3. Aproveitamento da experiência da equipe técnica: A equipe responsável pela operação da solução já possui experiência consolidada na administração da plataforma atualmente utilizada, permitindo maior eficiência na resolução de incidentes e na implementação de melhorias.

11.13.6. A substituição da plataforma atualmente utilizada por solução de fabricante distinto implicaria reengenharia significativa do ambiente de balanceamento e segurança de aplicações.

11.13.7. Entre as atividades necessárias nesse cenário destacam-se:

11.13.7.1. recriação das políticas de balanceamento de carga existentes;
11.13.7.2. recriação de regras de segurança e políticas de proteção de aplicações web;
11.13.7.3. adaptação de integrações com sistemas institucionais;
11.13.7.4. revisão ou reescrita de scripts e customizações existentes;
11.13.7.5. testes extensivos de validação e homologação;
11.13.7.6. período de estabilização da nova solução após implantação.

11.13.8. Considerando que o ambiente de balanceamento de aplicações do CNPq suporta serviços institucionais críticos operando em regime contínuo (24x7), tais atividades aumentariam significativamente o risco operacional associado à migração tecnológica.

11.13.9. Assim, embora existam múltiplas soluções tecnicamente capazes no mercado, conclui-se que a continuidade com a plataforma atualmente utilizada apresenta maior alinhamento com os princípios da eficiência, segurança operacional, continuidade do serviço público e mitigação de riscos associados à migração tecnológica.

11.13.10. Diante dos aspectos técnicos, operacionais e estratégicos apresentados, conclui-se que a solução que melhor atende às necessidades do CNPq consiste na modernização da plataforma de balanceamento de aplicações baseada na tecnologia atualmente utilizada, por meio da aquisição de nova infraestrutura corporativa de *Application Delivery Controller* (ADC), com funcionalidades integradas de balanceamento de carga de aplicações e firewall de aplicações web (WAF), baseada na plataforma F5 BIG-IP.

11.13.11. A adoção dessa alternativa permite:

11.13.11.1. preservar a padronização tecnológica do ambiente institucional;
11.13.11.2. reduzir riscos associados à migração de plataforma;
11.13.11.3. aproveitar o conhecimento técnico acumulado pela equipe institucional;
11.13.11.4. garantir elevados níveis de disponibilidade, segurança e desempenho para as aplicações institucionais.

11.13.12. Diante das análises técnicas, operacionais e de mercado apresentadas neste Estudo Técnico Preliminar, conclui-se que a alternativa mais adequada para atendimento da necessidade institucional do CNPq consiste na aquisição de solução corporativa de *Application Delivery Controller* (ADC) no modelo *on-premise*, com funcionalidades integradas de balanceamento de carga em camadas 4 e 7 (L4/L7) e firewall de aplicações web (WAF).

11.13.13. A solução deverá ser composta por *appliances* operando em arquitetura de alta disponibilidade (cluster), com licenciamento, subscrição de segurança, garantia e suporte técnico do fabricante durante todo o período contratual, bem como serviços especializados necessários à implantação, configuração e apoio técnico pós-implantação.

11.13.14. Considerando os requisitos técnicos, operacionais e de segurança apresentados ao longo deste estudo, bem como a necessidade de continuidade tecnológica e padronização do ambiente institucional, registra-se que a solução escolhida corresponde à seguinte alternativa: *Aquisição de solução ADC corporativa on-premise baseada na plataforma F5 BIG-IP, com funcionalidades integradas de balanceamento de carga e proteção de aplicações web (WAF), em arquitetura de alta disponibilidade.*

11.13.15. Essa solução permitirá assegurar:

11.13.15.1. elevada disponibilidade dos serviços digitais do CNPq;
11.13.15.2. proteção das aplicações institucionais contra ameaças direcionadas;
11.13.15.3. melhor desempenho na entrega de aplicações;
11.13.15.4. padronização e continuidade da infraestrutura tecnológica existente;
11.13.15.5. redução de riscos operacionais associados à migração de plataforma.

11.13.16. Dessa forma, conclui-se que a solução proposta atende de maneira adequada aos requisitos técnicos, operacionais e de segurança identificados neste Estudo Técnico Preliminar, estando alinhada aos princípios da eficiência, economicidade, continuidade do serviço público e segurança da informação.

11.13.17. A escolha da solução observa o disposto nos art. 41, inciso I da Lei nº 14.133/2021, no que se refere à padronização tecnológica e à justificativa técnica da solução adotada.

11.14. ANÁLISE COMPARATIVA DE CUSTOS

11.14.1. O Custo Total de Propriedade (*Total Cost of Ownership – TCO*) é instrumento utilizado para análise dos custos diretos e indiretos envolvidos ao longo do ciclo de vida da solução de TIC, abrangendo não apenas o custo inicial de aquisição, mas também os custos relacionados à implantação, suporte técnico, garantia, atualização e sustentação da solução durante a vigência contratual.

11.14.2. No presente caso, a análise comparativa de custos considerou a alternativa tecnicamente viável selecionada neste Estudo Técnico Preliminar, qual seja, a contratação de solução corporativa de *Application Delivery Controller* (ADC) com funcionalidades integradas de *Web Application Firewall* (WAF), em modelo *on-premise*, composta por *appliances* em arquitetura de alta disponibilidade, com serviços associados de implantação e suporte técnico especializado.

11.14.3. As alternativas consideradas inviáveis na etapa de análise comparativa de soluções não foram submetidas à análise detalhada de custo total de propriedade, tendo em vista que não atendem adequadamente aos requisitos técnicos, operacionais e de segurança definidos pelo CNPq, nos termos já registrados neste Estudo Técnico Preliminar.

11.14.4. Para fins de composição do custo total estimado da solução selecionada, foram considerados os seguintes componentes principais da contratação:

11.14.4.1. *appliances de Application Delivery Controller* (ADC) com funcionalidades integradas de *Web Application Firewall* (WAF), destinados à operação em arquitetura de alta disponibilidade, bem como o respectivo licenciamento da solução, as subscrições de segurança e a garantia com suporte técnico oficial do fabricante durante todo o período contratual;

11.14.4.2. serviços especializados de instalação, configuração, implantação e entrada em produção da solução;

11.14.4.3. apoio técnico especializado pós-implantação, sob demanda;

11.14.4.4. suporte técnico especializado complementar à garantia do fabricante, incluindo atividades preventivas, corretivas e evolutivas.

11.14.5. A pesquisa de preços utilizada para subsidiar a estimativa do custo total da contratação foi elaborada em conformidade com o art. 23 da Lei nº 14.133/2021 e com o art. 5º da Instrução Normativa SEGES/ME nº 65/2021, admitindo a utilização combinada ou não dos parâmetros disponíveis para formação da cesta de preços aceitáveis.

11.14.6. Para composição da estimativa de custo, foram considerados, quando cabíveis, valores obtidos a partir de contratações similares realizadas por outros órgãos e entidades da Administração Pública, dados extraídos de sistemas oficiais de compras e contratações públicas e pesquisa direta com fornecedores.

11.14.7. A memória de cálculo detalhada, bem como os documentos comprobatórios das fontes utilizadas, constam na Nota Técnica de pesquisa de preços (SEI n° 2752922), vinculada ao presente processo de contratação.

11.14.8. A estimativa do custo total da contratação foi realizada mediante a multiplicação dos quantitativos definidos neste Estudo Técnico Preliminar pelos respectivos valores unitários médios apurados na pesquisa de preços. A consolidação desses valores encontra-se apresentada na Tabela abaixo.

ITEM	DESCRIÇÃO	QUANTIDADE	UNIDADE DE MEDIDA	VALOR UNITÁRIO	VALOR TOTAL ESTIMADO
1	Appliance físico de Application Delivery Controller (ADC) com funcionalidades integradas de Web Application Firewall (WAF)	2	Unidade	R$ 704.871,29	**R$ 1.409.742,58**
2	Licenciamento da solução de ADC/WAF	2	Unidade	R$ 522.396,45	**R$ 1.044.792,90**
3	Garantia e suporte técnico oficial do fabricante da solução por 60 meses	2	Unidade	R$ 770.832,49	**R$ 1.541.664,98**
4	Subscrições e assinaturas de segurança da solução por 60 meses	2	Unidade	R$ 468.107,56	**R$ 936.215,12**
5	Serviços especializados de instalação, configuração e implantação	1	Serviço	R$ 259.951,25	**R$ 259.951,25**
6	Serviços de consultoria técnica especializada (sob demanda)	480	Hora	R$ 572,00	**R$ 274.560,00**
7	Serviços de suporte técnico especializado da solução em regime 24x7	60	Mês	R$ 9.655,73	**R$ 579.343,80**
VALOR TOTAL ESTIMADO DA CONTRATAÇÃO					**R$ 6.046.270,63**

11.14.9. A análise do custo total de propriedade da solução deve considerar que, além do custo direto dos equipamentos e serviços associados, a alternativa selecionada também apresenta vantagens econômicas indiretas relevantes, especialmente em razão de:

11.14.9.1. redução dos custos operacionais decorrentes da continuidade tecnológica da plataforma atualmente utilizada no ambiente do CNPq;

11.14.9.2. diminuição do esforço de migração, reconfiguração e reimplementação de políticas de balanceamento e segurança já existentes;

11.14.9.3. aproveitamento da experiência acumulada pela equipe técnica responsável pela administração da solução;

11.14.9.4. mitigação de riscos de indisponibilidade de aplicações institucionais durante processo de atualização tecnológica;

11.14.9.5. concentração, em uma única plataforma integrada, de funcionalidades de entrega de aplicações e proteção de aplicações web.

11.14.10. Nesse contexto, a solução escolhida apresenta melhor relação entre custo e benefício para a Administração, uma vez que combina aderência técnica, continuidade operacional, redução de riscos e racionalização de custos diretos e indiretos ao longo do ciclo de vida da solução.

11.14.11. Assim, a análise comparativa de custos (TCO) corrobora a escolha da solução selecionada neste Estudo Técnico Preliminar, demonstrando sua compatibilidade com os princípios da economicidade, eficiência, continuidade do serviço público e vantajosidade para a Administração Pública.

11.15. CÁLCULO DOS CUSTOS TOTAIS DE PROPRIEDADE (TCO)

Item	Descrição dos elementos de custos	Estimativa de TCO ao longo dos anos					Custo Total
		ANO 1	ANO 2	ANO 3	ANO 4	ANO 5	
1	Aquisição dos appliances de ADC/WAF	R$ 1.409.742,58	-	-	-	-	**R$ 1.409.742,58**
2	Licenciamento da solução	R$ 1.044.792,90	-	-	-	-	**R$ 1.044.792,90**
3	Garantia e suporte técnico oficial do fabricante por 60 meses	R$ 308.332,99	R$ 308.332,99	R$ 308.332,99	R$ 308.332,99	R$ 308.332,99	**R$ 1.541.664,98**
4	Subscrições e assinaturas de segurança da solução por 60 meses	R$ 187.243,02	R$ 187.243,02	R$ 187.243,02	R$ 187.243,02	R$ 187.243,04	**R$ 936.215,12**
5	Serviços especializados de instalação, configuração e implantação	R$ 259.951,25	-	-	-	-	**R$ 259.951,25**
6	Serviços de consultoria técnica especializada	R$ 54.912,00	R$ 54.912,00	R$ 54.912,00	R$ 54.912,00	R$ 54.912,00	**R$ 274.560,00**
7	Serviços de suporte técnico especializado 24x7	R$ 115.868,76	R$ 115.868,76	R$ 115.868,76	R$ 115.868,76	R$ 115.868,76	**R$ 579.343,80**
TOTAL		**R$ 3.380.843,50**	**R$ 666.356,77**	**R$ 666.356,77**	**R$ 666.356,77**	**R$ 666.356,82**	**R$ 6.046.270,63**

12. Descrição da solução de TIC a ser contratada

12.1. Diante das análises realizadas neste Estudo Técnico Preliminar, verificou-se que a alternativa mais adequada para atendimento da demanda institucional consiste na ***contratação de solução corporativa de Application Delivery Controller (ADC), baseada na plataforma F5 BIG-IP, com funcionalidades integradas de Web Application Firewall (WAF), a ser instalada em ambiente on-premise no data center do CNPq, contemplando o fornecimento dos appliances, do respectivo licenciamento da solução, da garantia e suporte técnico oficial do fabricante, das subscrições e assinaturas de segurança, bem como dos serviços especializados de instalação, configuração e implantação, suporte técnico especializado da contratada em regime 24x7 e serviços de consultoria técnica especializada sob demanda, pelo prazo de 60 (sessenta) meses.***

ITEM	DESCRIÇÃO	QUANTIDADE	UNIDADE DE MEDIDA
1	Appliance de *Application Delivery Controller* (ADC) baseada na plataforma F5 BIG-IP, com funcionalidades integradas de *Web Application Firewall* (WAF)	2	Unidade
2	Licenças de software F5 BIG-IP	2	Unidade
3	Garantia e suporte técnico oficial do fabricante da solução	2	Unidade
4	Subscrições e assinaturas de segurança da solução F5 BIG-IP	2	Unidade
5	Serviços especializados de instalação, configuração e implantação da solução	1	Serviço
6	Serviços de consultoria técnica especializada (sob demanda)	480	Hora
7	Serviços de suporte técnico especializado da contratada em regime 24x7	60	Mês

12.2. A solução deverá ser composta por *appliances* dedicados de alto desempenho, projetados especificamente para processamento avançado de tráfego de aplicações, operando em arquitetura de alta disponibilidade (cluster), de modo a assegurar continuidade operacional, resiliência da infraestrutura e elevada disponibilidade dos serviços digitais disponibilizados pela instituição.

12.3. A plataforma deverá prover funcionalidades avançadas de entrega, otimização e proteção de aplicações, incluindo, entre outras capacidades:

12.3.1. balanceamento de carga de aplicações em camadas L4 e L7;
12.3.2. inspeção e processamento de tráfego criptografado SSL/TLS, com suporte a *offload* criptográfico;
12.3.3. proteção de aplicações web por meio de *Web Application Firewall* (WAF);
12.3.4. mitigação de ataques comuns a aplicações web, incluindo vulnerabilidades amplamente documentadas em padrões como o OWASP Top 10 e ameaças direcionadas a APIs;
12.3.5. monitoramento de disponibilidade de serviços por meio de mecanismos de *health checks* e persistência de sessão;
12.3.6. gerenciamento avançado de tráfego e otimização de conexões entre clientes e servidores de aplicação;
12.3.7. integração com ferramentas institucionais de monitoramento, auditoria e registro de eventos de segurança.

12.4. A solução deverá operar de forma integrada à infraestrutura de rede e segurança atualmente existente no ambiente tecnológico do CNPq, permitindo sua implantação no perímetro do data center institucional e atuando como componente central na arquitetura de entrega e proteção de aplicações.

12.5. A adoção de solução desse tipo apresenta diversas vantagens para o ambiente institucional, entre as quais se destacam:

12.5.1. maior controle sobre dados e infraestrutura, em conformidade com as políticas institucionais de segurança da informação;
12.5.2. redução de latência no acesso às aplicações institucionais, uma vez que o processamento de tráfego ocorre localmente no data center do órgão;

12.5.3. maior aderência à arquitetura de segurança existente, permitindo integração com mecanismos já implementados de proteção de rede e monitoramento;
12.5.4. elevada disponibilidade dos serviços digitais, por meio de operação em arquitetura redundante e mecanismos automáticos de *failover*;
12.5.5. capacidade de escalabilidade e evolução da infraestrutura de aplicações, acompanhando o crescimento das demandas institucionais.

12.6. Adicionalmente, plataformas de *Application Delivery Controller* com funcionalidades de *Web Application Firewall* são amplamente utilizadas em ambientes de missão crítica de organizações públicas e privadas, sendo reconhecidas como tecnologias consolidadas para otimização da entrega de aplicações, melhoria de desempenho e fortalecimento da segurança de aplicações expostas à internet.

12.7. Dessa forma, a solução proposta permitirá modernizar a infraestrutura de entrega e proteção de aplicações do CNPq, contribuindo para o fortalecimento da segurança da informação, para a melhoria da disponibilidade dos serviços institucionais e para a sustentação da evolução tecnológica do ambiente computacional da instituição.

12.8. JUSTIFICATIVA PARA O NÃO PARCELAMENTO DA SOLUÇÃO

12.8.1. Nos termos do art. 47 da Lei nº 14.133/2021, o parcelamento do objeto constitui regra geral nas contratações públicas, sempre que tecnicamente viável e economicamente vantajoso para a Administração.

12.8.2. Entretanto, o mesmo dispositivo legal admite exceções quando o parcelamento comprometer a funcionalidade, a integração, a padronização ou a eficiência do objeto contratado.

12.8.3. No caso da presente contratação, verificou-se que o parcelamento do objeto não se mostra tecnicamente adequado, em razão das características intrínsecas da solução pretendida.

12.8.4. A solução de entrega e proteção de aplicações objeto desta contratação caracteriza-se como plataforma tecnológica integrada, composta por hardware, software, licenciamento, subscrições, suporte técnico e serviços especializados de implantação e operação.

12.8.5. Os componentes dessa solução operam de forma interdependente, compartilhando recursos computacionais, mecanismos de processamento de tráfego e funcionalidades avançadas de segurança e gerenciamento.

12.8.6. Entre os elementos que integram essa arquitetura destacam-se:

12.8.6.1. mecanismos de balanceamento de carga de aplicações em camada 4 e camada 7;
12.8.6.2. inspeção e processamento de tráfego criptografado SSL/TLS;
12.8.6.3. firewall de aplicações web (WAF);
12.8.6.4. mecanismos de proteção contra ataques automatizados e negação de serviço;
12.8.6.5. gerenciamento centralizado da solução;
12.8.6.6. integração com sistemas de monitoramento, auditoria e observabilidade.

12.8.7. Essas funcionalidades são implementadas de forma nativamente integrada nas plataformas modernas de *Application Delivery Controller*, compartilhando recursos internos de processamento e mecanismos comuns de inspeção de tráfego.

12.8.8. A eventual separação desses componentes em diferentes fornecedores ou soluções tecnológicas distintas poderia resultar em impactos negativos relevantes, entre os quais se destacam:

12.8.8.1. perda de integração nativa entre os mecanismos de balanceamento de carga e segurança de aplicações;
12.8.8.2. aumento da complexidade operacional do ambiente tecnológico;
12.8.8.3. maior dificuldade na identificação e resolução de incidentes;
12.8.8.4. aumento do tempo de resposta em situações de indisponibilidade;
12.8.8.5. maior esforço administrativo na gestão contratual e técnica de múltiplos fornecedores;
12.8.8.6. risco de incompatibilidade entre soluções de diferentes fabricantes.

12.8.9. Adicionalmente, a fragmentação da solução poderia comprometer funcionalidades avançadas que dependem da integração entre os componentes da plataforma, tais como:

12.8.9.1. inspeção de tráfego criptografado associada a políticas de segurança de aplicações;
12.8.9.2. aplicação coordenada de políticas de balanceamento e segurança;
12.8.9.3. compartilhamento de informações de sessão entre mecanismos de entrega e proteção de aplicações;
12.8.9.4. operação centralizada de logs, telemetria, auditoria e eventos de segurança.

12.8.10. Dessa forma, a divisão do objeto em múltiplos itens independentes poderia comprometer a integridade funcional da solução, reduzindo sua eficiência operacional e aumentando riscos de indisponibilidade.

12.8.11. Embora, para fins de planejamento da contratação, da pesquisa de preços e da formação do orçamento estimado, os componentes da solução tenham sido individualizados em itens distintos, trata-se de uma plataforma tecnológica integrada, cujos elementos operam de forma interdependente e são necessários ao pleno funcionamento da solução.

12.8.12. Nesse contexto, a contratação integrada da solução mostra-se mais adequada para garantir:

12.8.12.1. pleno funcionamento da arquitetura tecnológica;
12.8.12.2. simplificação da gestão contratual;
12.8.12.3. maior eficiência na operação e suporte da solução;
12.8.12.4. redução de riscos operacionais associados à integração de múltiplas tecnologias.

12.8.13. Assim, conclui-se que o parcelamento do objeto não se mostra técnica nem operacionalmente viável, razão pela qual a contratação deverá ocorrer de forma integrada, contemplando todos os componentes necessários ao pleno funcionamento da solução.

13. Estimativa de custo total da contratação

Valor (R$): 6.046.270,63

13.1. A Tabela a seguir representa o custo total máximo estimado para esta contratação.

ITEM	DESCRIÇÃO	QUANTIDADE	UNIDADE DE MEDIDA	VALOR UNITÁRIO	VALOR TOTAL ESTIMADO
1	Appliance de *Application Delivery Controller* (ADC) baseada na plataforma F5 BIG-IP, com funcionalidades integradas de *Web Application Firewall* (WAF)	2	Unidade	R$ 704.871,29	**R$ 1.409.742,58**
2	Licenças de software F5 BIG-IP	2	Unidade	R$ 522.396,45	**R$ 1.044.792,90**
3	Garantia e suporte técnico oficial do fabricante da solução	2	Unidade	R$ 770.832,49	**R$ 1.541.664,98**
4	Subscrições e assinaturas de segurança da solução F5 BIG-IP	2	Unidade	R$ 468.107,56	**R$ 936.215,12**
5	Serviços especializados de instalação, configuração e implantação da solução	1	Serviço	R$ 259.951,25	**R$ 259.951,25**
6	Serviços de consultoria técnica especializada (sob demanda)	480	Hora	R$ 572,00	**R$ 274.560,00**
7	Serviços de suporte técnico especializado da contratada em regime 24x7	60	Mês	R$ 9.655,73	**R$ 579.343,80**
VALOR TOTAL ESTIMADO DA CONTRATAÇÃO					**R$ 6.046.270,63**

14. Justificativa técnica da escolha da solução

14.1. Conforme apresentado nas seções anteriores deste Estudo Técnico Preliminar, a escolha da solução tecnológica para modernização da infraestrutura de entrega e proteção de aplicações do CNPq levou em consideração os requisitos institucionais de segurança da informação, disponibilidade dos serviços digitais, desempenho das aplicações e continuidade operacional do ambiente computacional.

14.2. O ambiente tecnológico do CNPq hospeda diversas aplicações institucionais críticas, acessadas por servidores, pesquisadores e usuários externos. Nesse contexto, torna-se essencial a utilização de mecanismos especializados capazes de garantir a disponibilidade, a integridade e a proteção dessas aplicações contra ameaças direcionadas a ambientes web.

14.3. Considerando o cenário atual de crescimento de ataques cibernéticos voltados a aplicações web e APIs, torna-se necessário adotar soluções tecnológicas capazes de realizar inspeção avançada de tráfego, balanceamento inteligente de conexões e proteção contra vulnerabilidades exploradas em aplicações expostas à internet.

14.4. Nesse contexto, as plataformas de *Application Delivery Controller* (ADC) com funcionalidades integradas de *Web Application Firewall* (WAF) são amplamente utilizadas em ambientes corporativos e governamentais para garantir a distribuição eficiente de tráfego entre servidores de aplicação e a proteção contra ataques direcionados às aplicações.

14.5. Para proteção adequada do ambiente de aplicações institucionais, faz-se necessário que a solução adotada seja capaz de:

14.5.1. realizar balanceamento de carga em camadas 4 e 7 (L4/L7), permitindo a distribuição inteligente de tráfego entre múltiplos servidores de aplicação;

14.5.2. realizar inspeção e processamento de tráfego criptografado (SSL/TLS), garantindo visibilidade e controle sobre conexões seguras;

14.5.3. identificar e bloquear ataques comuns a aplicações web, incluindo vulnerabilidades amplamente documentadas em padrões como o OWASP Top 10 e ameaças direcionadas a APIs;

14.5.4. prover mecanismos avançados de monitoramento e análise de tráfego, permitindo maior visibilidade sobre o comportamento das aplicações e usuários;

14.5.5. operar em arquitetura de alta disponibilidade, assegurando continuidade dos serviços digitais mesmo em cenários de falha de componentes da infraestrutura.

14.6. Outro fator relevante considerado na escolha da solução refere-se à continuidade operacional dos serviços institucionais. A interrupção ou degradação da disponibilidade das aplicações institucionais pode impactar diretamente a prestação de serviços digitais do CNPq, ocasionando prejuízos operacionais e institucionais.

14.7. Nesse sentido, soluções de ADC/WAF operando em arquitetura redundante e com mecanismos automáticos de *failover* permitem garantir níveis adequados de disponibilidade e resiliência da infraestrutura, reduzindo riscos de indisponibilidade de aplicações críticas.

14.8. Adicionalmente, a adoção de solução baseada em *appliances* dedicados instalados no data center institucional (modelo *on-premise*) permite maior controle sobre a infraestrutura tecnológica, maior aderência às políticas institucionais de segurança da informação e melhor integração com os mecanismos de proteção e monitoramento já existentes no ambiente do CNPq.

14.9. Outro aspecto considerado na definição da solução foi a compatibilidade com a arquitetura tecnológica atualmente existente no ambiente institucional, permitindo preservar padrões operacionais já consolidados, reduzir riscos associados à migração tecnológica e aproveitar o conhecimento técnico acumulado pela equipe responsável pela administração da infraestrutura.

14.10. O ambiente atualmente em operação no CNPq encontra-se baseado na plataforma F5 BIG-IP, amplamente utilizada para execução de políticas de balanceamento de carga, segurança de aplicações e tratamento avançado de tráfego, incluindo a utilização de configurações específicas, perfis de aplicação e regras customizadas (*iRules*), que compõem a lógica de funcionamento das aplicações institucionais.

14.11. A eventual substituição por solução de fabricante distinto implicaria a necessidade de reengenharia completa do ambiente, incluindo:

14.11.1. recriação de políticas de balanceamento de carga e segurança;

14.11.2. reescrita de regras customizadas (*iRules*) em linguagens e modelos proprietários distintos;

14.11.3. reconfiguração de perfis de aplicação, certificados digitais e políticas de inspeção;

14.11.4. validação integral de compatibilidade com sistemas institucionais;

14.11.5. execução de novos ciclos de testes funcionais, de desempenho e de segurança.

14.12. Tais atividades implicariam aumento significativo da complexidade da implantação, elevação do esforço operacional da equipe técnica, ampliação do tempo de estabilização do ambiente e incremento dos riscos de indisponibilidade de sistemas críticos.

14.13. Adicionalmente, a adoção de solução distinta da atualmente utilizada acarretaria perda da continuidade tecnológica, com impacto direto sobre:

14.13.1. o conhecimento técnico acumulado pela equipe interna;

14.13.2. a padronização operacional do ambiente;

14.13.3. a eficiência na operação, troubleshooting e resposta a incidentes;

14.13.4. a integração com sistemas e ferramentas já existentes no ecossistema tecnológico do CNPq.

14.14. Ressalta-se que a plataforma F5 BIG-IP é amplamente consolidada no mercado, sendo adotada por diversos órgãos da Administração Pública e instituições que operam ambientes de missão crítica, o que reforça sua aderência aos requisitos institucionais de disponibilidade, desempenho e segurança.

14.15. Nesse contexto, a manutenção da mesma linha tecnológica, com atualização da infraestrutura para versões mais recentes e suportadas pelo fabricante, permite:

14.15.1. reduzir significativamente os riscos de migração tecnológica;

14.15.2. preservar as configurações existentes e a lógica de funcionamento das aplicações;

14.15.3. acelerar o processo de implantação e entrada em produção;

14.15.4. otimizar a curva de aprendizagem e operação da equipe técnica;

14.15.5. garantir maior previsibilidade operacional e estabilidade do ambiente.

14.16. Sob a perspectiva técnica e operacional, a continuidade da utilização da plataforma F5 BIG-IP, por meio de sua atualização tecnológica, apresenta-se como a alternativa que melhor equilibra desempenho, segurança, integração e mitigação de riscos, quando comparada à adoção de soluções de fabricantes distintos.

15. Justificativa econômica da escolha da solução

15.1. A análise econômica da solução proposta considerou não apenas o custo direto de aquisição da infraestrutura tecnológica, mas também os aspectos relacionados ao custo total de propriedade (*Total Cost of Ownership – TCO*), incluindo fatores como manutenção, suporte técnico, riscos operacionais, continuidade dos serviços, esforço de migração tecnológica e custos indiretos associados à operação do ambiente.

15.2. Nesse contexto, verificou-se que a adoção de solução corporativa de *Application Delivery Controller* (ADC) com funcionalidades integradas de *Web Application Firewall* (WAF), instalada em ambiente on-premise no data center institucional, apresenta melhor relação entre custo e benefício para o CNPq, especialmente quando considerada a continuidade tecnológica da plataforma atualmente utilizada.

15.3. A escolha dessa alternativa permite concentrar em uma única plataforma tecnológica as funcionalidades de balanceamento de carga de aplicações, proteção de aplicações web e gerenciamento avançado de tráfego, reduzindo a necessidade de aquisição, integração e operação de múltiplas soluções independentes, o que implicaria aumento de custos de licenciamento, infraestrutura, suporte e operação.

15.4. Adicionalmente, a eventual substituição da plataforma atualmente utilizada no ambiente do CNPq, baseada na tecnologia F5 BIG-IP, por solução de fabricante distinto implicaria custos indiretos relevantes, não imediatamente evidentes na fase de aquisição, mas com impacto significativo ao longo do ciclo de vida da solução, tais como:

15.4.1. necessidade de reimplementação de políticas de balanceamento de carga, segurança e entrega de aplicações;

15.4.2. recriação de configurações específicas de aplicações institucionais, incluindo perfis avançados de tráfego e regras customizadas (*iRules*);

15.4.3. custos adicionais de capacitação, treinamento e adaptação da equipe técnica a nova plataforma tecnológica;

15.4.4. necessidade de contratação de serviços especializados adicionais para migração e reconfiguração do ambiente;

15.4.5. esforço operacional elevado para estabilização do ambiente após a implantação de solução distinta;

15.4.6. aumento do tempo de implantação e, consequentemente, maior exposição a riscos operacionais durante o período de transição.

15.5. Tais fatores configuram custos indiretos relevantes que devem ser considerados na análise de vantajosidade econômica, uma vez que impactam diretamente o custo total de propriedade da solução ao longo de sua vida útil.

15.6. Nesse contexto, a manutenção da mesma linha tecnológica atualmente adotada, por meio da atualização da plataforma F5 BIG-IP, permite significativa redução desses custos indiretos, ao:

15.6.1. preservar as configurações existentes e reduzir a necessidade de retrabalho técnico;

15.6.2. minimizar o esforço de migração e validação do ambiente;

15.6.3. aproveitar o conhecimento técnico acumulado pela equipe interna;

15.6.4. reduzir a dependência de serviços externos especializados para adaptação da solução;

15.6.5. acelerar o processo de implantação e entrada em operação;

15.6.6. diminuir o risco de indisponibilidade de aplicações críticas durante a transição tecnológica.

15.7. Outro fator relevante refere-se à redução de riscos operacionais, uma vez que a adoção de solução compatível com a arquitetura existente minimiza a probabilidade de falhas, indisponibilidades e incidentes de segurança durante o processo de atualização tecnológica, evitando custos associados à interrupção de serviços institucionais.

15.8. Adicionalmente, a contratação da solução com garantia e suporte técnico especializado do fabricante durante todo o período contratual assegura acesso contínuo a atualizações de software, correções de segurança e suporte técnico qualificado, contribuindo para a preservação da estabilidade, segurança e desempenho do ambiente tecnológico.

15.9. Considerando que a infraestrutura de balanceamento de aplicações e proteção de aplicações web constitui componente essencial da arquitetura de serviços digitais do CNPq, eventuais falhas ou indisponibilidades podem gerar impactos operacionais e institucionais relevantes, o que reforça a necessidade de adoção de solução tecnológica consolidada, com menor risco operacional e maior previsibilidade de custos.

15.10. Dessa forma, ao considerar conjuntamente os custos diretos de aquisição, os custos operacionais ao longo do ciclo de vida da solução e, especialmente, os custos indiretos evitados pela continuidade tecnológica da plataforma atualmente utilizada, conclui-se que a alternativa baseada na atualização da solução F5 BIG-IP apresenta maior vantajosidade econômica para a Administração, atendendo aos princípios da economicidade, eficiência, continuidade do serviço público e interesse público.

16. Benefícios a serem alcançados com a contratação

16.1. A contratação da solução de *Application Delivery Controller* (ADC) com funcionalidades integradas de *Web Application Firewall* (WAF) permitirá ao CNPq modernizar sua infraestrutura de entrega e proteção de aplicações, proporcionando maior disponibilidade, desempenho e segurança para os serviços digitais disponibilizados pela instituição.

16.2. A adoção dessa solução contribui para fortalecer a arquitetura tecnológica do ambiente institucional, assegurando que as aplicações institucionais possam operar com níveis adequados de desempenho, resiliência e proteção contra ameaças direcionadas a aplicações web.

16.3. Adicionalmente, a solução permitirá maior visibilidade sobre o comportamento do tráfego de aplicações e maior capacidade de controle sobre o acesso aos serviços institucionais, contribuindo para a melhoria da governança da infraestrutura de tecnologia da informação.

16.4. A modernização da infraestrutura de balanceamento e proteção de aplicações também possibilita maior alinhamento com boas práticas de segurança da informação e continuidade de serviços, especialmente em ambientes que demandam elevada disponibilidade e operação contínua.

16.5. Destaca-se, adicionalmente, que a adoção de solução baseada na mesma linha tecnológica atualmente utilizada no ambiente do CNPq, notadamente a plataforma F5 BIG-IP, potencializa os benefícios da contratação, ao permitir:

16.5.1. reaproveitamento de configurações existentes, incluindo políticas de balanceamento, perfis de aplicação e regras customizadas (*iRules*);

16.5.2. redução do tempo de implantação e entrada em produção da nova solução;

16.5.3. minimização de riscos operacionais durante o processo de transição tecnológica;

16.5.4. preservação da padronização tecnológica do ambiente;

16.5.5. aproveitamento do conhecimento técnico já consolidado pela equipe responsável pela administração da plataforma;

16.5.6. maior eficiência na operação, monitoramento e resposta a incidentes.

16.6. De forma complementar, destacam-se, de maneira não exaustiva, alguns dos principais benefícios esperados com a contratação da solução:

16.6.1. aumento da disponibilidade e da resiliência das aplicações institucionais por meio de mecanismos de balanceamento de carga e alta disponibilidade;

16.6.2. melhoria do desempenho no acesso às aplicações institucionais, com distribuição inteligente de tráfego entre servidores de aplicação;

16.6.3. fortalecimento da segurança das aplicações web por meio da utilização de mecanismos especializados de *Web Application Firewall* (WAF);

16.6.4. proteção contra ataques direcionados a aplicações web, incluindo exploração de vulnerabilidades amplamente documentadas em padrões como o OWASP Top 10 e ameaças voltadas a APIs;

16.6.5. maior visibilidade e controle sobre o tráfego de aplicações e comportamento das conexões de usuários;

16.6.6. melhoria na capacidade de monitoramento e diagnóstico de incidentes relacionados ao acesso e funcionamento das aplicações;

16.6.7. redução do risco de indisponibilidade de serviços institucionais decorrentes de falhas de infraestrutura ou sobrecarga de servidores;

16.6.8. maior aderência às políticas institucionais de segurança da informação e proteção de dados;

16.6.9. fortalecimento da governança da infraestrutura de tecnologia da informação do CNPq;

16.6.10. suporte à evolução tecnológica do ambiente institucional, permitindo maior escalabilidade e adaptação a novas demandas de serviços digitais.

16.7. Dessa forma, a contratação da solução proposta contribuirá para o fortalecimento da infraestrutura tecnológica do CNPq, garantindo melhores condições para a prestação de serviços digitais institucionais com níveis adequados de segurança, disponibilidade e desempenho.

16.8. Ressalta-se que os benefícios associados à continuidade da plataforma tecnológica atualmente utilizada refletem diretamente na redução de custos operacionais, na diminuição de riscos de indisponibilidade e na maior eficiência da gestão do ambiente, contribuindo para a obtenção de ganhos concretos e mensuráveis ao longo do ciclo de vida da solução.

17. Providências a serem Adotadas

17.1. Em atendimento à alínea “e”, Inciso II, art. 11, da IN SGD/ME n.º 94/2022, não serão necessárias providências para adequação do ambiente do órgão para viabilizar a execução contratual.

18. Declaração de Viabilidade

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

18.1. Justificativa da Viabilidade

18.1. Esta equipe de planejamento declara viável esta contratação.

18.2. JUSTIFICATIVA DA VIABILIDADE

18.2.1. Conforme descrito neste Estudo Técnico e no Documento de Formalização de Demanda, o CNPq necessita e possui condições de adquirir e operar a contratação ora apresentada.

19. Responsáveis

Todas as assinaturas eletrônicas seguem o horário oficial de Brasília e fundamentam-se no §3º do Art. 4º do Decreto nº 10.543, de 13 de novembro de 2020.

IRISLENISSON DE SOUZA OLIVEIRA

Integrante Requisitante

Assinou eletronicamente em 19/08/2026 às 14:18:50.

LEONARDO FABIANO SEGER

Integrante Técnico

Assinou eletronicamente em 19/08/2026 às 14:27:20.

gov.br
Documento assinado digitalmente
GERALDO SORTE
Data: 21/08/2026 15:28:50-0300
Verifique em https://validar.iti.gov.br

GERALDO SORTE

CONSELHO NACIONAL DE DESENVOLVIMENTO CIENTÍFICO E TECNOLÓGICO
COORDENAÇÃO DE GESTÃO DE DADOS E ARQUITETURA CORPORATIVA - CODAC/CGETI/DASD

ANEXO I

ESPECIFICAÇÃO TÉCNICA MÍNIMA DA SOLUÇÃO

1.1. A solução é composta por um cluster contendo 2 (dois) equipamentos do tipo Application Delivery Controller (ADC), com funcionalidades integradas de Web Application Firewall (WAF), estruturada nos seguintes componentes: fornecimento dos appliances, licenciamento da solução, garantia e suporte técnico oficial do fabricante, subscrições e assinaturas de segurança, serviços especializados de implantação, serviços de consultoria técnica especializada e serviços de suporte técnico especializado, todos técnica e funcionalmente integrados e indispensáveis à implantação, operação e sustentação da solução.

1.2. Para comprovação dos itens das especificações técnicas da solução, serão aceitos:

- **1.2.1.** Datasheets oficiais do fabricante;
- **1.2.2.** Documentação técnica oficial (manuais, guias, whitepapers);
- **1.2.3.** Cartas ou declarações do fabricante;
- **1.2.4.** Evidências extraídas da CLI (Command Line Interface);
- **1.2.5.** Documentação oficial disponível em portal do fabricante;
- **1.2.6.** Declaração formal do fabricante ou do licitante, nos casos em que o requisito não seja passível de comprovação por documentação pública.

Itens 1 a 4 – Requisitos Técnicos da Solução de Application Delivery Controller (ADC), com funcionalidades integradas de Web Application Firewall (WAF)	
1	**HARDWARE**
1.1	**REQUISITOS MÍNIMOS GERAIS**
1.1.1	A solução deverá ser composta por 2 (dois) dispositivos de hardware do tipo appliance, idênticos, capazes de operar em alta disponibilidade, utilizando os licenciamentos e componentes de software previstos nesta contratação.
1.1.2	Cada equipamento e sistema proposto deverá atender integralmente às características técnicas mínimas obrigatórias estabelecidas neste Anexo.
1.1.3	Os equipamentos deverão ser novos, de primeiro uso, estar em linha de fabricação na data da entrega, com a versão mais recente de software e/ou firmware disponível e serem comercializados pelo fabricante.

1.1.4	Os appliances deverão possuir altura máxima de 1U para instalação em rack padrão 19”, devendo ser fornecidos com todos os acessórios necessários à instalação.
1.1.5	Os equipamentos deverão possuir capacidade de processamento e memória suficientes para operar simultaneamente todas as funcionalidades contratadas, considerando o volume máximo de tráfego especificado.
1.1.6	Não serão aceitos equipamentos baseados em servidores genéricos ou sistemas operacionais de uso geral.
1.1.7	Os equipamentos deverão possuir, no mínimo, 1 (uma) interface de console dedicada para configuração via CLI (Command Line Interface).
1.1.8	A solução deverá suportar operação em alta disponibilidade, nos modos ativo-passivo e/ou ativo-ativo, garantindo a continuidade do processamento do tráfego em caso de falha de um dos equipamentos.
1.1.9	A solução de alta disponibilidade não deverá depender de protocolos de roteamento dinâmico, tais como BGP.
1.1.10	A solução deverá suportar mecanismos de balanceamento global de tráfego baseados em DNS, quando aplicável, sem prejuízo das funcionalidades principais de balanceamento local.
1.1.11	A solução deverá permitir a definição de políticas individualizadas por aplicação.
1.1.12	A solução deverá suportar integração com plataformas de orquestração de containers (tais como Kubernetes e OpenShift), por meio de APIs.
1.1.13	Todos os equipamentos deverão possuir certificações exigidas pela legislação brasileira aplicável, incluindo, quando pertinente, certificação da ANATEL em nome do fabricante.
1.1.14	Os equipamentos e softwares não poderão estar classificados como “End of Sale” (EOS) ou “End of Life” (EOL) até a data de abertura das propostas.
1.1.15	Por razões de compatibilidade, suporte, gerenciamento e garantia, todos os componentes da solução deverão ser do mesmo fabricante.
1.1.16	A solução deverá incluir todos os componentes necessários ao pleno funcionamento, incluindo elementos físicos, lógicos e de integração ao ambiente da CONTRATANTE.
1.1.17	Os equipamentos deverão possuir fonte de alimentação interna, com suporte às seguintes características: a) operação em tensão de 100 a 240V AC, com seleção automática; b) frequência de operação de 50/60 Hz; c) capacidade de operação plena com apenas uma fonte ativa; d) possibilidade de substituição sem interrupção do funcionamento; e) conexão a circuitos elétricos independentes; f) fornecimento de cabos de energia no padrão NBR 14.136.
1.1.18	Os equipamentos deverão operar em temperaturas entre 0°C e 40°C, com umidade relativa entre 5% e 85%, sem condensação.
1.1.19	A solução deverá ser fornecida completamente operacional, incluindo todos os elementos necessários à sua instalação, configuração e funcionamento.
1.1.20	Não será admitida a necessidade de desenvolvimento adicional para atendimento dos requisitos especificados.

1.1.21	Todas as funcionalidades deverão estar disponíveis na versão ofertada no momento da entrega da solução.
1.1.22	Não serão aceitas funcionalidades previstas apenas em roadmap do fabricante.
1.1.23	O appliance deve permitir a expansão de recursos de processamento e multitenância através de licenciamento de software possibilitando a evolução do modelo para classes superiores da mesma família sem a necessidade de substituição física do chassi.
1.1.24	A solução deve possuir uma camada de plataforma baseada em microserviços permitindo o isolamento total de recursos entre instâncias (tenants).
1.2	**DESEMPENHO DOS APPLIANCES**
1.2.1	A solução deverá suportar throughput SSL mínimo de 35 Gbps (trinta e cinco gigabits por segundo), considerando operações de balanceamento de carga com criptografia.
1.2.2	A solução deverá suportar, no mínimo, 75.000.000 (setenta e cinco milhões) de conexões simultâneas em camada 4.
1.2.3	A solução deverá suportar, no mínimo, 2.500.000 (dois milhões e quinhentas mil) requisições por segundo em camada 7, sem degradação de desempenho.
1.2.4	A solução deverá suportar, no mínimo, 1.000.000 (um milhão) novas conexões por segundo em camada 4, sem degradação de desempenho.
1.2.5	A solução deverá suportar, no mínimo, 60.000 (sessenta mil) transações SSL por segundo (TPS),considerando chaves RSA de 2.048 bits.
1.2.6	A solução deverá suportar, no mínimo, 750.000 (setecentas e cinquenta mil) conexões SSL simultâneas.
1.2.7	A solução deverá suportar, no mínimo, 30.000 (trinta mil) transações SSL por segundo utilizando chaves ECDSA P-256.
1.2.8	A solução deverá suportar, no mínimo, 35 Gbps de tráfego HTTP com compressão habilitada.
1.2.9	A solução deverá possuir throughput mínimo de 95 Gbps para balanceamento de carga em camada 4.
1.2.10	A solução deverá possuir throughput mínimo de 60 Gbps para balanceamento de carga em camada 7.
1.2.11	A solução deverá suportar, no mínimo, 2.500.000 (dois milhões e quinhentas mil) novas conexões por segundo em camada 7.
1.2.12	A solução deverá possuir mecanismos integrados de proteção contra ataques de negação de serviço (DoS e DDoS), incluindo, no mínimo, mitigação de ataques do tipo SYN Flood.
1.2.13	A solução deverá suportar capacidade de mitigação de ataques SYN Flood de, no mínimo 80.000.000 (oitenta milhões) de cookies por segundo.
1.2.14	A solução deve ser capaz de criar até 8 instâncias virtualizadas em cada appliance fornecido.
1.2.15	Os valores de desempenho (throughput e RPS) exigidos neste termo devem ser garantidos com a virtualização/multitenância ativa, não sendo aceita a degradação de performance por overhead de camada de virtualização ('virtualization tax').
1.2.16	O hardware deve utilizar tecnologia moderna de FPGA dedicada para mitigar mais de 100 vetores de ataque em hardware e realizar o offload de processamento UDP, evitando a exaustão dos recursos da CPU principal durante eventos de DDoS.
1.3	**INTERFACES (PARA CADA DISPOSITIVO DO PAR)**

1.3.1	A solução deverá suportar agregação de links utilizando o protocolo LACP (IEEE 802.3ad), permitindo a formação de grupos com, no mínimo, 2 (duas) interfaces por agregação.
1.3.2	A solução deverá suportar, no mínimo, 512 (quinhentas e doze) VLANs.
1.3.3	Todas as interfaces de rede deverão garantir isolamento lógico de comunicação entre si, conforme as políticas de configuração definidas.
1.3.4	A solução deverá suportar o transporte de múltiplas VLANs por uma única interface física ou grupo de interfaces agregadas, utilizando o padrão IEEE 802.1Q.
1.3.5	Cada equipamento deverá possuir, no mínimo 2 (duas) portas 100G/40G QSFP28 e 8 (oito) portas 25G/10G SFP28, fornecido com os respectivos transceivers, para uso com fibra óptica multimodo OM4, com conectores LC.
1.3.6	Cada equipamento deverá possuir, no mínimo, 1 (uma) interface de rede de 1 Gbps, do tipo1000BASE-T (RJ45), operando em full-duplex, sendo pelo menos 1 (uma) interface dedicada para gerenciamento.
1.3.7	Os transceptores ópticos, cabos de fibra e demais acessórios necessários à operação das interfaces deverão ser fornecidos, incluindo cabeamento óptico multimodo OM4 com comprimento de até 10 (dez) metros, conforme especificação da CONTRATANTE no momento da contratação.
1.3.8	A solução deverá suportar o encaminhamento de jumbo frames, com tamanho mínimo de 9.000 bytes, em todas as interfaces destinadas ao tráfego de dados.
1.3.9	Cada equipamento deverá possuir interface dedicada para acesso à console, podendo ser do tipo RS-232, USB ou RJ45, devendo ser fornecido o respectivo cabo compatível.
1.3.10	A solução deverá permitir a configuração de interfaces específicas para comunicação de alta disponibilidade (heartbeat), possibilitando a utilização de rede dedicada para essa finalidade.
1.3.11	O fornecimento deverá incluir todos os componentes necessários ao pleno funcionamento das interfaces, incluindo cabos, conectores, transceptores (SFP/SFP+) e demais acessórios.
2	**SOFTWARE**
2.1	O licenciamento da solução deverá garantir o pleno funcionamento de todas as funcionalidades contratadas durante toda a vigência do contrato.
2.2	Deverão estar incluídos no licenciamento: a) atualizações de software e firmware; b) atualizações de assinaturas e bases de inteligência; c) suporte técnico do fabricante; d) correções de segurança.
2.3	Após o término do período contratual, as funcionalidades que não dependam de atualizações periódicas deverão permanecer operacionais.
2.4	Todos os módulos, licenças e componentes necessários ao atendimento integral dos requisitos deste Anexo deverão estar incluídos na proposta, sem custos adicionais.

2.5	A solução deverá permitir gerenciamento centralizado dos dispositivos que compõem a infraestrutura.
2.6	A solução deverá suportar acesso seguro à gerência por meio de protocolos criptografados, incluindo SSH e HTTPS.
2.7	A solução deverá suportar operação em ambiente de alta disponibilidade.
2.8	A solução deverá possuir escalabilidade, permitindo expansão por meio da adição de novos appliances.
2.9	A solução deverá suportar sincronização de sessões entre dispositivos em alta disponibilidade, garantindo a continuidade das conexões em caso de falha.
2.10	A solução deverá suportar mecanismos de autenticação, autorização e auditoria (AAA), incluindo integração com MFA (autenticação multifator), quando aplicável.
2.11	A solução deverá permitir a definição de perfis de acesso para usuários e administradores.
2.12	A solução deverá suportar integração com serviços de diretório, incluindo LDAP seguro e Microsoft Active Directory.
2.13	A solução deverá possuir interface gráfica (GUI) acessível via navegador web, utilizando protocolo HTTPS.
2.14	A solução deverá permitir transferência segura de arquivos entre a estação de gerenciamento e os equipamentos.
2.15	A solução deverá permitir configuração baseada em perfis e templates, incluindo suporte a perfis hierárquicos.
2.16	A solução deverá permitir armazenamento de logs localmente e/ou em servidores externos.
2.17	A solução deverá suportar integração com servidores Syslog para armazenamento de longo prazo.
2.18	A solução deverá permitir retenção de logs por período mínimo de 365 (trezentos e sessenta e cinco) dias, considerando armazenamento externo.
2.19	A solução deverá suportar rotacionamento automático de logs com base em tempo e/ou tamanho.
2.20	A solução deverá possuir funcionalidades de geração de relatórios gerenciais e estatísticos, contendo, no mínimo: a) quantidade de acessos por servidor virtual; b) quantidade de acessos por serviços e servidores; c) quantidade de usuários conectados; d) quantidade de requisições por período; e) transações por segundo; f) tempo de latência (cliente e servidor); g) Throughput de tráfego; h) quantidade de sessões.
2.21	A solução deverá possuir relatórios em tempo real, incluindo, no mínimo: a) tempo de resposta da aplicação; b) latência de rede;

	c) conexões por servidor ou grupo de servidores; d) análise por URL.
2.22	A solução deverá permitir aplicação de filtros nos relatórios, incluindo, no mínimo: a) servidores virtuais; b) servidores balanceados; c) URLs; d) geolocalização (GEOIP); e) identificação de cliente (User-Agent).
2.23	A solução deverá permitir exportação de relatórios nos formatos HTML, PDF e CSV.
2.24	A solução deverá permitir geração de relatórios sob demanda e de forma automatizada, com base em eventos e thresholds configuráveis.
2.25	A solução deverá permitir acesso aos dados e relatórios por meio de API.
2.26	A solução deverá suportar monitoramento via SNMP, incluindo versões v2c e v3.
2.27	A solução deverá permitir integração com sistemas de gerenciamento de rede (NMS), incluindo fornecimento de MIBs.
2.28	A solução deverá suportar criptografia na comunicação entre seus componentes.
2.29	A solução deverá permitir backup e restauração de configurações e logs, de forma manual e automática.
2.30	A solução deverá permitir exportação e importação de configurações por meio de protocolos seguros, incluindo HTTPS, SFTP e SCP.
2.31	A solução deverá permitir sincronização de configurações entre dispositivos, de forma manual ou automática.
2.32	A solução deverá permitir reinicialização dos equipamentos por meio de interface gráfica ou linha de comando.
2.33	A solução deve suportar nativamente interfaces de configuração declarativas (API REST), permitindo o provisionamento completo de serviços (L4-L7) através de um único arquivo JSON, compatível com ferramentas de CI/CD (Ansible/Terraform).
2.34	A solução deve suportar roteamento dinâmico para IPv6 através dos protocolos BGP, OSPFv3 e RIPng, permitindo múltiplas tabelas de roteamento independentes.
2.35	A solução deverá permitir a criação de códigos ou scripts capazes de manipular o tráfego, incluindo descartar, redirecionar, alterar, substituir e comparar valores e atributos, a partir de informações extraídas da conexão, sessão e protocolos;
2.36	A solução deverá permitir utilizar listas de dados como fonte de dados por um script para validar se as conexões a serem estabelecidas obedecem a um dos critérios contidos nessa base de dados;
3	**TRÁFEGO SSL/TLS OFFLOADING**
3.1	A solução deverá implementar funcionalidades de SSL/TLS offload, incluindo Full Offload e Bridging.
3.2	A solução deverá ser capaz de realizar descriptografia de tráfego SSL/TLS independentemente da porta TCP utilizada.

3.3	A solução deverá suportar, no mínimo, os protocolos TLS 1.2 e TLS 1.3.
3.4	A solução deverá suportar verificação de certificados digitais de clientes e servidores.
3.5	A solução deverá suportar o protocolo OCSP para validação de certificados.
3.6	A solução deverá possuir aceleração criptográfica por hardware para operações SSL/TLS.
3.7	A solução deverá permitir configuração de parâmetros de sessão SSL/TLS.
3.8	A solução deverá suportar gerenciamento de tráfego criptografado entre cliente e servidor, incluindo recriptografia.
3.9	A solução deverá suportar Server Name Indication (SNI).
3.10	O hardware deve possuir aceleração dedicada para ciphers de Curva Elíptica (ECC), permitindo o escalonamento de Forward Secrecy sem impacto no processamento geral da aplicação.
4	**BALANCEAMENTO**
4.1	A solução deverá suportar balanceamento de carga nas camadas 4 a 7 do modelo OSI.
4.2	A solução deverá suportar, no mínimo, os seguintes algoritmos de balanceamento: a) Round Robin; b) Least Connections; c) Round Trip Time; d) Response Time; e) Weighted (por peso).
4.3	A solução deverá permitir balanceamento de novas sessões, preservando sessões existentes no mesmo servidor, por meio de mecanismos de persistência.
4.4	A solução deverá suportar, no mínimo, os seguintes métodos de persistência: a) inserção de cookie; b) uso de cookie da aplicação; c) endereço IP de origem; d) endereço IP de destino; e) sessão SSL; f) URL; g) parâmetros de cabeçalho HTTP; h) identificadores de aplicação (ex.: SIP Call ID); i) inspeção de conteúdo em camada 7.
4.5	A solução deverá suportar balanceamento de carga para, no mínimo, os seguintes protocolos: a) TCP; b) UDP;

	c) IP; d) DNS; e) HTTP e HTTPS; f) HTTP/2; g) FTP; h) SIP; i) RDP; j) RADIUS; k) MySQL e MSSQL; l) RTMP; m) RTSP.
4.6	A solução deverá suportar monitoramento de disponibilidade dos servidores reais (health check), incluindo, no mínimo: a) Camada 3: ICMP; b) Camada 4: TCP e UDP; c) Camada 7: protocolos de aplicação.
4.7	Deverá suportar monitoramento em camada 7 para, no mínimo: HTTP, HTTPS, FTP, RADIUS, SMTP, Microsoft SQL, Oracle, LDAP, IMAP, POP3, SIP e SNMP.
4.8	A solução deverá permitir limitação de sessões simultâneas por: a) servidor real; b) servidor virtual; c) grupo de servidores (pool); d) equipamento físico.
4.9	A solução deverá suportar Network Address Translation (NAT).
4.10	A solução deverá suportar criação de servidores virtuais com endereços IPv4 e servidores reais com endereços IPv6.
4.11	A solução deverá ter a capacidade de atuar como gateway de transição, suportando servidores virtuais IPv4 para servidores reais IPv6, bem como servidores virtuais IPv6 para servidores reais IPv4.
4.12	A solução deverá possuir mecanismos de proteção contra ataques de negação de serviço (DoS e DDoS), incluindo mitigação de ataques do tipo SYN Flood.
4.13	A solução deverá permitir compressão de conteúdo HTTP, incluindo suporte a algoritmos como gzip e deflate.
4.14	A solução deverá permitir definição de políticas de compressão por tipo de conteúdo.
4.15	A solução deverá suportar aceleração SSL, com terminação de sessões criptografadas no equipamento.
4.16	A solução deverá permitir criação de políticas de manipulação de tráfego por meio de interface gráfica.

4.17	As políticas deverão suportar, no mínimo, os seguintes critérios: a) Cliente (host); b) Sessão SSL; c) Cookie; d) Cabeçalho HTTP; e) URL; f) Geolocalização (GEOIP).
4.18	As políticas deverão permitir, no mínimo, as seguintes ações: a) bloqueio de tráfego; b) reescrita de URL; c) registro de eventos (log); d) inserção de cabeçalhos HTTP; e) redirecionamento de tráfego; f) aplicação de políticas específicas por aplicação.
4.19	A solução deverá registrar informações das sessões, incluindo, no mínimo: a) endereço IP de origem; b) porta de origem; c) endereço IP de destino; d) porta de destino; e) protocolo de transporte; f) data e hora; g) URL acessada.
4.20	A solução deverá suportar integração com plataformas de orquestração de containers (como Kubernetes e OpenShift), por meio de APIs.
4.21	A solução deverá permitir atualização dinâmica das configurações de balanceamento com base nas alterações do ambiente orquestrado.
4.22	A solução deverá suportar balanceamento de carga dinâmico em ambientes de containers.
4.23	A solução deverá fornecer estatísticas de tráfego nas camadas L4 a L7, compatíveis com ferramentas externas de análise.
4.24	A solução deverá suportar operação nos modos: a) Reverse Proxy; b) Transparente; c) WCCP/WCCPv2.
4.25	A solução deverá permitir redirecionamento automático do tráfego para servidores disponíveis, conforme políticas definidas, em caso de indisponibilidade de recursos.
5	**FIREWALL DE APLICAÇÃO WEB (WAF)**

5.1	A solução deverá ser capaz de identificar, isolar e bloquear ataques cibernéticos em camada de aplicação (camada 7), sem impactar negativamente o desempenho das aplicações protegidas.
5.2	A solução deverá prover proteção para aplicações web contra ameaças e ataques direcionados aos protocolos HTTP e HTTPS.
5.3	A solução deverá suportar modelo de segurança positivo (whitelisting), incluindo proteção baseada nas principais vulnerabilidades descritas no OWASP Top 10 (versão mais atual vigente).
5.4	A solução deverá permitir criação de políticas de segurança por aplicação e por URL.
5.5	A solução deverá permitir criação automática e/ou assistida de políticas de segurança com base em aprendizado de tráfego ou integração com ferramentas de análise de vulnerabilidades.
5.6	A solução deverá suportar proteção baseada em assinaturas atualizadas pelo fabricante.
5.7	As assinaturas deverão ser atualizadas durante toda a vigência contratual, sem custos adicionais.
5.8	A solução deverá possuir mecanismo de reputação de endereços IP, incluindo base de dados dinâmica atualizada automaticamente, tanto para IPv4 quanto para IPv6.
5.9	A solução deverá permitir classificação de reputação, incluindo, no mínimo: a) Origem de SPAM; b) Origem de ataques; c) Botnets; d) Proxies/VPN; e) Scanners.
5.10	A solução deverá permitir criação de listas de exceção (whitelist) e bloqueio (blacklist).
5.11	A solução ofertada deverá possuir funcionalidades nativas e mecanismos internos de proteção do mesmo fabricante, sem a necessidade de componentes de terceiros para atendimento deste requisito, capazes de identificar, bloquear, mitigar e registrar, no mínimo, os seguintes tipos de ataques: a) SQL Injection; b) Cross-Site Scripting (XSS); c) Cross-Site Request Forgery (CSRF); d) Buffer Overflow; e) Parameter Tampering; f) Cookie Poisoning; g) HTTP Request Smuggling; h) Sequestro de sessão; i) Força bruta; j) Ataques a APIs (JSON/XML);

	k) XML Bombs/DoS; l) Credential Stuffing.
5.12	A solução deverá suportar proteção contra ataques de negação de serviço (DoS/DDoS) em camada 7.
5.13	A solução deverá permitir criação de políticas baseadas em geolocalização (GEOIP).
5.14	A solução deverá permitir bloqueio automático de clientes que excedam limites configuráveis de requisições ou violações.
5.15	A solução deverá permitir definição de tempo de bloqueio configurável.
5.16	A solução deverá permitir criação de listas dinâmicas e estáticas de bloqueio e exceção.
5.17	A solução deverá implementar, no mínimo: a) validação de URLs; b) validação de métodos HTTP; c) validação de headers HTTP; d) validação de formulários; e) inspeção de payload; f) proteção contra vazamento de informações sensíveis.
5.18	A solução deverá suportar criptografia e proteção de cookies.
5.19	A solução deverá suportar detecção de clientes inválidos por meio de análise de User-Agent.
5.20	A solução deverá suportar mecanismos de proteção contra exposição de informações internas da aplicação (information leakage).
5.21	A solução deverá suportar integração com ferramentas de análise de vulnerabilidade.
5.22	A solução poderá suportar integração via ICAP ou possuir mecanismos nativos equivalentes para inspeção de conteúdo.
5.23	A solução deverá fornecer relatórios consolidados de segurança contendo, no mínimo: a) resumo geral de políticas e eventos; b) principais ataques; c) principais IPs de origem; d) tipos de ataques; e) violações de protocolo; f) URLs acessadas; g) geolocalização; h) severidade.
5.24	A solução deverá fornecer visualização gráfica dos eventos, incluindo, no mínimo: a) por política; b) por tipo de ataque; c) por URL;

	d) por endereço IP; e) por país; f) por severidade; g) por código de resposta HTTP.
5.25	A solução deverá permitir bloqueio automático de endereços IP com base em comportamento suspeito.
5.26	A solução deverá permitir desbloqueio manual ou automático de endereços IP.
5.27	A solução deverá permitir inclusão dinâmica de endereços IP em blacklist com base em eventos.
5.28	A solução deverá manter lista dinâmica de reputação global de IPs maliciosos, incluindo, no mínimo: a) Web Attacks; b) Botnets; c) Exploits; d) Scanners; e) DoS/DDoS; f) Proxies anônimos; g) Phishing; h) Reputação geral.
5.29	A solução deve implementar mitigação proativa de DoS comportamental (BaDoS) e proteção contra bots maliciosos em tempo real.
5.30	A solução deve implementar criptografia no nível do campo e ofuscação de dados sensíveis para prevenir vazamento de informações em camadas de erro.
5.31	A solução deve implementar funcionalidade para ocultar erros de aplicação ou infraestrutura do usuário.
5.32	A solução deve permitir a configuração de fluxo de navegação da aplicação, de forma que um usuário só pode alcançar determinada URL se passar por outras anteriormente.
5.33	Deve suportar acesso a serviços de terminais através de: a) Citrix XenApp; b) Citrix XenDesktop; c) Microsoft RDP; d) VMware Horizon View.
5.34	A solução deverá realizar federação através de SAML Artifact Binding onde a comunicação será direta entre o Identity Provider (IdP) e o Service Provider (SP).
5.35	A solução deverá atuar como gateway para o acesso MSRDP, deverá ser possível realizar autenticação via NTLM dos usuários, sem a necessidade de software adicional.
5.36	A Solução deverá permitir o uso de one-time passcode (OTP) como segundo fator de autenticação através da integração com RSA SecurID.

5.37	Deve implementar Bot Defense com análise comportamental e Machine Learning, diferenciando bots 'bons' de 'ruins' e mitigando web scraping avançado.
5.38	A solução deve oferecer proteção comportamental ilimitada contra ataques DoS em L7 por Servidor Virtual, com autoaprendizado da aplicação.
5.39	Deve possuir API Discovery automático para identificar Shadow APIs e validar schemas REST/GraphQL via importação de arquivos Swagger/OpenAPI.
5.40	Deve implementar criptografia de dados no navegador (DataSafe) para proteção contra keyloggers e malwares Man-in-the-Browser.
5.41	A arquitetura de segurança deve realizar a inspeção e mitigação de ameaças das camadas L3 a L7 em um único fluxo de processamento (one-pass), garantindo a menor latência possível para o tráfego legítimo.
5.42	A solução deve possuir proteção via hardware contra ataques de inundação (flood) de pacotes ICMPv6, fornecendo estatísticas detalhadas de descarte.
6	**BALANCEAMENTO GLOBAL (GLOBAL SERVER LOAD BALANCING)**
6.1	A solução deverá suportar balanceamento global de carga (GSLB), com base em resolução de nomes DNS.
6.2	A solução deverá suportar operação como: a) Servidor DNS autoritativo; b) Servidor DNS secundário; c) Servidor DNS cache; d) Balanceador de servidores DNS.
6.3	A solução deverá suportar DNSSEC.
6.4	A solução deverá suportar comunicação segura entre servidores DNS utilizando TSIG, com algoritmos como HMAC-SHA.
6.5	A solução deverá possuir mecanismos de proteção contra ataques DNS, incluindo, no mínimo: a) validação de protocolo; b) proteção contra UDP Flood; c) proteção contra pacotes malformados; d) proteção contra ataques de amplificação e reflexão DNS; e) proteção contra NXDOMAIN Flood; f) proteção contra cache poisoning.
6.6	A solução deverá suportar inspeção stateful de tráfego DNS.
6.7	A solução deverá suportar transferência de zona (zone transfer) entre servidores DNS.
6.8	A solução deverá ser capaz de responder consultas DNS com base em cache em memória.
6.9	A solução deverá suportar os seguintes tipos de registros DNS, no mínimo: a) SOA; b) A;

	c) AAAA; d) CNAME; e) MX; f) NS; g) PTR; h) SRV; i) TXT.
6.10	A solução deverá suportar políticas de distribuição de tráfego baseadas em: a) Geolocalização (GEOIP); b) Disponibilidade de servidores; c) Latência; d) Round Robin; e) Capacidade do serviço; f) Persistência baseada em cliente (LDNS ou IP).
6.11	A solução deverá permitir ajuste do número de endereços retornados nas respostas DNS.
6.12	A solução deverá permitir respostas baseadas em topologia, considerando localização geográfica ou origem da requisição.
6.13	A solução deverá suportar monitoramento de saúde de: a) Servidores; b) Serviços; c) Links de comunicação.
6.14	A solução deverá responder às consultas DNS apenas com endereços de serviços disponíveis.
6.15	A solução deverá suportar operação em alta disponibilidade.
6.16	A alta disponibilidade deverá ser baseada em mecanismos próprios da solução, não dependendo exclusivamente de protocolos de roteamento dinâmico.
6.17	A solução deverá permitir integração com a infraestrutura DNS existente, com impacto mínimo na arquitetura atual.
6.18	A solução deverá permitir operação de forma transparente ao ambiente existente.
6.19	A solução deverá possuir base de geolocalização de endereços IP atualizada.
6.20	A solução deverá implementar mecanismos de transição IPv6, incluindo a funcionalidade de DNS64.

Item 5 - Serviços especializados de instalação, configuração e implantação da solução	
7	**REQUISITOS**

7.1	A CONTRATADA deverá prestar serviços especializados de instalação, configuração e implantação da solução adquirida, abrangendo todos os seus componentes (hardware e software).
7.2	A CONTRATADA será responsável por todas as atividades logísticas necessárias à implantação, incluindo transporte, entrega, desembalagem e instalação dos equipamentos.
7.3	Os serviços deverão contemplar, no mínimo: a) montagem física dos equipamentos em rack; b) fornecimento e instalação de trilhos, cabos e acessórios; c) interligação física e lógica à rede da CONTRATANTE; d) instalação e configuração de todos os softwares necessários; e) parametrização completa da solução.
7.4	Os serviços deverão ser realizados em dias úteis, no horário de 08h às 17h, podendo, mediante acordo entre as partes, serem executados fora desse período.
7.5	A execução dos serviços deverá ser previamente agendada com a equipe técnica da CONTRATANTE.
7.6	A implementação deverá ser realizada por profissionais qualificados pelo fabricante da solução.
7.7	Todas as despesas relacionadas à execução dos serviços serão de responsabilidade da CONTRATADA.
7.8	A CONTRATADA deverá realizar visita técnica nas dependências da CONTRATANTE, no prazo de até 5 (cinco) dias corridos após a assinatura do contrato.
7.9	Como resultado da visita, deverá ser elaborado relatório técnico contendo, no mínimo: a) levantamento do ambiente; b) definição de posicionamento dos equipamentos; c) requisitos elétricos e de rede; d) recomendações técnicas para implantação.
7.10	A CONTRATADA deverá elaborar e apresentar Projeto Executivo para aprovação da CONTRATANTE.
7.11	O Projeto Executivo deverá conter, no mínimo: a) descrição da solução; b) pré-requisitos de instalação; c) relatório do site survey; d) cronograma de execução; e) arquitetura lógica; f) arquitetura física; g) políticas de configuração; h) plano de rollback; i) caderno de Testes e Homologação.

7.12	A CONTRATANTE terá prazo de até 5 (cinco) dias corridos para análise e aprovação do Projeto Executivo.
7.13	Caso necessário, a CONTRATADA deverá realizar ajustes no prazo de até 2 (dois) dias corridos.
7.14	A CONTRATADA deverá realizar análise do ambiente tecnológico existente, com base nas informações fornecidas pela CONTRATANTE.
7.15	A implantação deverá ser planejada de forma a não causar interrupções não programadas nos serviços.
7.16	A instalação física do equipamento deverá ser feita de forma presencial, por técnico qualificado pelo fabricante. As demais atividades de implantação poderão ser executadas remotamente, mas sendo obrigatoriamente executadas por técnicos qualificados pelo fabricante.
7.17	Caso necessário, as atividades deverão ser executadas em janelas de manutenção previamente acordadas, inclusive em horários não comerciais, sem custos adicionais.
7.18	A solução implantada não deverá causar degradação de desempenho no ambiente da CONTRATANTE.
7.19	A CONTRATADA será responsável pelo correto dimensionamento da solução.
7.20	Caso o desempenho da solução não atenda aos requisitos estabelecidos, a CONTRATADA deverá realizar os ajustes necessários, sem ônus adicional.
7.21	Após a implantação, a CONTRATADA deverá executar os testes previstos no Caderno de Testes e Homologação.
7.22	Os testes deverão ser acompanhados pela equipe técnica da CONTRATANTE.
7.23	Caso sejam identificadas falhas, a CONTRATADA deverá realizar as correções necessárias e repetir os testes.
7.24	A solução será considerada implantada após a conclusão satisfatória dos testes.
7.25	A homologação será iniciada após a conclusão da implantação.
7.26	Durante a homologação, não deverão ocorrer falhas ou interrupções.
7.27	Caso sejam identificadas divergências ou falhas, a CONTRATADA deverá realizar as correções necessárias.
7.28	A CONTRATADA terá prazo de até 10 (dez) dias úteis para correção, após notificação formal.
7.29	Ao final da implantação, a CONTRATADA deverá entregar documentação técnica completa (As-Built), contendo: a) arquitetura implementada; b) configurações realizadas; c) procedimentos executados; d) resultados dos testes; e) parâmetros da solução.
7.30	A conclusão dos serviços será atestada mediante entrega da solução em pleno funcionamento e da documentação técnica.
7.31	A CONTRATANTE possui um ambiente configurado utilizando solução F5 com diversas regras e proteções configuradas. A CONTRATADA deverá considerar no seu tempo de implantação e migração horas de forma a contemplar todo a instalação do ambiente, sem gerar custos adicionais a CONTRATANTE.

Item 6 - Serviços de consultoria técnica especializada	
8	**REQUISITOS**
8.1	Os serviços de consultoria técnica especializada têm por objetivo apoiar a CONTRATANTE na evolução, otimização e adequação da solução implantada, bem como no aprimoramento técnico da equipe responsável por sua operação e administração.
8.2	Os serviços serão prestados sob demanda, mediante emissão de Ordens de Serviço (OS) pela CONTRATANTE.
8.3	Cada Ordem de Serviço deverá conter, no mínimo: a) descrição das atividades a serem executadas; b) quantidade estimada de horas; c) prazo para execução; d) local de execução (remoto ou presencial); e) responsáveis técnicos.
8.4	Os serviços poderão ser prestados de forma presencial (onsite) ou remota, conforme a natureza da atividade.
8.5	A CONTRATADA deverá disponibilizar profissionais devidamente capacitados fabricante da solução.
8.6	Os serviços poderão abranger, mas não se limitar a: a) implementação de novas funcionalidades; b) ajustes e otimizações na configuração da solução; c) operação assistida, incluindo alocação de técnico dedicado; d) apoio técnico em troubleshooting e resolução de incidentes; e) consultoria para definição de arquitetura e melhores práticas; f) análise de compatibilidade com outras soluções; g) reconfiguração e adequação do ambiente.
8.7	Os serviços deverão ser executados preferencialmente em horário comercial (segunda a sexta-feira).
8.8	Quando houver necessidade de intervenção em ambiente de produção, os serviços poderão ser executados em janelas de manutenção previamente acordadas, sem custos adicionais.
8.9	A execução dos serviços será controlada por meio das seguintes etapas: a) emissão da Ordem de Serviço pela CONTRATANTE; b) acompanhamento da execução pela equipe técnica da CONTRATANTE; c) entrega de relatório técnico ao final da execução.
8.10	Ao término de cada Ordem de Serviço, a CONTRATADA deverá apresentar Relatório de Atividades contendo, no mínimo: a) descrição das atividades executadas; b) horas efetivamente utilizadas; c) resultados obtidos;

	d) evidências técnicas; e) recomendações, quando aplicável.
8.11	O pagamento dos serviços estará condicionado ao aceite do relatório pela CONTRATANTE.
8.12	A CONTRATADA deverá iniciar a execução dos serviços em até 7 (sete) dias corridos após a emissão da Ordem de Serviço.
8.13	Prazos distintos poderão ser definidos na própria Ordem de Serviço, mediante justificativa técnica.

Item 7 - Serviços de suporte técnico especializado da solução em regime 24x7	
9	**CONDIÇÕES GERAIS**
9.1	A CONTRATADA deverá prestar serviços de suporte técnico, manutenção e atualização da solução pelo período de 60 (sessenta) meses, contados a partir da emissão do Termo de Recebimento Definitivo.
9.2	O suporte técnico deverá ser prestado em regime 24 (vinte e quatro) horas por dia, 7 (sete) dias por semana, incluindo finais de semana e feriados.
9.3	A CONTRATADA deverá atender às solicitações da CONTRATANTE a qualquer tempo, respeitando os níveis de serviço estabelecidos neste Termo de Referência.
9.4	Somente serão aceitas licenças originais do fabricante para todos os componentes da solução.
9.5	Os serviços de suporte técnico deverão contemplar, no mínimo: a) atualização de versões de software e firmware; b) atualização de assinaturas e bases de inteligência; c) correção de falhas (bugs); d) aplicação de patches de segurança; e) apoio técnico para diagnóstico e resolução de incidentes; f) execução de testes de funcionamento e conectividade; g) apoio em ajustes de configuração; h) backup das configurações, quando necessário; i) disponibilização de documentação técnica atualizada.
9.6	As atualizações e correções deverão ser fornecidas sem ônus adicional durante toda a vigência contratual.
9.7	Novas versões de software disponibilizadas pelo fabricante deverão ser fornecidas em prazo não superior a 5 (cinco) dias corridos após sua liberação oficial.
9.8	A solução deverá garantir atualização contínua das licenças e funcionalidades contratadas durante toda a vigência do contrato.
9.9	As atualizações de licenças e bases de inteligência deverão ser disponibilizadas em prazo máximo de 36 (trinta e seis) horas após sua liberação pelo fabricante.
9.10	A CONTRATADA deverá disponibilizar canal de atendimento para abertura e acompanhamento de chamados técnicos.

9.11	O sistema de atendimento deverá permitir: a) registro de chamados; b) acompanhamento do status; c) histórico de atendimentos; d) controle de usuários autorizados.
9.12	A CONTRATADA deverá manter cadastro atualizado dos usuários indicados pela CONTRATANTE para abertura e encerramento de chamados.
9.13	O acesso ao sistema de suporte deverá ser realizado de forma segura, mediante autenticação individual.
9.14	A CONTRATADA deverá garantir acesso irrestrito à base de conhecimento do fabricante, incluindo: a) documentação técnica; b) guias de instalação e configuração; c) base de conhecimento (FAQ e troubleshooting); d) atualizações e downloads.
9.15	A CONTRATADA deverá aplicar correções de falhas e atualizações em data e horário definidos pela CONTRATANTE.
9.16	A aplicação de patches e correções estará condicionada à disponibilização pelo fabricante, devendo a CONTRATADA atuar de forma proativa na sua implementação.
9.17	A prestação do serviço deverá observar os requisitos de suporte e manutenção definidos neste Termo de Referência.
9.18	A CONTRATADA deverá manter registro de todos os atendimentos realizados, disponibilizando tais informações à CONTRATANTE quando solicitado.

Referência: Processo nº 01300.003396/2025-91 SEI nº 2759327

Documento assinado eletronicamente por **IRISLENISSON DE SOUZA OLIVEIRA**, **Analista em Ciência e Tecnologia**, em 19/08/2026, às 14:02, conforme o art. 6º do Decreto nº 8.539, de 08 de outubro de 2015.

Documento assinado eletronicamente por **Leonardo Fabiano Seger**, **Analista em Ciência e Tecnologia**, em 19/08/2026, às 14:16, conforme o art. 6º do Decreto nº 8.539, de 08 de outubro de 2015.

Documento assinado eletronicamente por **JOAO PAULO DOS REIS JUNIOR**, **Integrante Administrativo**, em 19/08/2026, às 15:03, conforme o art. 6º do Decreto nº 8.539, de 08 de outubro de 2015.



A autenticidade do documento pode ser conferida no site http://sei.cnpq.br/verifica.html informando o código verificador **2759327** e o código CRC **E137AC05**.

CONSELHO NACIONAL DE DESENVOLVIMENTO CIENTÍFICO E TECNOLÓGICO
COORDENAÇÃO DE GESTÃO DE DADOS E ARQUITETURA CORPORATIVA - CODAC/CGETI/DASD

ANEXO II

MATRIZ DE COMPROVAÇÃO DE ATENDIMENTO À ESPECIFICAÇÃO TÉCNICA MÍNIMA DA SOLUÇÃO

1. DISPOSIÇÕES GERAIS

1.1. Para comprovação do atendimento aos requisitos técnicos da solução, serão aceitos:

- **1.1.1.** Datasheets oficiais do fabricante;
- **1.1.2.** Documentação técnica oficial (manuais, guias, whitepapers);
- **1.1.3.** Cartas ou declarações do fabricante;
- **1.1.4.** Evidências extraídas da CLI (Command Line Interface);
- **1.1.5.** Documentação oficial disponível em portal do fabricante;
- **1.1.6.** Declaração formal do fabricante ou do licitante, nos casos em que o requisito não seja passível de comprovação por documentação pública.

1.2. Os documentos apresentados deverão:

- **1.2.1.** permitir a identificação inequívoca do produto ofertado;
- **1.2.2.** demonstrar de forma objetiva o atendimento aos requisitos;
- **1.2.3.** indicar versão, modelo e fabricante.

1.3. O licitante deverá preencher obrigatoriamente:

- **1.3.1.** Coluna **“ATENDE (SIM/NÃO)”**
- **1.3.2.** Coluna **“COMPROVAÇÃO”**, indicando página, seção ou evidência objetiva

1.4. O não preenchimento da coluna “COMPROVAÇÃO”, ou a apresentação de documentação insuficiente, poderá implicar na desclassificação da proposta.

1.5. A Administração poderá realizar diligências técnicas para validação das informações.

1.7. Requisitos de natureza declaratória, operacional ou não mensurável poderão ser comprovados por declaração formal do fabricante ou do licitante.

HARDWARE

ITEM	REQUISITO	OBRIGATÓRIO	ATENDE	COMPROVAÇÃO
1.1.1	A solução deverá ser composta por 2 (dois) dispositivos de hardware do tipo appliance, idênticos, capazes de operar em alta disponibilidade, utilizando os licenciamentos e componentes de software previstos nesta contratação.	Sim		

1.1.3	Os equipamentos deverão ser novos, de primeiro uso, estar em linha de fabricação na data da entrega, com a versão mais recente de software e/ou firmware disponível e serem comercializados pelo fabricante.	Sim		
1.1.4	Os appliances deverão possuir altura máxima de 1U para instalação em rack padrão 19”, devendo ser fornecidos com todos os acessórios necessários à instalação.	Sim		
1.1.6	Não serão aceitos equipamentos baseados em servidores genéricos ou sistemas operacionais de uso geral.	Sim		
1.1.8	A solução deverá suportar operação em alta disponibilidade, nos modos ativo-passivo e/ou ativo-ativo, garantindo a continuidade do processamento do tráfego em caso de falha de um dos equipamentos.	Sim		
1.1.13	Todos os equipamentos deverão possuir certificações exigidas pela legislação brasileira aplicável, incluindo, quando pertinente, certificação da ANATEL em nome do fabricante.	Sim		
1.1.14	Os equipamentos e softwares não poderão estar classificados como “End of Sale” (EOS) ou “End of Life” (EOL) até a data de abertura das propostas.			
1.1.17	Os equipamentos deverão possuir fonte de alimentação interna, com suporte às seguintes características: a) Operação em tensão de 100 a 240V AC, com seleção automática; b) Frequência de operação de 50/60 Hz; c) Capacidade de operação plena com apenas uma fonte ativa; d) Possibilidade de substituição sem interrupção do funcionamento; e) Conexão a circuitos elétricos independentes; f) Fornecimento de cabos de energia no padrão NBR 14.136.	Sim		
1.1.23	O appliance deve permitir a expansão de recursos de processamento e multitenância através de licenciamento de software possibilitando a evolução do modelo para classes superiores da mesma família sem a necessidade de substituição física do chassi.	Sim		
1.1.24	A solução deve possuir uma camada de plataforma baseada em microserviços permitindo o isolamento total de recursos entre instâncias (tenants).	Sim		

DESEMPENHO DOS APPLIANCES

ITEM	REQUISITO	OBRIGATÓRIO	ATENDE	COMPROVAÇÃO
1.2.1	A solução deverá suportar throughput SSL mínimo de 35 Gbps (trinta e cinco gigabits por segundo), considerando operações de balanceamento de carga com criptografia.	Sim		

1.2.2	A solução deverá suportar, no mínimo, 75.000.000 (setenta e cinco milhões) de conexões simultâneas em camada 4.	Sim		
1.2.3	A solução deverá suportar, no mínimo, 2.500.000 (dois milhões e quinhentas mil) requisições por segundo em camada 7, sem degradação de desempenho.	Sim		
1.2.4	A solução deverá suportar, no mínimo, 1.000.000 (um milhão) novas conexões por segundo em camada 4, sem degradação de desempenho.	Sim		
1.2.5	A solução deverá suportar, no mínimo, 60.000 (sessenta mil) transações SSL por segundo (TPS),considerando chaves RSA de 2.048 bits.	Sim		
1.2.7	A solução deverá suportar, no mínimo, 30.000 (trinta mil) transações SSL por segundo utilizando chaves ECDSA P-256.	Sim		
1.2.9	A solução deverá possuir throughput mínimo de 95 Gbps para balanceamento de carga em camada 4.	Sim		
1.2.10	A solução deverá possuir throughput mínimo de 60 Gbps para balanceamento de carga em camada 7.	Sim		
1.2.12	A solução deverá possuir mecanismos integrados de proteção contra ataques de negação de serviço (DoS e DDoS), incluindo, no mínimo, mitigação de ataques do tipo SYN Flood.	Sim		
1.2.13	A solução deverá suportar capacidade de mitigação de ataques SYN Flood de, no mínimo 80.000.000 (oitenta milhões) de cookies por segundo.	Sim		
1.2.14	A solução deve ser capaz de criar até 8 instâncias virtualizadas em cada appliance fornecido.	Sim		
1.2.16	O hardware deve utilizar tecnologia moderna de FPGA dedicada para mitigar mais de 100 vetores de ataque em hardware e realizar o offload de processamento UDP, evitando a exaustão dos recursos da CPU principal durante eventos de DDoS.	Sim		

INTERFACES (PARA CADA DISPOSITIVO DO PAR)

ITEM	REQUISITO	OBRIGATÓRIO	ATENDE	COMPROVAÇÃO
1.3.1	A solução deverá suportar agregação de links utilizando o protocolo LACP (IEEE 802.3ad), permitindo a formação de grupos com, no mínimo, 2 (duas) interfaces por agregação.	Sim		
1.3.2	A solução deverá suportar, no mínimo, 512 (quinhentas e doze) VLANs.	Sim		
1.3.5	Cada equipamento deverá possuir, no mínimo 2 (duas) portas 100G/40G QSFP28 e 8 (oito) portas 25G/10G SFP28, fornecido com os respectivos transceivers, para uso com fibra óptica multimodo OM4, com conectores LC.	Sim		
1.3.6	Cada equipamento deverá possuir, no mínimo, 1 (uma) interface de rede de 1 Gbps, do tipo1000BASE-T (RJ45), operando em full-duplex, sendo pelo menos 1 (uma) interface dedicada para gerenciamento.	Sim		

1.3.8	A solução deverá suportar o encaminhamento de jumbo frames, com tamanho mínimo de 9.000 bytes, em todas as interfaces destinadas ao tráfego de dados.	Sim		
1.3.10	A solução deverá permitir a configuração de interfaces específicas para comunicação de alta disponibilidade (heartbeat), possibilitando a utilização de rede dedicada para essa finalidade.	Sim		

SOFTWARE

ITEM	REQUISITO	OBRIGATÓRIO	ATENDE	COMPROVAÇÃO
2.5	A solução deverá permitir gerenciamento centralizado dos dispositivos que compõem a infraestrutura.	Sim		
2.6	A solução deverá suportar acesso seguro à gerência por meio de protocolos criptografados, incluindo SSH e HTTPS.	Sim		
2.10	A solução deverá suportar mecanismos de autenticação, autorização e auditoria (AAA), incluindo integração com MFA (autenticação multifator), quando aplicável.	Sim		
2.12	A solução deverá suportar integração com serviços de diretório, incluindo LDAP seguro e Microsoft Active Directory.	Sim		
2.17	A solução deverá suportar integração com servidores Syslog para armazenamento de longo prazo.	Sim		
2.25	A solução deverá permitir acesso aos dados e relatórios por meio de API.	Sim		
2.26	A solução deverá suportar monitoramento via SNMP, incluindo versões v2c e v3.	Sim		
2.33	A solução deve suportar nativamente interfaces de configuração declarativas (API REST), permitindo o provisionamento completo de serviços (L4-L7) através de um único arquivo JSON, compatível com ferramentas de CI/CD (Ansible/Terraform).	Sim		

TRÁFEGO SSL/TLS OFFLOADING

ITEM	REQUISITO	OBRIGATÓRIO	ATENDE	COMPROVAÇÃO
3.1	A solução deverá implementar funcionalidades de SSL/TLS offload, incluindo Full Offload e Bridging.	Sim		
3.3	A solução deverá suportar, no mínimo, os protocolos TLS 1.2 e TLS 1.3.	Sim		
3.5	A solução deverá suportar o protocolo OCSP para validação de certificados.	Sim		
3.6	A solução deverá possuir aceleração criptográfica por hardware para operações SSL/TLS.	Sim		
3.9	A solução deverá suportar Server Name Indication (SNI).	Sim		

BALANCEAMENTO

ITEM	REQUISITO	OBRIGATÓRIO	ATENDE	COMPROVAÇÃO
4.1	A solução deverá suportar balanceamento de carga nas camadas 4 a 7 do modelo OSI.	Sim		
4.2	A solução deverá suportar, no mínimo, os seguintes algoritmos de balanceamento: a) Round Robin; b) Least Connections; c) Round Trip Time; d) Response Time; e) Weighted (por peso).	Sim		
4.3	A solução deverá permitir balanceamento de novas sessões, preservando sessões existentes no mesmo servidor, por meio de mecanismos de persistência.	Sim		
4.5	A solução deverá suportar balanceamento de carga para, no mínimo, os seguintes protocolos: a) TCP; b) UDP; c) IP; d) DNS; e) HTTP e HTTPS; f) HTTP/2; g) FTP; h) SIP; i) RDP; j) RADIUS; k) MySQL e MSSQL; l) RTMP; m) RTSP.	Sim		
4.6	A solução deverá suportar monitoramento de disponibilidade dos servidores reais (health check), incluindo, no mínimo: a) Camada 3: ICMP; b) Camada 4: TCP e UDP; c) Camada 7: protocolos de aplicação.	Sim		
4.9	A solução deverá suportar Network Address Translation (NAT).	Sim		

4.11	A solução deverá ter a capacidade de atuar como gateway de transição, suportando servidores virtuais IPv4 para servidores reais IPv6, bem como servidores virtuais IPv6 para servidores reais IPv4.	Sim		
4.13	A solução deverá permitir compressão de conteúdo HTTP, incluindo suporte a algoritmos como gzip e deflate.	Sim		
4.17	As políticas deverão suportar, no mínimo, os seguintes critérios: a) Cliente (host); b) Sessão SSL; c) Cookie; d) Cabeçalho HTTP; e) URL; f) Geolocalização (GEOIP).	Sim		
4.19	A solução deverá registrar informações das sessões, incluindo, no mínimo: a) Endereço IP de origem; b) Porta de origem; c) Endereço IP de destino; d) Porta de destino; e) Protocolo de transporte; f) Data e hora; g) URL acessada.	Sim		
4.20	A solução deverá suportar integração com plataformas de orquestração de containers (como Kubernetes e OpenShift), por meio de APIs.	Sim		

FIREWALL DE APLICAÇÃO WEB (WAF)

ITEM	REQUISITO	OBRIGATÓRIO	ATENDE	COMPROVAÇÃO
5.1	A solução deverá ser capaz de identificar, isolar e bloquear ataques cibernéticos em camada de aplicação (camada 7), sem impactar negativamente o desempenho das aplicações protegidas.	Sim		
5.2	A solução deverá prover proteção para aplicações web contra ameaças e ataques direcionados aos protocolos HTTP e HTTPS.	Sim		
5.3	A solução deverá suportar modelo de segurança positivo (whitelisting), incluindo proteção baseada nas principais vulnerabilidades descritas no OWASP Top 10 (versão mais atual vigente).	Sim		
5.4	A solução deverá permitir criação de políticas de segurança por aplicação e por URL.	Sim		

5.5	A solução deverá permitir criação automática e/ou assistida de políticas de segurança com base em aprendizado de tráfego ou integração com ferramentas de análise de vulnerabilidades.	Sim		
5.6	A solução deverá suportar proteção baseada em assinaturas atualizadas pelo fabricante.	Sim		
5.7	As assinaturas deverão ser atualizadas durante toda a vigência contratual, sem custos adicionais.	Sim		
5.8	A solução deverá possuir mecanismo de reputação de endereços IP, incluindo base de dados dinâmica atualizada automaticamente, tanto para IPv4 quanto para IPv6.	Sim		
5.9	A solução deverá permitir classificação de reputação, incluindo, no mínimo: a) Origem de SPAM; b) Origem de ataques; c) Botnets; d) Proxies/VPN; e) Scanners.	Sim		
5.10	A solução deverá permitir criação de listas de exceção (whitelist) e bloqueio (blacklist).	Sim		
5.11	A solução deverá possuir mecanismos de proteção contra, no mínimo: a) SQL Injection; b) Cross-Site Scripting (XSS); c) Cross-Site Request Forgery (CSRF); d) Buffer Overflow; e) Parameter Tampering; f) Cookie Poisoning; g) HTTP Request Smuggling; h) Sequestro de sessão; i) Força bruta; j) Ataques a APIs (JSON/XML); k) XML Bombs/DoS; l) Credential Stuffing.	Sim		
5.12	A solução deverá suportar proteção contra ataques de negação de serviço (DoS/DDoS) em camada 7.	Sim		
5.13	A solução deverá permitir criação de políticas baseadas em geolocalização (GEOIP).	Sim		
5.14	A solução deverá permitir bloqueio automático de clientes que excedam limites configuráveis de requisições ou violações.	Sim		
5.15	A solução deverá permitir definição de tempo de bloqueio configurável.	Sim		
5.16	A solução deverá permitir criação de listas dinâmicas e estáticas de bloqueio e exceção.	Sim		
5.17	A solução deverá implementar, no mínimo: a) Validação de URLs; b) Validação de métodos HTTP;	Sim		

	c) Validação de headers HTTP; d) Validação de formulários; e) Inspeção de payload; f) Proteção contra vazamento de informações sensíveis.			
5.18	A solução deverá suportar criptografia e proteção de cookies.	Sim		
5.19	A solução deverá suportar detecção de clientes inválidos por meio de análise de User-Agent.	Sim		
5.20	A solução deverá suportar mecanismos de proteção contra exposição de informações internas da aplicação (information leakage).	Sim		
5.21	A solução deverá suportar integração com ferramentas de análise de vulnerabilidade.	Sim		
5.22	A solução poderá suportar integração via ICAP ou possuir mecanismos nativos equivalentes para inspeção de conteúdo.	Sim		
5.23	A solução deverá fornecer relatórios consolidados de segurança contendo, no mínimo: a) Resumo geral de políticas e eventos; b) Principais ataques; c) Principais IPs de origem; d) Tipos de ataques; e) Violações de protocolo; f) URLs acessadas; g) Geolocalização; h) Severidade.	Sim		
5.24	A solução deverá fornecer visualização gráfica dos eventos, incluindo, no mínimo: a) Por política; b) Por tipo de ataque; c) Por URL; d) Por endereço IP; e) Por país; f) Por severidade;	Sim		
5.25	A solução deverá permitir bloqueio automático de endereços IP com base em comportamento suspeito.	Sim		
5.26	A solução deverá permitir desbloqueio manual ou automático de endereços IP.	Sim		
5.27	A solução deverá permitir inclusão dinâmica de endereços IP em blacklist com base em eventos.	Sim		
5.28	A solução deverá manter lista dinâmica de reputação global de IPs maliciosos, incluindo, no mínimo: a) Web Attacks; b) Botnets; c) Exploits;	Sim		

	d) Scanners; e) DoS/DDoS; f) Proxies anônimos; g) Phishing; h) Reputação geral.			
5.29	A solução deve implementar mitigação proativa de DoS comportamental (BaDoS) e proteção contra bots maliciosos em tempo real.	Sim		
5.30	A solução deve implementar criptografia no nível do campo e ofuscação de dados sensíveis para prevenir vazamento de informações em camadas de erro	Sim		
5.31	A solução deve implementar funcionalidade para ocultar erros de aplicação ou infraestrutura do usuário;	Sim		
5.32	A solução deve permitir a configuração de fluxo de navegação da aplicação, de forma que um usuário só pode alcançar determinada URL se passar por outras anteriormente	Sim		
5.33	Deve suportar acesso a serviços de terminais através de: a) Citrix XenApp; b) Citrix XenDesktop; c) Microsoft RDP; d) VMware Horizon View.	Sim		
5.34	A solução deverá realizar federação através de SAML Artifact Binding onde a comunicação será direta entre o Identity Provider (IdP) e o Service Provider (SP).	Sim		
5.35	A solução deverá atuar como gateway para o acesso MSRDP, deverá ser possível realizar autenticação via NTLM dos usuários, sem a necessidade de software adicional.	Sim		
5.36	A Solução deverá permitir o uso de one-time passcode (OTP) como segundo fator de autenticação através da integração com RSA SecurID.	Sim		
5.37	Deve implementar Bot Defense com análise comportamental e Machine Learning, diferenciando bots 'bons' de 'ruins' e mitigando web scraping avançado	Sim		
5.38	A solução deve oferecer proteção comportamental ilimitada contra ataques DoS em L7 por Servidor Virtual, com autoaprendizado da aplicação	Sim		
5.39	Deve possuir API Discovery automático para identificar Shadow APIs e validar schemas REST/GraphQL via importação de arquivos Swagger/OpenAPI	Sim		
5.40	Deve implementar criptografia de dados no navegador (DataSafe) para proteção contra keyloggers e malwares Man-in-the-Browser	Sim		
5.41	A arquitetura de segurança deve realizar a inspeção e mitigação de ameaças das camadas L3 a L7 em um único fluxo de processamento (one-pass), garantindo a menor latência possível para o tráfego legítimo.	Sim		

5.42	A solução deve possuir proteção via hardware contra ataques de inundação (flood) de pacotes ICMPv6, fornecendo estatísticas detalhadas de descarte	Sim		

BALANCEAMENTO GLOBAL (GLOBAL SERVER LOAD BALANCING)

ITEM	REQUISITO	OBRIGATÓRIO	ATENDE	COMPROVAÇÃO
6.1	A solução deverá suportar balanceamento global de carga (GSLB), com base em resolução de nomes DNS.	Sim		
6.2	A solução deverá suportar operação como: a) Servidor DNS autoritativo; b) Servidor DNS secundário; c) Servidor DNS cache; d) Balanceador de servidores DNS.	Sim		
6.3	A solução deverá suportar DNSSEC.	Sim		
6.5	A solução deverá possuir mecanismos de proteção contra ataques DNS, incluindo, no mínimo: a) Validação de protocolo; b) Proteção contra UDP Flood; c) Proteção contra pacotes malformados; d) Proteção contra ataques de amplificação e reflexão DNS; e) Proteção contra NXDOMAIN Flood; f) Proteção contra cache poisoning.	Sim		
6.7	A solução deverá suportar transferência de zona (zone transfer) entre servidores DNS.	Sim		
6.10	A solução deverá suportar políticas de distribuição de tráfego baseadas em: a) Geolocalização (GEOIP); b) Disponibilidade de servidores; c) Latência; d) Round Robin; e) Capacidade do serviço; f) Persistência baseada em cliente (LDNS ou IP).	Sim		
6.13	A solução deverá suportar monitoramento de saúde de: a) Servidores; b) Serviços; c) Links de comunicação.	Sim		

6.20	A solução deverá implementar mecanismos de transição IPv6, incluindo a funcionalidade de DNS64.	Sim		

Referência: Processo nº 01300.003396/2025-91 SEI nº 2759875

Documento assinado eletronicamente por **IRISLENISSON DE SOUZA OLIVEIRA**, **Analista em Ciência e Tecnologia**, em 19/08/2026, às 14:02, conforme o art. 6º do Decreto nº 8.539, de 08 de outubro de 2015.

Documento assinado eletronicamente por **Leonardo Fabiano Seger**, **Analista em Ciência e Tecnologia**, em 19/08/2026, às 14:16, conforme o art. 6º do Decreto nº 8.539, de 08 de outubro de 2015.

Documento assinado eletronicamente por **JOAO PAULO DOS REIS JUNIOR**, **Integrante Administrativo**, em 19/08/2026, às 15:03, conforme o art. 6º do Decreto nº 8.539, de 08 de outubro de 2015.

A autenticidade do documento pode ser conferida no site http://sei.cnpq.br/verifica.html informando o código verificador **2759875** e o código CRC **ACEDF8C2**.

CONSELHO NACIONAL DE DESENVOLVIMENTO CIENTÍFICO E TECNOLÓGICO
COORDENAÇÃO DE GESTÃO DE DADOS E ARQUITETURA CORPORATIVA - CODAC/CGETI/DASD

ANEXO III

TERMO DE COMPROMISSO DE MANUTENÇÃO DE SIGILO

INTRODUÇÃO
O Termo de Compromisso de Manutenção de Sigilo registra o comprometimento formal da Contratada em cumprir as condições estabelecidas no documento relativas ao acesso e utilização de informações sigilosas da Contratante em decorrência de relação contratual, vigente ou não. **Referência: Art. 18, Inciso V, alínea "a" da IN SGD/ME Nº 94/2022.**

Pelo presente instrumento o <NOME DO ÓRGÃO>, sediado em <ENDEREÇO>, CNPJ n° <Nº do CNPJ>, doravante denominado **CONTRATANTE**, e, de outro lado, a <NOME DA EMPRESA>, sediada em <ENDEREÇO>, CNPJ n° <Nº do CNPJ>, doravante denominada **CONTRATADA**;
CONSIDERANDO que, em razão do **CONTRATO N.º nº do contrato** 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 e Privacidade da **CONTRATANTE**;
Resolvem celebrar o presente **TERMO DE COMPROMISSO DE MANUTENÇÃO DE SIGILO,** doravante **TERMO**, vinculado ao **CONTRATO PRINCIPAL**, mediante as seguintes cláusulas e condições abaixo discriminadas.

1. OBJETO

Constitui objeto deste TERMO o estabelecimento de condições específicas para regulamentar as obrigações a serem observadas pela CONTRATADA, no que diz respeito ao trato de informações sigilosas disponibilizadas pela CONTRATANTE e a observância às normas de segurança da informação e privacidade por força dos procedimentos necessários para a execução do objeto do CONTRATO PRINCIPAL celebrado entre as partes e em acordo com o que dispõem a Lei 12.527, de 18 de novembro de 2011, Lei nº 13.709, de 14 de agosto de 2018, e os Decretos 7.724, de 16 de maio de 2012, e 7.845, de 14 de novembro de 2012, que regulamentam os procedimentos para acesso e tratamento de informação classificada em qualquer grau de sigilo.

2. CONCEITOS E DEFINIÇÕES

Para os efeitos deste TERMO, são estabelecidos os seguintes conceitos e definições:

INFORMAÇÃO: dados, processados ou não, que podem ser utilizados para produção e transmissão de conhecimento, contidos em qualquer meio, suporte ou formato.

INFORMAÇÃO SIGILOSA: aquela submetida temporariamente à restrição de acesso público em razão de sua imprescindibilidade para a segurança da sociedade e do Estado, e aquela abrangida pelas demais hipóteses legais de sigilo.

CONTRATO PRINCIPAL: contrato celebrado entre as partes, ao qual este TERMO se vincula.

3. DA INFORMAÇÃO SIGILOSA

Serão consideradas como informação sigilosa, toda e qualquer informação classificada ou não nos graus de sigilo ultrassecreto, secreto e reservado. O TERMO abrangerá toda informação escrita, verbal, ou em linguagem computacional em qualquer nível, ou de qualquer outro modo apresentada, tangível ou intangível, podendo incluir, mas não se limitando a: *know-how*, técnicas, especificações, relatórios, compilações, código fonte de programas de computador na íntegra ou em partes, fórmulas, desenhos, cópias, modelos, amostras de ideias, aspectos financeiros e econômicos, definições, informações sobre as atividades da CONTRATANTE e/ou quaisquer informações técnicas/comerciais relacionadas/resultantes ou não ao CONTRATO PRINCIPAL, doravante denominados INFORMAÇÕES, a que diretamente ou pelos seus empregados, a CONTRATADA venha a ter acesso, conhecimento ou que venha a lhe ser confiada durante e em razão das atuações de execução do CONTRATO PRINCIPAL celebrado entre as partes.

4. DOS LIMITES DO SIGILO

As obrigações constantes deste TERMO não serão aplicadas às INFORMAÇÕES que:

I – sejam comprovadamente de domínio público no momento da revelação, exceto se tal fato decorrer de ato ou omissão da CONTRATADA;

II – tenham sido comprovadas e legitimamente recebidas de terceiros, estranhos ao presente TERMO;

III – sejam reveladas em razão de requisição judicial ou outra determinação válida do Governo, somente até a extensão de tais ordens, desde que as partes cumpram qualquer medida de proteção pertinente e tenham sido notificadas sobre a existência de tal ordem, previamente e por escrito, dando a esta, na medida do possível, tempo hábil para pleitear medidas de proteção que julgar cabíveis.

5. DIREITOS E OBRIGAÇÕES

As partes se comprometem a não revelar, copiar, transmitir, reproduzir, utilizar, transportar ou dar conhecimento, em hipótese alguma, a terceiros, bem como a não permitir que qualquer empregado envolvido direta ou indiretamente na execução do CONTRATO PRINCIPAL, em qualquer nível hierárquico de sua estrutura

organizacional e sob quaisquer alegações, faça uso dessas INFORMAÇÕES, que se restringem estritamente ao cumprimento do CONTRATO PRINCIPAL.

Parágrafo Primeiro – A CONTRATADA se compromete a não efetuar qualquer tipo de cópia da informação sigilosa sem o consentimento prévio e expresso da CONTRATANTE.

Parágrafo Segundo – A CONTRATADA compromete-se a dar ciência e obter o aceite formal da direção e empregados que atuarão direta ou indiretamente na execução do CONTRATO PRINCIPAL sobre a existência deste TERMO bem como da natureza sigilosa das informações.

I – A CONTRATADA deverá firmar acordos por escrito com seus empregados visando garantir o cumprimento de todas as disposições do presente TERMO e dará ciência à CONTRATANTE dos documentos comprobatórios.

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

Parágrafo Quarto – Cada parte permanecerá como fiel depositária das informações reveladas à outra parte em função deste TERMO.

I – Quando requeridas, as INFORMAÇÕES deverão retornar imediatamente ao proprietário, bem como todas e quaisquer cópias eventualmente existentes.

Parágrafo Quinto – A CONTRATADA obriga-se por si, sua controladora, suas controladas, coligadas, representantes, procuradores, sócios, acionistas e cotistas, por terceiros eventualmente consultados, seus empregados, contratados e subcontratados, assim como por quaisquer outras pessoas vinculadas à CONTRATADA, direta ou indiretamente, a manter sigilo, bem como a limitar a utilização das informações disponibilizadas em face da execução do CONTRATO PRINCIPAL.

Parágrafo Sexto – A CONTRATADA, na forma disposta no parágrafo primeiro, acima, também se obriga a:

I – Não discutir perante terceiros, usar, divulgar, revelar, ceder a qualquer título ou dispor das INFORMAÇÕES, no território brasileiro ou no exterior, para nenhuma pessoa, física ou jurídica, e para nenhuma outra finalidade que não seja exclusivamente relacionada ao objetivo aqui referido, cumprindo-lhe adotar cautelas e precauções adequadas no sentido de impedir o uso indevido por qualquer pessoa que, por qualquer razão, tenha acesso a elas;

II – Responsabilizar-se por impedir, por qualquer meio em direito admitido, arcando com todos os custos do impedimento, mesmos judiciais, inclusive as despesas processuais e outras despesas derivadas, a divulgação ou utilização das INFORMAÇÕES por seus agentes, representantes ou por terceiros;

III – Comunicar à CONTRATANTE, de imediato, de forma expressa e antes de qualquer divulgação, caso tenha que revelar qualquer uma das INFORMAÇÕES, por determinação judicial ou ordem de atendimento obrigatório determinado por órgão competente; e

IV – Identificar as pessoas que, em nome da CONTRATADA, terão acesso às informações sigilosas.

6. 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.

7. PENALIDADES

A quebra do sigilo e/ou da confidencialidade das INFORMAÇÕES, devidamente comprovada, possibilitará a imediata aplicação de penalidades previstas conforme disposições contratuais e legislações em vigor que tratam desse assunto, podendo até culminar na rescisão do CONTRATO PRINCIPAL firmado entre as PARTES. Neste caso, a CONTRATADA, estará sujeita, por ação ou omissão, ao pagamento ou recomposição de todas as perdas e danos sofridos pela CONTRATANTE,

inclusive as de ordem moral, bem como as de responsabilidades civil e criminal, as quais serão apuradas em regular processo administrativo ou judicial, sem prejuízo das demais sanções legais cabíveis, conforme previsto nos arts. 155 a 163 da Lei nº. 14.133, de 2021.

8. DISPOSIÇÕES GERAIS

Este TERMO de Confidencialidade é parte integrante e inseparável do CONTRATO PRINCIPAL.

Parágrafo Primeiro – Surgindo divergências quanto à interpretação do disposto neste instrumento, ou quanto à execução das obrigações dele decorrentes, ou constatando-se casos omissos, as partes buscarão solucionar as divergências de acordo com os princípios de boa fé, da equidade, da razoabilidade, da economicidade e da moralidade.

Parágrafo Segundo – O disposto no presente TERMO prevalecerá sempre em caso de dúvida e, salvo expressa determinação em contrário, sobre eventuais disposições constantes de outros instrumentos conexos firmados entre as partes quanto ao sigilo de informações, tal como aqui definidas.

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

I – A CONTRATANTE terá o direito de, a qualquer tempo e sob qualquer motivo, auditar e monitorar as atividades da CONTRATADA;

II – A CONTRATADA deverá disponibilizar, sempre que solicitadas formalmente pela CONTRATANTE, todas as informações requeridas pertinentes ao CONTRATO PRINCIPAL.

III – A omissão ou tolerância das partes, em exigir o estrito cumprimento das condições estabelecidas neste instrumento, não constituirá novação ou renúncia, nem afetará os direitos, que poderão ser exercidos a qualquer tempo;

IV – Todas as condições, termos e obrigações ora constituídos serão regidos pela legislação e regulamentação brasileiras pertinentes;

V – O presente TERMO somente poderá ser alterado mediante TERMO aditivo firmado pelas partes;

VI – Alterações do número, natureza e quantidade das informações disponibilizadas para a CONTRATADA não descaracterizarão ou reduzirão o compromisso e as obrigações pactuadas neste TERMO, que permanecerá válido e com todos seus efeitos legais em qualquer uma das situações tipificadas neste instrumento;

VII – O acréscimo, complementação, substituição ou esclarecimento de qualquer uma das informações, conforme definição do item 3 deste documento, 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 para a outra Parte, nem como obrigação de celebrarem qualquer outro acordo entre si.

9. FORO

A CONTRATANTE elege o foro da <CIDADE DA CONTRATANTE>, onde está localizada a sede da CONTRATANTE, para dirimir quaisquer dúvidas originadas do presente TERMO, com renúncia expressa a qualquer outro, por mais privilegiado que seja.

10. ASSINATURAS

CONTRATADA	CONTRATANTE
_____ <Nome> <Qualificação>	_____ <Nome> **Matrícula:** xxxxxxxx

TESTEMUNHAS	
_____ <Nome> <Qualificação>	_____ <Nome> <Qualificação>

Referência: Processo nº 01300.003396/2025-91 SEI nº 2616611

Documento assinado eletronicamente por **IRISLENISSON DE SOUZA OLIVEIRA**, **Analista em Ciência e Tecnologia**, em 08/06/2026, às 11:37, conforme o art. 6º do Decreto nº 8.539, de 08 de outubro de 2015.

Documento assinado eletronicamente por **Leonardo Fabiano Seger**, **Integrante técnico da contratação**, em 10/06/2026, às 09:49, conforme o art. 6º do Decreto nº 8.539, de 08 de outubro de 2015.

Documento assinado eletronicamente por **JOAO PAULO DOS REIS JUNIOR**, **Integrante Administrativo**, em 10/06/2026, às 10:54, conforme o art. 6º do Decreto nº 8.539, de 08 de outubro de 2015.



A autenticidade do documento pode ser conferida no site http://sei.cnpq.br/verifica.html informando o código verificador **2616611** e o código CRC **06E8FBD3**.

CONSELHO NACIONAL DE DESENVOLVIMENTO CIENTÍFICO E TECNOLÓGICO
COORDENAÇÃO DE GESTÃO DE DADOS E ARQUITETURA CORPORATIVA - CODAC/CGETI/DASD

ANEXO IV

TERMO DE CIÊNCIA

INTRODUÇÃO
O Termo de Ciência visa obter o comprometimento formal dos empregados da Contratada diretamente envolvidos na contratação quanto ao conhecimento da declaração de manutenção de sigilo e das normas de segurança vigentes no órgão/entidade. No caso de substituição ou inclusão de empregados da contratada, o preposto deverá entregar ao Fiscal Administrativo do Contrato os Termos de Ciência assinados pelos novos empregados envolvidos na execução dos serviços contratados. **Referência: Art. 18, Inciso V, alínea "b" da IN SGD/ME Nº 94/2022.**

1 – IDENTIFICAÇÃO			
CONTRATO Nº	xxxx/aaaa		
OBJETO	obje to do contrato		
CONTRATADA	nome da c ontratada	**CNPJ**	xxxxxxxxxxxx
PREPOSTO	Nome do Pr eposto da Contratada		
GESTOR DO CONTRATO	Nome do Ges tor do Contrato	**MATR.**	xxxxxxxxxxxxx

2 – CIÊNCIA

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

FUNCIONÁRIOS DA CONTRATADA		
NOME	**MATRÍCULA**	**ASSINATURA**

⍰Nome do(a) Funcionário(a)⍰	⍰xxxxxxxxxx⍰	
⍰Nome do(a) Funcionário(a)⍰	⍰xxxxxxxxxx⍰	
...	...	...

_____ ⍰Loc al⍰, ⍰dia⍰ de ⍰mês⍰ de ⍰ano⍰.

Referência: Processo nº 01300.003396/2025-91 SEI nº 2616627

Documento assinado eletronicamente por **IRISLENISSON DE SOUZA OLIVEIRA**, **Analista em Ciência e Tecnologia**, em 08/06/2026, às 11:37, conforme o art. 6º do Decreto nº 8.539, de 08 de outubro de 2015.

Documento assinado eletronicamente por **Leonardo Fabiano Seger**, **Integrante técnico da contratação**, em 10/06/2026, às 09:49, conforme o art. 6º do Decreto nº 8.539, de 08 de outubro de 2015.

Documento assinado eletronicamente por **JOAO PAULO DOS REIS JUNIOR**, **Integrante Administrativo**, em 10/06/2026, às 10:54, conforme o art. 6º do Decreto nº 8.539, de 08 de outubro de 2015.

A autenticidade do documento pode ser conferida no site http://sei.cnpq.br/verifica.html informando o código verificador **2616627** e o código CRC **6FEA96D7**.

CONSELHO NACIONAL DE DESENVOLVIMENTO CIENTÍFICO E TECNOLÓGICO
COORDENAÇÃO DE GESTÃO DE DADOS E ARQUITETURA CORPORATIVA - CODAC/CGETI/DASD

ANEXO V

MODELO DO TERMO DE VISTORIA TÉCNICA

1. TERMO DE VISTORIA TÉCNICA

Certifico sob as penas da lei que a empresa <**NOME DA EMPRESA**>, inscrita no Cadastro Nacional de Pessoa Jurídica, CNPJ/MF sob o número <**CNPJ DA EMPRESA**>, com sede na <**ENDEREÇO DA EMPRESA**>, por intermédio de seu representante legal, do(a) Senhor(a) <**REPRESENTANTE LEGAL DA EMPRESA**>, portador(a) da carteira de identidade número <**RG DO REPRESENTANTE LEGAL**>, expedida pela <**ÓRGÃO EXPEDIDOR DO DOCUMENTO**> e do cadastro de Pessoa Física, CPF/MF, sob o número <**CPF DO REPRESENTANTE LEGAL**> visitou as dependências do CONSELHO NACIONAL DE DESENVOLVIMENTO CIENTÍFICO E TECNOLÓGICO - CNPq, tomando conhecimento dos locais onde serão prestados os serviços objeto do Pregão Eletrônico SRP nº. <**PREGÃO**>, estando plenamente consciente da infraestrutura que tem a disposição, das metodologias e das condições para a prestação dos serviços.

Brasília/DF, ____ de _____ de 20__.

_____
Representante da Empresa

_____
Representante do CNPq

Documento assinado eletronicamente por **IRISLENISSON DE SOUZA OLIVEIRA**, **Analista em Ciência e Tecnologia**, em 08/06/2026, às 11:37, conforme o art. 6º do Decreto nº 8.539, de 08 de outubro de 2015.

Documento assinado eletronicamente por **Leonardo Fabiano Seger**, **Integrante técnico da contratação**, em 10/06/2026, às 09:50, conforme o art. 6º do Decreto nº 8.539, de 08 de outubro de 2015.

Documento assinado eletronicamente por **JOAO PAULO DOS REIS JUNIOR**, **Integrante Administrativo**, em 10/06/2026, às 10:54, conforme o art. 6º do Decreto nº 8.539, de 08 de outubro de 2015.

A autenticidade do documento pode ser conferida no site http://sei.cnpq.br/verifica.html informando o código verificador **2616618** e o código CRC **4AFAB4AA**.

CONSELHO NACIONAL DE DESENVOLVIMENTO CIENTÍFICO E TECNOLÓGICO
COORDENAÇÃO DE GESTÃO DE DADOS E ARQUITETURA CORPORATIVA - CODAC/CGETI/DASD

ANEXO VI

MODELO DE RECUSA DE VISTORIA TÉCNICA

1. DECLARAÇÃO DE DISPENSA DE VISTORIA

A empresa <**NOME DA EMPRESA**>, CNPJ <**CNPJ DA EMPRESA**>, por intermédio do(a) Senhor(a) <**REPRESENTANTE LEGAL DA EMPRESA**>, indicado expressamente como seu representante, declara ter conhecimento do serviço a ser prestado através do Edital e seus Anexos, dispensando a necessidade da vistoria "*in loco*" prevista no Edital do Pregão Eletrônico SRP nº. <**PREGÃO**>. Declara, ainda, que se responsabiliza pela dispensa e por situações supervenientes. Declaro que me foi dado acesso às dependências do CONSELHO NACIONAL DE DESENVOLVIMENTO CIENTÍFICO E TECNOLÓGICO - CNPq, através de cláusula expressa no Edital e anexos, ao qual dispensei por ter conhecimento suficiente para a prestação dos serviços com as informações constantes do Termo de Referência e Edital.

Brasília/DF, ____ de _____ de 20__.

_____
Representante da Empresa

Referência: Processo nº 01300.003396/2025-91 SEI nº 2616622

Documento assinado eletronicamente por **IRISLENISSON DE SOUZA OLIVEIRA**, **Analista em Ciência e Tecnologia**, em 08/06/2026, às 11:37, conforme o art. 6º do Decreto nº 8.539, de 08 de outubro de 2015.

Documento assinado eletronicamente por **Leonardo Fabiano Seger**, **Integrante técnico da contratação**, em 10/06/2026, às 09:50, conforme o art. 6º do Decreto nº 8.539, de 08 de outubro de 2015.

Documento assinado eletronicamente por **JOAO PAULO DOS REIS JUNIOR**, **Integrante Administrativo**, em 10/06/2026, às 10:54, conforme o art. 6º do Decreto nº 8.539, de 08 de outubro de 2015.

A autenticidade do documento pode ser conferida no site http://sei.cnpq.br/verifica.html informando o código verificador **2616622** e o código CRC **844954A4**.

CONSELHO NACIONAL DE DESENVOLVIMENTO CIENTÍFICO E TECNOLÓGICO
COORDENAÇÃO DE GESTÃO DE DADOS E ARQUITETURA CORPORATIVA - CODAC/CGETI/DASD

ANEXO VII

MODELO DA PLANILHA DE CUSTOS E FORMAÇÃO DE PREÇOS PARA CONTRATAÇÃO DE SOFTWARE E SERVIÇOS DE COMPUTAÇÃO EM NUVEM

1. MODELO DE PLANILHA DE CUSTOS E FORMAÇÃO DE PREÇOS PARA A CONTRATAÇÃO

1.1. A Planilha de Custos e Formação de Preços é uma importante ferramenta que contribui para a análise crítica da composição dos preços unitários e total, com vistas a mitigar a assimetria de informações e auxiliar na eventual realização de diligências destinadas a esclarecer ou a complementar a instrução do processo.
1.□. Por se tratar de contratação exclusivamente vinculada à entrega de produtos e ao atendimento aos níveis mínimos de serviços, não se configura como contratação com dedicação exclusiva de mão de obra, contratação por homem/hora tampouco por postos de trabalho.
1.□. P ara cada item a ser licitado, deve-se entregar a planilha de custos e formação de preços modelada na tabela 1 deste anexo.
1.□. A Planilha de Custos e Formação de Preços deve ser entregue pelo licitante durante a fase de recebimento de propostas e não se vincula à estimativa apresentada pelo órgão contratante na fase de planejamento da contratação.

Tabela 1: modelo de planilha de custos e formação de preços

Identificação da Licitação:	
N.º do Processo:	
N.º da Licitação:	
Nome da Empresa:	
CNPJ:	
GRUPO 1	
ITEM X - *<descrição do Item>*	
Componentes de Custo	
Descrição	**Valor Unitário (□)**
Custo de pessoal	R$ XX,XX
Custos com software	R$ XX,XX

Custos com recursos de computação	R$ XX,XX
Custos com suporte técnico	R$ XX,XX
Custos com atualização e correção	R$ XX,XX
Custos com hardware	R$ XX,XX
Custos com serviços de informações	R$ XX,XX
Outros custos (especificar)	R$ XX,XX
Subtotal dos demais componentes de custo	**R$ XXXX,XX**
Componentes de Preço (não compreendidos na composição do fator K)	
Descrição	**Valor Unitário (R$)**
Elementos Comerciais (Fatores/Ajustes Comerciais)	R$ XX,XX
Cobertura Tributária	R$ XX,XX
Outros componentes (especificar)	R$ XX,XX
Subtotal dos componentes de preço:	**R$ XXXX,XX**
Total Mensal:	**R$ XXXX,XX**
Quantidade Total Estimada:	**R$ XXXX,XX**
Valor Total do [item/grupo]:[Valor unitário x quantidade estimada para contratação]:	**R$ XXXX,XX**

3. COMPONENTES DE CUSTOS QUE INTEGRAM A PLANILHA

3.1. Custo de Pessoal consolida todos os custos incorridos com a utilização de serviços de profissionais necessários à intermediação, operação e utilização dos recursos tecnológicos. Deverá ser computado o somatório de todos os custos acrescidos dos encargos aprovisionados (tais como remuneração, encargos sociais, auxílios e benefícios dos recursos humanos diretamente envolvidos).

3.2. Custos com software equivale ao somatório de todos os custos de disponibilização e utilização de recursos de software que integrarão a prestação dos serviços (tais como licenciamento, subscrição).

3.3. Custos com recursos de computação equivale ao somatório de todos os custos de disponibilização e utilização de recursos lógicos e virtuais de computação que integrarão a prestação dos serviços (tais como infraestrutura como serviço, plataforma como serviço, instâncias de computação, plataformas, armazenamento, rede, backup, segurança, middlewares, centrais de processamento de dados, entre outros recursos de computação).

3.4. Custos com suporte técnico equivale ao somatório de todos os custos de suporte técnico que integrarão a prestação dos serviços (tais como atendimento e suporte técnico dos produtos de software ou recursos computacionais).

3.5. Custos com atualização e correção equivale ao somatório de todos os custos de atualização e correção dos recursos tecnológicos que integrarão a prestação dos serviços (tais como atualizações de versão dos produtos e correção de erros – bug fix).

3.6. Custos com hardware equivale ao somatório de todos os custos de disponibilização e utilização de hardware localmente e diretamente na prestação dos serviços (tais como appliances, controladoras, servidores de computação, recursos tecnológicos físicos).

. **Custos com serviços de informações:** equivale ao somatório de todos os custos de fornecimento de informações técnicas especializadas às equipes que prestam os serviços (tais como plataformas digitais de fornecimento de conteúdo técnico especializado, serviços de mentoring e consultoria, plataformas de suporte especializado, entre outras soluções de fornecimento de informações técnicas especializadas).

. **Elementos Comerciais (Fatores/Ajustes Comerciais):** fator de preço que pode ser aplicado, tendo como base estratégias de negócio, elementos mercadológicos e estratégias de precificação da empresa (tais como margem operacional, margem de risco, margem de lucro, markup, custo de revenda dentre outros fatores interno e externos considerados na precificação).

. **Cobertura Tributária:** fator de preço que inclui os custos tributários associados à prestação dos serviços que variam de acordo com o planejamento tributário de cada empresa.

Referência: Processo nº 01300.003396/2025-91 SEI nº 2624334

Documento assinado eletronicamente por **IRISLENISSON DE SOUZA OLIVEIRA**, **Analista em Ciência e Tecnologia**, em 08/06/2026, às 11:37, conforme o art. 6º do Decreto nº 8.539, de 08 de outubro de 2015.

Documento assinado eletronicamente por **Leonardo Fabiano Seger**, **Integrante técnico da contratação**, em 10/06/2026, às 09:50, conforme o art. 6º do Decreto nº 8.539, de 08 de outubro de 2015.

Documento assinado eletronicamente por **JOAO PAULO DOS REIS JUNIOR**, **Integrante Administrativo**, em 10/06/2026, às 10:54, conforme o art. 6º do Decreto nº 8.539, de 08 de outubro de 2015.

A autenticidade do documento pode ser conferida no site http://sei.cnpq.br/verifica.html informando o código verificador **2624334** e o código CRC **08FAA9BF**.

CONSELHO NACIONAL DE DESENVOLVIMENTO CIENTÍFICO E TECNOLÓGICO
COORDENAÇÃO DE GESTÃO DE DADOS E ARQUITETURA CORPORATIVA - CODAC/CGETI/DASD

ANEXO VIII

MODELO DE PLANILHA DE COMPOSIÇÃO DE CUSTOS E FORMAÇÃO DE PREÇOS DE SERVIÇOS DE GERENCIAMENTO, MIGRAÇÃO E CONSULTORIA ESPECIALIZADA

1. MODELO DE PLANILHA DE CUSTOS E FORMAÇÃO DE PREÇOS PARA A CONTRATAÇÃO DE SOFTWARE E SERVIÇOS DE COMPUTAÇÃO EM NUVEM

1.1. As Planilhas de Custos e Formação de Preços é uma importante ferramenta que contribui para a análise crítica da composição dos preços unitários e total, com vistas a mitigar a assimetria de informações e auxiliar na eventual realização de diligências destinadas a esclarecer ou a complementar a instrução do processo.
1.□. Por se tratar de contratação exclusivamente vinculada à entrega de produtos e ao atendimento aos níveis mínimos de serviços, não se configura como contratação com dedicação exclusiva de mão de obra, contratação por homem/hora tampouco por postos de trabalho.
1.□. P ara cada item a ser licitado, deve-se entregar as planilhas de custos e formação de preços modeladas nas tabela □ des te anexo.
1.□. As Planilhas de Custos e Formação de Preços devem ser entregues pelo licitante durante a fase de recebimento de propostas e não se vinculam à estimativa apresentada pelo órgão contratante na fase de planejamento da contratação.

□. MODEL O DE PLANILHA DE CUSTOS E FORMAÇÃO DE PREÇOS DE SERVIÇOS DE GERENCIAMENTO, MIGRAÇÃO E CONSULTORIA ESPECIALIZADA

Tabela □: Modelo de planilha de c omposição de custos e formação de preços de serviços de gerenciamento, migração e consultoria especializada

Identificação da Licitação:
N.º do Processo:
N.º da Licitação:
Nome da Empresa:
CNPJ:
GRUPO 1
ITEM X - *□descriç ão do Item□*

Componentes de Custo de Pessoal					
Identificação do Perfil Profissional	**Salário (S)**	**Fator K (K)**	**Custo total por perfil (CT = S x K)**	**Qtde. de profissionais por perfil (Q)**	**Custo Mensal por Perfil (CM = CT x Q)**
Subtotal componentes de custo de Pessoal					
Demais Componentes de Custo					**Valor Unitário (R$)**
Custo com software					R$ XX,XX
Custos com recursos de computação					R$ XX,XX
Custos com suporte técnico					R$ XX,XX
Custos com atualização e correção					R$ XX,XX
Custos com hardware					R$ XX,XX
Custos com serviços de informações					R$ XX,XX
Outros custos (especificar)					R$ XX,XX
Subtotal componentes de custo					**R$ XXXX,XX**
Componentes de Preço					
Descrição					**Valor Unitário (R$)**
Elementos Comerciais (Fatores/Ajustes Comerciais)					R$ XX,XX
Cobertura Tributária					R$ XX,XX
Outros componentes (especificar)					R$ XX,XX
Subtotal dos componentes de preço:					**R$ XXXX,XX**
Total Unitário:					**R$ XXXX,XX**
Quantidade Total Estimada:					**R$ XXXX,XX**
Valor Total do [item/grupo]:[Valor unitário x quantidade estimada para contratação]:					**R$ XXXX,XX**

. C OMPONENTES DE CUSTOS QUE INTEGRAM A PLANILHA

.1. Custo de Pessoal consolida todos os custos incorridos com a utilização de serviços de profissionais necessários à intermediação, operação e utilização dos recursos tecnológicos. Deverá ser computado o somatório de todos os custos acrescidos dos encargos aprovisionados (tais como remuneração, encargos sociais, auxílios e benefícios dos recursos humanos diretamente envolvidos).

.. Custos com software equivale ao somatório de todos os custos de disponibilização e utilização de recursos de software que integrarão a prestação dos serviços (tais como licenciamento, subscrição).

. **Custos com recursos de computação:** equivale ao somatório de todos os custos de disponibilização e utilização de recursos lógicos e virtuais de computação que integrarão a prestação dos serviços (tais como infraestrutura como serviço, plataforma como serviço, instâncias de computação, plataformas, armazenamento, rede, backup, segurança, middlewares, centrais de processamento de dados, entre outros recursos de computação).

. **Custos com suporte técnico:** equivale ao somatório de todos os custos de suporte técnico que integrarão a prestação dos serviços (tais como atendimento e suporte técnico dos produtos de software ou recursos computacionais).

. **Custos com atualização e correção:** equivale ao somatório de todos os custos de atualização e correção dos recursos tecnológicos que integrarão a prestação dos serviços (tais como atualizações de versão dos produtos e correção de erros – bug fix).

. **Custos com hardware:** equivale ao somatório de todos os custos de disponibilização e utilização de hardware localmente e diretamente na prestação dos serviços (tais como appliances, controladoras, servidores de computação, recursos tecnológicos físicos).

. **Custos com serviços de informações:** equivale ao somatório de todos os custos de fornecimento de informações técnicas especializadas às equipes que prestam os serviços (tais como plataformas digitais de fornecimento de conteúdo técnico especializado, serviços de mentoring e consultoria, plataformas de suporte especializado, entre outras soluções de fornecimento de informações técnicas especializadas).

. **Elementos Comerciais (Fatores/Ajustes Comerciais):** fator de preço que pode ser aplicado, tendo como base estratégias de negócio, elementos mercadológicos e estratégias de precificação da empresa (tais como margem operacional, margem de risco, margem de lucro, markup, custo de revenda dentre outros fatores interno e externos considerados na precificação).

. **Cobertura Tributária:** fator de preço que inclui os custos tributários associados à prestação dos serviços que variam de acordo com o planejamento tributário de cada empresa.

Referência: Processo nº 01300.003396/2025-91 SEI nº 2624338

Documento assinado eletronicamente por **IRISLENISSON DE SOUZA OLIVEIRA**, **Analista em Ciência e Tecnologia**, em 08/06/2026, às 11:37, conforme o art. 6º do Decreto nº 8.539, de 08 de outubro de 2015.

Documento assinado eletronicamente por **Leonardo Fabiano Seger**, **Integrante técnico da contratação**, em 10/06/2026, às 09:50, conforme o art. 6º do Decreto nº 8.539, de 08 de outubro de 2015.

Documento assinado eletronicamente por **JOAO PAULO DOS REIS JUNIOR**, **Integrante Administrativo**, em 10/06/2026, às 10:54, conforme o art. 6º do Decreto nº 8.539, de 08 de outubro de 2015.



A autenticidade do documento pode ser conferida no site http://sei.cnpq.br/verifica.html informando o código verificador **2624338** e o código CRC **4D3FFAD3**.

MODELO DE TERMO DE CONTRATO
Lei nº 14.133, de 1º de abril de 2021
TECNOLOGIAS DA INFORMAÇÃO E COMUNICAÇÃO - TIC
AQUISIÇÕES – LICITAÇÃO E CONTRATAÇÃO DIRETA

ÓRGÃO OU ENTIDADE PÚBLICA

(Processo Administrativo n° *01300.003396/2025-91*)

CONTRATO ADMINISTRATIVO Nº *xx*/*xxxx*, QUE FAZEM ENTRE SI O CONSELHO NACIONAL DE DESENVOLVIMENTO CIENTÍFICO E TECNOLÓGICO – CNPq E A EMPRESA.....

O *CONSELHO NACIONAL DE DESENVOLVIMENTO CIENTÍFICO E TECNOLÓGICO – CNPq*, com sede no *Setor de Autarquias Sul (SAUS), Quadra 01, Lote 06, Bloco H, Ed. Telemundi II, Bairro Asa Sul, CEP 70.070-010*, na cidade de *Brasília*/*DF*, inscrito(a) no CNPJ sob o nº *33.654.831/0001-36*, neste ato representado(a) pelo(a) [*cargo e nome*], nomeado(a) pela Portaria nº *XX*, de *[dia]* de *[mês]* de *[ano]*, publicada no *DOU* de *[dia]* de *[mês]* de *[ano]*, portador da Matrícula Funcional nº *[nº matrícula]*, doravante denominado CONTRATANTE, e o(a) *[CONTRATADO]*, inscrito(a) no CNPJ/MF sob o nº *[CNPJ]*, sediado(a) na *[endereço]*, na cidade de *[cidade]*/*[UF]*, doravante designado CONTRATADO, neste ato representado(a) por *[nome e função no CONTRATADO]*, conforme *[atos constitutivos da empresa]* ***OU*** *[procuração apresentada nos autos]*, tendo em vista o que consta no Processo nº 01300.003396/2025-91 e em observância às disposições da Lei nº 14.133, de 1º de abril de 2021, e demais legislação aplicável, resolvem celebrar o presente Termo de Contrato, decorrente do(a) *Pregão Eletrônico* nº *XXXX/2026,* mediante as cláusulas e condições a seguir enunciadas.

CLÁUSULA PRIMEIRA – OBJETO

1.1. O objeto do presente instrumento é a contratação de solução de tecnologia da informação e comunicação de aquisição *de solução corporativa de Application Delivery Controller (ADC), baseada na plataforma F5 BIG-IP, com funcionalidades integradas de Web Application Firewall (WAF), a ser instalada em ambiente on-premise no data center do CNPq, contemplando o fornecimento dos appliances, das licenças de software F5 BIG-IP, da garantia e do suporte técnico oficial do fabricante, das subscrições e assinaturas de segurança da solução, bem como dos serviços especializados de instalação, configuração e implantação, dos serviços de suporte técnico especializado da contratada em regime 24x7 e dos serviços de consultoria técnica especializada sob demanda, pelo prazo de 60 (sessenta) meses*, nas condições estabelecidas no Termo de Referência.

1.2. Objeto da contratação:

Grupo 1

Câmara Nacional de Modelos de Licitações e Contratos da Consultoria-Geral da União
Termo de contrato modelo para Pregão Eletrônico para contratação de compras/Solução de Tecnologia da Informação e Comunicação
Aprovado pela Secretaria de Governo Digital
Identidade visual pela Secretaria de Gestão
Atualização: AGO/2025

ITEM	ESPECIFICAÇÃO	CATMAT/ CATSER	UNIDADE DE MEDIDA	QUANTI.	VALOR UNITÁRIO	VALOR TOTAL
1	Appliance de Application Delivery Controller (ADC) baseada na plataforma F5 BIG-IP, com funcionalidades integradas de Web Application Firewall (WAF)	481646	Unidade	2		
2	Licenças de software F5 BIG-IP	27464	Unidade	2		
3	Garantia e suporte técnico oficial do fabricante para a solução F5 BIG-IP	27740	Unidade	2		
4	Subscrições e assinaturas de segurança da plataforma F5 BIG-IP	27502	Unidade	2		
5	Serviços especializados de instalação, configuração e implantação da solução	26972	Unidade	1		
6	Serviços de consultoria técnica especializada (sob demanda)	27340	Hora	480		
7	Serviços de suporte técnico especializado da contratada em regime	27740	Mês	60		

Câmara Nacional de Modelos de Licitações e Contratos da Consultoria-Geral da União
Termo de contrato modelo para Pregão Eletrônico para contratação de compras/Solução de Tecnologia da Informação e Comunicação
Aprovado pela Secretaria de Governo Digital
Identidade visual pela Secretaria de Gestão
Atualização: AGO/2025

	24x7					
VALOR TOTAL						

1.3. Vinculam esta contratação, independentemente de transcrição:

1.3.1. O Termo de Referência;

1.3.2. *O Edital da Licitação;*

1.3.3. A Proposta do contratado;

1.3.4. Eventuais anexos dos documentos supracitados.

CLÁUSULA SEGUNDA – VIGÊNCIA E PRORROGAÇÃO

2.1. O prazo de vigência da contratação é de 5 anos contados da assinatura do contrato, prorrogável para até 10 anos, na forma dos ***arts. 106 e 107 da Lei n° 14.133, de 2021***.

2.2. A prorrogação aplica-se aos serviços de natureza continuada, permanecendo os itens de fornecimento sujeitos à execução única, conforme Termo de Referência.

CLÁUSULA TERCEIRA – MODELOS DE EXECUÇÃO E GESTÃO CONTRATUAIS

3.1. O regime de execução contratual, os modelos de gestão e de execução, assim como os prazos e condições de conclusão, entrega, observação e recebimento do objeto constam no Termo de Referência, anexo a este Contrato.

CLÁUSULA QUARTA – SUBCONTRATAÇÃO

4.1. As regras sobre a subcontratação do objeto são aquelas estabelecidas no Termo de Referência, anexo a este Contrato.

CLÁUSULA QUINTA - PREÇO

5.1. O valor total da contratação é de R$ **xxxxxx** (**xxxxxxxxx**).

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

5.3. O valor acima é meramente estimativo, de forma que os pagamentos devidos ao contratado dependerão dos quantitativos efetivamente fornecidos.

CLÁUSULA SEXTA - PAGAMENTO

6.1. O prazo para pagamento ao contratado e demais condições a ele referentes encontram-se definidos no Termo de Referência, anexo a este Contrato.

CLÁUSULA SÉTIMA - REAJUSTE

7.1. As regras acerca do reajuste do valor contratual são aquelas definidas no Termo de Referência, anexo a este Contrato.

CLÁUSULA OITAVA - OBRIGAÇÕES DO CONTRATANTE

8.1. São obrigações do Contratante, além das previstas no termo de referência:

8.1.1. Exigir o cumprimento de todas as obrigações assumidas pelo Contratado, de acordo com o contrato e seus anexos;

8.1.2. Receber o objeto no prazo e condições estabelecidas no Termo de Referência;

8.1.3. Notificar o Contratado, por escrito, sobre vícios, defeitos incorreções, imperfeições, falhas ou irregularidades verificadas na execução do objeto contratual, fixando prazo para que seja substituído, reparado ou corrigido, total ou parcialmente, às suas expensas, certificando-se de que as soluções por ele propostas sejam as mais adequadas;

8.1.4. Acompanhar e fiscalizar a execução do contrato e o cumprimento das obrigações pelo Contratado;

8.1.5. Efetuar o pagamento ao Contratado do valor correspondente ao fornecimento do objeto, no prazo, forma e condições estabelecidos no presente Contrato e no Termo de Referência;

8.1.6. Aplicar ao Contratado as sanções previstas na lei e neste Contrato;

8.1.7. Cientificar o órgão de representação judicial da Advocacia-Geral da União para adoção das medidas cabíveis quando do descumprimento de obrigações pelo Contratado;

8.1.8. Explicitamente emitir decisão sobre todas as solicitações e reclamações relacionadas à execução do presente Contrato, ressalvados os requerimentos manifestamente impertinentes, meramente protelatórios ou de nenhum interesse para a boa execução do ajuste.

8.1.9. A Administração terá o prazo de 30 (trinta) dias, a contar da data do protocolo do requerimento para decidir, admitida a prorrogação motivada, por igual período.

8.1.10. Responder eventuais pedidos de reestabelecimento do equilíbrio econômico-financeiro feitos pelo contratado no prazo máximo de 30 (trinta) dias.

8.1.11. *Notificar os emitentes das garantias quanto ao início de processo administrativo para apuração de descumprimento de cláusulas contratuais.*

8.2. A Administração não responderá por quaisquer compromissos assumidos pelo Contratado com terceiros, ainda que vinculados à execução do contrato, bem como por qualquer dano causado a terceiros em decorrência de ato do Contratado, de seus empregados, prepostos ou subordinados.

CLÁUSULA NONA - OBRIGAÇÕES DO CONTRATADO

9.1. O Contratado deve 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, observando, ainda, as obrigações a seguir dispostas, além das previstas no termo de referência:

9.1.1. Responsabilizar-se pelos vícios e danos decorrentes do objeto, de acordo com o Código de Defesa do Consumidor (Lei nº 8.078, de 1990);

9.1.2. Comunicar ao contratante, no prazo máximo de 24 (vinte e quatro) horas que antecede a data da entrega, os motivos que impossibilitem o cumprimento do prazo previsto, com a devida comprovação;

9.1.3. Atender às determinações regulares emitidas pelo fiscal ou gestor do contrato ou autoridade superior e prestar todo esclarecimento ou informação por eles solicitados;

9.1.4. 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 verificarem vícios, defeitos ou incorreções resultantes da execução ou dos materiais empregados;

9.1.5. 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;

9.1.6. Quando não for possível a verificação da regularidade no Sistema de Cadastro de Fornecedores – SICAF, o Contratado deverá entregar ao setor responsável pela fiscalização do contrato, junto com a Nota Fiscal para fins de pagamento, os seguintes documentos:

9.1.7.1. prova de regularidade relativa à Seguridade Social;

9.1.7.2. certidão conjunta relativa aos tributos federais e à Dívida Ativa da União;

9.1.7.3. certidões que comprovem a regularidade perante a Fazenda Estadual ou Distrital do domicílio ou sede do CONTRATADO;

9.1.7.4. Certidão de Regularidade do FGTS – CRF; e

9.1.7.5. Certidão Negativa de Débitos Trabalhistas – CNDT.

9.1.7. Responsabilizar-se pelo cumprimento de todas as obrigações trabalhistas, sociais, previdenciárias, tributárias, 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;

9.1.8. Comunicar ao Fiscal do contrato tempestivamente, observada a urgência da situação, qualquer ocorrência anormal ou acidente que se verifique no local da execução do objeto contratual, não ultrapassando o prazo de 24 (vinte e quatro) horas;

9.1.9. 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.

9.1.10. Manter durante toda a vigência do contrato, em compatibilidade com as obrigações assumidas, todas as condições exigidas para habilitação na licitação ou para qualificação na contratação direta;

9.1.11. Cumprir, durante todo o período de execução do contrato, a reserva de cargos prevista em lei para pessoa com deficiência, para reabilitado da Previdência Social ou para aprendiz, bem como as reservas de cargos previstas na legislação;

9.1.12. Comprovar a reserva de cargos a que se refere a cláusula acima, no prazo fixado pelo fiscal do contrato, com a indicação dos empregados que preencheram as referidas vagas;

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

9.1.14. Arcar com o ônus decorrente de eventual equívoco no dimensionamento dos quantitativos de sua proposta, inclusive quanto aos custos variáveis decorrentes de fatores futuros e incertos, devendo complementá-los, caso o previsto inicialmente em sua proposta não seja satisfatório para o atendimento do objeto da contratação, exceto quando ocorrer algum dos eventos arrolados no art. 124, II, d, da Lei nº 14.133, de 2021.

9.1.15. Cumprir, além dos postulados legais vigentes de âmbito federal, estadual ou municipal, as normas de segurança do contratante;

9.1.17. Alocar os empregados necessários ao perfeito cumprimento das cláusulas deste contrato, com habilitação e conhecimento adequados;

9.1.18. Prestar os serviços dentro dos parâmetros e rotinas estabelecidos;

Câmara Nacional de Modelos de Licitações e Contratos da Consultoria-Geral da União
Termo de contrato modelo para Pregão Eletrônico para contratação de compras/Solução de Tecnologia da Informação e Comunicação
Aprovado pela Secretaria de Governo Digital
Identidade visual pela Secretaria de Gestão
Atualização: AGO/2025

9.1.19. Fornecer todos os materiais, equipamentos, ferramentas e utensílios demandados, em quantidade, qualidade e tecnologia adequadas, com a observância às recomendações aceitas pela boa técnica, normas e legislação de regência;

9.1.20. Orientar e treinar seus empregados sobre os deveres previstos na Lei nº 13.709, de 14 de agosto de 2018, adotando medidas eficazes para proteção de dados pessoais a que tenha acesso por força da execução deste contrato;

9.1.21. Conduzir os trabalhos com estrita observância às normas da legislação pertinente, cumprindo as determinações dos Poderes Públicos, mantendo sempre limpo o local de execução do objeto e nas melhores condições de segurança, higiene e disciplina;

9.1.22. Submeter previamente, por escrito, ao CONTRATANTE, para análise e aprovação, quaisquer mudanças nos métodos executivos que fujam às especificações do memorial descritivo ou instrumento congênere;

9.1.23. Cumprir as normas de proteção ao trabalho, inclusive aquelas relativas à segurança e à saúde no trabalho;

9.1.24. Não submeter os trabalhadores a condições degradantes de trabalho, jornadas exaustivas, servidão por dívida ou trabalhos forçados;

9.1.25. Não permitir a utilização de qualquer trabalho do menor de dezesseis anos de idade, exceto na condição de aprendiz para os maiores de quatorze anos de idade, observada a legislação pertinente;

9.1.26. Não submeter o menor de dezoito anos de idade à realização de trabalho noturno e em condições perigosas e insalubres e à realização de atividades constantes na Lista de Piores Formas de Trabalho Infantil, aprovada pelo Decreto nº 6.481, de 12 de junho de 2008;

9.1.27. Receber e dar o tratamento adequado a denúncias de discriminação, violência e assédio no ambiente de trabalho.

CLÁUSULA DÉCIMA – GARANTIA DE EXECUÇÃO

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

CLÁUSULA DÉCIMA PRIMEIRA – INFRAÇÕES E SANÇÕES ADMINISTRATIVAS

11.1. As regras acerca de infrações e sanções administrativas referentes à execução do contrato são aquelas definidas no Termo de Referência, anexo a este Contrato.

CLÁUSULA DÉCIMA SEGUNDA– DA EXTINÇÃO CONTRATUAL

12.1. O contrato será extinto quando vencido o prazo nele estipulado, independentemente de terem sido cumpridas ou não as obrigações de ambas as partes contraentes.

12.1.1. *O contrato poderá ser extinto antes do prazo nele fixado, sem ônus para o Contratante, quando esta não dispuser de créditos orçamentários para sua continuidade ou quando entender que o contrato não mais lhe oferece vantagem.*

12.1.2. *A extinção nesta hipótese ocorrerá na próxima data de aniversário do contrato, desde que haja a notificação do contratado pelo contratante nesse sentido com pelo menos 2 (dois) meses de antecedência desse dia.*

12.1.3. *Caso a notificação da não-continuidade do contrato de que trata este subitem ocorra com menos de 2 (dois) meses da data de aniversário, a extinção contratual ocorrerá após 2 (dois) meses da data da comunicação.*

Câmara Nacional de Modelos de Licitações e Contratos da Consultoria-Geral da União
Termo de contrato modelo para Pregão Eletrônico para contratação de compras/Solução de Tecnologia da Informação e Comunicação
Aprovado pela Secretaria de Governo Digital
Identidade visual pela Secretaria de Gestão
Atualização: AGO/2025

12.2. O contrato poderá ser extinto antes de cumpridas as obrigações nele estipuladas, ou antes do prazo nele fixado, por algum dos motivos previstos no art. 137 da Lei nº 14.133/21, bem como amigavelmente, assegurados o contraditório e a ampla defesa.

12.2.1. Nesta hipótese, aplicam-se também os arts. 138 e 139 da mesma Lei.

12.2.2. A alteração social ou a modificação da finalidade ou da estrutura da empresa não ensejará a extinção se não restringir sua capacidade de concluir o contrato.

12.2.2.1. Se a operação implicar mudança da pessoa jurídica contratada, deverá ser formalizado termo aditivo para alteração subjetiva.

12.3. O termo de extinção, sempre que possível, será precedido:

12.3.1. Do balanço dos eventos contratuais já cumpridos ou parcialmente cumpridos;

12.3.2. Da relação dos pagamentos já efetuados e ainda devidos;

12.3.3. Das indenizações e multas.

12.4. A extinção do contrato não configura óbice para o reconhecimento do desequilíbrio econômico-financeiro, hipótese em que será concedida indenização por meio de termo indenizatório.

12.5. O Contratante poderá ainda:

12.5.1. nos casos de obrigação de pagamento de multa pelo CONTRATADO, reter a garantia prestada a ser executada, conforme legislação que rege a matéria; e

12.5.2. nos casos em que houver necessidade de ressarcimento de prejuízos causados à Administração, nos termos do inciso IV do art. 139 da Lei n.º 14.133, de 2021, reter os eventuais créditos existentes em favor do CONTRATADO decorrentes do contrato.

12.6. O contrato poderá ser extinto caso se constate que o CONTRATADO mantém vínculo de natureza técnica, comercial, econômica, financeira, trabalhista ou civil com dirigente do órgão ou entidade contratante ou com agente público que tenha desempenhado função na licitação ou na contratação direta, ou 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.

CLÁUSULA DÉCIMA TERCEIRA – ALTERAÇÕES

13.1. Eventuais alterações contratuais reger-se-ão pela disciplina dos arts. 124 e seguintes da Lei nº 14.133, de 2021.

13.2. O contratado é obrigado a aceitar, nas mesmas condições contratuais, os acréscimos ou supressões que se fizerem necessários, até o limite de 25% (vinte e cinco por cento) do valor inicial atualizado do contrato.

13.3. As alterações contratuais deverão ser promovidas mediante celebração de termo aditivo, submetido à prévia aprovação da consultoria jurídica do contratante, salvo nos casos de justificada necessidade de antecipação de seus efeitos, hipótese em que a formalização do aditivo deverá ocorrer no prazo máximo de 1 (um) mês (art. 132 da Lei nº 14.133, de 2021).

13.4. 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 nº 14.133, de 2021.

13.5. As supressões resultantes de acordo celebrado entre as partes contratantes poderão exceder o limite de 25% (vinte e cinco por cento) do valor inicial atualizado do contrato.

Câmara Nacional de Modelos de Licitações e Contratos da Consultoria-Geral da União
Termo de contrato modelo para Pregão Eletrônico para contratação de compras/Solução de Tecnologia da Informação e Comunicação
Aprovado pela Secretaria de Governo Digital
Identidade visual pela Secretaria de Gestão
Atualização: AGO/2025

CLÁUSULA DÉCIMA QUARTA – DOTAÇÃO ORÇAMENTÁRIA

14.1. As despesas decorrentes da presente contratação correrão à conta de recursos específicos consignados no Orçamento Geral da União deste exercício, na dotação abaixo discriminada:

I) Gestão/Unidade: [...];
II) Fonte de Recursos: [...];
III) Programa de Trabalho: [...];
IV) Elemento de Despesa: [...];
V) Plano Interno: [...];
VI) Nota de Empenho: [...];

14.2. A dotação relativa aos exercícios financeiros subsequentes será indicada após aprovação da Lei Orçamentária respectiva e liberação dos créditos correspondentes, mediante apostilamento.

CLÁUSULA DÉCIMA QUINTA – DOS CASOS OMISSOS

15.1. Os casos omissos serão decididos pelo contratante, segundo as disposições contidas na Lei nº 14.133, de 2021, e demais normas federais aplicáveis e, subsidiariamente, segundo as disposições contidas na Lei nº 8.078, de 1990 – Código de Defesa do Consumidor – e normas e princípios gerais dos contratos.

CLÁUSULA DÉCIMA SEXTA – PUBLICAÇÃO

16.1. Incumbirá ao contratante divulgar o presente instrumento no Portal Nacional de Contratações Públicas (PNCP), na forma prevista no art. 94 da Lei 14.133, de 2021, bem como no respectivo sítio oficial na Internet, em atenção ao art. 91, *caput,* da Lei n.º 14.133, de 2021, e ao art. 8º, §2º, da Lei n. 12.527, de 2011, c/c art. 7º, §3º, inciso V, do Decreto n. 7.724, de 2012.

CLÁUSULA DÉCIMA SÉTIMA– FORO

17.1. Fica eleito o Foro da Justiça Federal em Brasília, Seção Judiciária do Distrito Federal para dirimir os litígios que decorrerem da execução deste Termo de Contrato que não puderem ser compostos pela conciliação, conforme art. 92, §1º, da Lei nº 14.133, de 2021.

[Local], [dia] de [mês] de [ano].

_____

Representante legal do CONTRATANTE

_____

Representante legal do CONTRATADO

TESTEMUNHAS:

1-

2-

Câmara Nacional de Modelos de Licitações e Contratos da Consultoria-Geral da União
Termo de contrato modelo para Pregão Eletrônico para contratação de compras/Solução de Tecnologia da Informação e Comunicação
Aprovado pela Secretaria de Governo Digital
Identidade visual pela Secretaria de Gestão
Atualização: AGO/2025