PREGÃO ELETRÔNICO N° 90009/2024

CONTRATANTE (UASG)

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

OBJETO

Contratação de solução de segurança de endpoints, servidores de rede, antispam, ambiente de colaboração, mobile, ambiente de containers e gerenciamento de superfície de ataque com atualização contínua, garantia, implantação, suporte técnico e treinamento, nos termos da tabela, conforme condições e exigências estabelecidas no Termo de Referência.

VALOR TOTAL DA CONTRATAÇÃO

R$ 3.923.404,60 (três milhões, novecentos e vinte e três mil, quatrocentos e quatro reais e sessenta centavos).

DATA DA SESSÃO PÚBLICA

Dia 19/11/2024 às 10h (Horário de Brasília)

CRITÉRIO DE JULGAMENTO:

Menor Preço Global

MODO DE DISPUTA:

Aberto e Fechado

PREFERÊNCIA ME/EPP/EQUIPARADAS

Não

Sumário

CONSELHO NACIONAL DE DESENVOLVIMENTO CIENTÍFICO E TECNOLÓGICO - CNPq
DIRETORIA DE GESTÃO ADMINISTRATIVA – DADM
COORDENAÇÃO GERAL DE ADMINISTRAÇÃO E LOGISTICA – CGLOG
SERVIÇO DE COMPRAS E LICITAÇÕES – SELIC

PREGÃO ELETRÔNICO Nº 90009/2024

(Processo Administrativo n° 01300.005789/2023-78)

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, Ed. Telemundi II, Bairro Asa Sul, CEP 70.070-010, Brasília/ DF, realizará licitação, na modalidade PREGÃO, na forma ELETRÔNICA, nos termos da Lei nº 14.133, 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 solução de segurança de endpoints, servidores de rede, antispam, ambiente de colaboração, mobile, ambiente de containers e gerenciamento de superfície de ataque com atualização contínua, garantia, implantação, suporte técnico e treinamento**,** conforme condições, quantidades e exigências estabelecidas neste Edital e seus anexos.

1.2. A licitação será realizada em grupo único, formados por 9 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

2.1.1. Poderão participar deste Pregão 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).

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

2.2. 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.

2.3. 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.

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

2.5. Será concedido tratamento favorecido para as microempresas e empresas de pequeno porte, para as sociedades cooperativas mencionadas no artigo 16 da Lei nº 14.133, de 2021, para o microempreendedor individual - MEI, nos limites previstos da Lei Complementar nº 123, de 2006 e do Decreto n.º 8.538, de 2015, bem como para bens e serviços produzidos com tecnologia produzida no país e bens produzidos de acordo com processo produtivo básico, na forma do art. 3º da Lei nº 8.248, de 1991 e art. 8º do Decreto nº 7.174, de 2010.

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. 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;

2.6.3. 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;

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

2.6.5. 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;

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

2.6.7. 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;

2.6.8. agente público do órgão ou entidade licitante;

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

2.6.10. 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.

2.7. O impedimento de que trata o item 2.6.4 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.

2.8. A critério da Administração e exclusivamente a seu serviço, o autor dos projetos e a empresa a que se referem os itens 2.6.2 e 2.6.3 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.

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

2.10. O disposto nos itens 2.6.2 e 2.6.3 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.

2.11. 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 14.133/2021.

2.12. A vedação de que trata o item 2.6.8 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. DA APRESENTAÇÃO DA PROPOSTA E DOS DOCUMENTOS DE HABILITAÇÃO

3.1. 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.

3.2. 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 7.1.1 e 7.11.1 deste Edital.

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

3.3.1. 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;

3.3.2. 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;

3.3.3. 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;

3.3.4. 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.

3.4. 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.

3.5. O fornecedor enquadrado como microempresa, empresa de pequeno porte ou sociedade cooperativa deverá declarar, ainda, em campo próprio do sistema eletrônico, que cumpre os requisitos estabelecidos no artigo 3° da Lei Complementar nº 123, de 2006, estando apto a usufruir do tratamento favorecido estabelecido em seus arts. 42 a 49, observado o disposto nos §§ 1º ao 3º do art. 4º, da Lei n.º 14.133, de 2021.

3.5.1. no item exclusivo para participação de microempresas e empresas de pequeno porte, a assinalação do campo “não” impedirá o prosseguimento no certame, para aquele item;

3.5.2. 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.

3.6. A falsidade da declaração de que trata os itens 3.3 ou 3.5 sujeitará o licitante às sanções previstas na Lei nº 14.133, de 2021, e neste Edital.

3.7. 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.

3.8. 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.

3.9. 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.

3.10. 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:

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

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

3.11. O valor final mínimo ou o percentual de desconto final máximo parametrizado no sistema poderá ser alterado pelo fornecedor durante a fase de disputa, sendo vedado:

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

3.11.2. percentual de desconto inferior a lance já registrado pelo fornecedor no sistema, quando adotado o critério de julgamento por maior desconto.

3.12. O valor final mínimo ou o percentual de desconto final máximo parametrizado na forma do item 3.10 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.

3.13. 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.

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

4. DO PREENCHIMENTO DA PROPOSTA

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

4.1.1. valor unitário, e total do item;

4.1.2. Marca;

4.1.3. Fabricante;

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

4.2.1. *O* licitante *[NÃO] poderá oferecer proposta em quantitativo inferior ao máximo previsto para contratação.*

4.3. 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.

4.4. 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.

4.5. 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.

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

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

4.8. 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.

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

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

4.10.1. Caso o critério de julgamento seja o de maior desconto, o preço já decorrente da aplicação do desconto ofertado deverá respeitar os preços máximos previstos no item 4.9.

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

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

5.1. 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.

5.2. 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.

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

5.4. 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.

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

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

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

5.8. O intervalo mínimo de diferença de valores ou percentuais entre os lances, que incidirá tanto em relação aos lances intermediários quanto em relação à proposta que cobrir a melhor oferta deverá ser de R$ 0,01 (um centavo).

5.9. 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.

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

5.11. Caso seja adotado para o envio de lances no pregão eletrônico o modo de disputa “aberto e fechado”, os licitantes apresentarão lances públicos e sucessivos, com lance final e fechado.

5.11.1. 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.

5.11.2. 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.

5.11.3. 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.

5.11.4. 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.

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

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

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

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

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

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

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

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

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

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

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

5.18. Será assegurado o direito de preferência previsto no artigo 3º da Lei nº 8.248, de 1991, conforme procedimento estabelecido nos artigos 5° e 8° do Decreto n° 7.174, de 2010, nos seguintes termos:

5.18.1. Após a aplicação das regras de preferência para microempresas e empresas de pequeno porte, caberá a aplicação das regras de preferência, sucessivamente, para:

5.18.1.1. bens e serviços com tecnologia desenvolvida no País e produzidos de acordo com o Processo Produtivo Básico (PPB), na forma definida pelo Poder Executivo Federal;

5.18.1.2. bens e serviços com tecnologia desenvolvida no País; e

5.18.1.3. bens e serviços produzidos de acordo com o PPB, na forma definida pelo Poder Executivo Federal, nos termos do art. 5º e 8º do Decreto 7.174, de 2010 e art. 3º da Lei nº 8.248, de 1991.

5.18.2. Os licitantes classificados que estejam enquadrados no item 5.18.1.1, na ordem de classificação, serão convocados para que possam oferecer nova proposta ou novo lance para igualar ou superar a melhor proposta válida, caso em que será declarado vencedor do certame.

5.18.3. Caso a preferência não seja exercida na forma do item 5.18.1.1, por qualquer motivo, serão convocadas as empresas classificadas que estejam enquadradas no item 5.18.1.2, na ordem de classificação, para a comprovação e o exercício do direito de preferência, aplicando-se a mesma regra para o item 5.18.1.3 caso esse direito não seja exercido.

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

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

5.19.1. 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:

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

5.19.1.2. 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;

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

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

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

5.19.2.1. 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;

5.19.2.2. empresas brasileiras;

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

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

5.20. 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 poderá negociar condições mais vantajosas, após definido o resultado do julgamento.

5.20.1. 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 os seguintes preços unitários máximos como critério de aceitabilidade:

5.20.2. 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.

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

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

5.20.5. O pregoeiro 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.

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

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

6. DA FASE DE JULGAMENTO

6.1. Encerrada a etapa de negociação, o pregoeiro verificará se o licitante provisoriamente classificado em primeiro lugar atende às condições de participação no certame, conforme previsto no art. 14 da Lei nº 14.133/2021, 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:

6.1.1. SICAF;

6.1.2. Cadastro Nacional de Empresas Inidôneas e Suspensas - CEIS, mantido pela Controladoria-Geral da União (https://www.portaltransparencia.gov.br/sancoes/ceis); e

6.1.3. Cadastro Nacional de Empresas Punidas – CNEP, mantido pela Controladoria-Geral da União (https://www.portaltransparencia.gov.br/sancoes/cnep).

6.2. A consulta aos cadastros será realizada em nome da empresa licitante e também de seu sócio majoritário, por força da vedação de que trata o artigo 12 da Lei n° 8.429, de 1992.

6.3. Caso conste na Consulta de Situação do licitante a existência de Ocorrências Impeditivas Indiretas, o Pregoeiro diligenciará para verificar se houve fraude por parte das empresas apontadas no Relatório de Ocorrências Impeditivas Indiretas. (IN nº 3/2018, art. 29, *caput*)

6.3.1. A tentativa de burla será verificada por meio dos vínculos societários, linhas de fornecimento similares, dentre outros. (IN nº 3/2018, art. 29, §1º).

6.3.2. O licitante será convocado para manifestação previamente a uma eventual desclassificação. (IN nº 3/2018, art. 29, §2º).

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

6.4. Caso atendidas as condições de participação, será iniciado o procedimento de habilitação.

6.5. Caso o licitante provisoriamente classificado em primeiro lugar tenha se utilizado de algum tratamento favorecido às ME/EPPs, o pregoeiro verificará se faz jus ao benefício, em conformidade com os itens 3.5.1 e 4.6 deste edital.

6.6. Verificadas as condições de participação e de utilização do tratamento favorecido, o pregoeiro examinará a proposta classificada em primeiro lugar quanto à adequação ao objeto e à compatibilidade do preço em relação ao máximo estipulado para contratação neste Edital e em seus anexos, observado o disposto no artigo 29 a 35 da IN SEGES nº 73, de 30 de setembro de 2022.

6.7. Será desclassificada a proposta vencedora que:

6.7.1. contiver vícios insanáveis;

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

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

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

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

6.8. 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.

6.8.1. A inexequibilidade, na hipótese de que trata o **caput**, só será considerada após diligência do pregoeiro, que comprove:

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

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

6.9. 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.

6.10. 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.

6.10.1. Caso a produtividade for diferente daquela utilizada pela Administração como referência, ou não estiver contida na faixa referencial de produtividade, mas admitida pelo ato convocatório, o licitante deverá apresentar a respectiva comprovação de exequibilidade;

6.10.2. Os licitantes poderão apresentar produtividades diferenciadas daquela estabelecida pela Administração como referência, desde que não alterem o objeto da contratação, não contrariem dispositivos legais vigentes e, caso não estejam contidas nas faixas referenciais de produtividade, comprovem a exequibilidade da proposta.

6.10.3. Para efeito do subitem anterior, admite-se a adequação técnica da metodologia empregada pela contratada, visando assegurar a execução do objeto, desde que mantidas as condições para a justa remuneração do serviço.

6.11. 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;

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

6.13. 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.

6.14. 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.

6.15. Caso o Termo de Referência exija a apresentação de amostra, o licitante classificado em primeiro lugar deverá apresentá-la, conforme disciplinado no Termo de Referência, sob pena de não aceitação da proposta.

6.16. Por meio de mensagem no sistema, será divulgado o local e horário de realização do procedimento para a avaliação das amostras, cuja presença será facultada a todos os interessados, incluindo os demais licitantes.

6.17. Os resultados das avaliações serão divulgados por meio de mensagem no sistema.

6.18. No caso de não haver entrega da amostra ou ocorrer atraso na entrega, sem justificativa aceita pelo Pregoeiro, ou havendo entrega de amostra fora das especificações previstas neste Edital, a proposta do licitante será recusada.

6.19. Se a(s) amostra(s) apresentada(s) pelo primeiro classificado não for(em) aceita(s), o Pregoeiro analisará a aceitabilidade da proposta ou lance ofertado pelo segundo classificado. Seguir-se-á com a verificação da(s)

amostra(s) e, assim, sucessivamente, até a verificação de uma que atenda às especificações constantes no Termo de Referência.

6.20. Caso o Termo de Referência exija prova de conceito, o licitante classificado em primeiro lugar será convocado pelo pregoeiro, com antecedência mínima de 15 (quinze) dias úteis da data estabelecia para sua realização, para executá-la, visando aferir o atendimento dos requisitos e funcionalidades mínimas da solução de tecnologia da informação e comunicação, conforme disciplinado no Termo de Referência.

6.21. Por meio de mensagem no sistema, será divulgado o local e horário de realização do procedimento para a realização da prova de conceito.

6.22. A prova de conceito será realizada por equipe técnica designada, responsável pela aferição do atendimento dos itens estabelecidos, e poderá ser acompanhada pelos demais licitantes, mediante registro formal junto ao pregoeiro.

6.23. Todas as despesas decorrentes de participação ou acompanhamento da prova de conceito são de responsabilidade de cada um dos licitantes.

6.24. A equipe técnica elaborará relatório com o resultado da prova de conceito, informando se a solução apresentada pelo licitante provisoriamente classificado em primeiro lugar está ou não de acordo com os requisitos e funcionalidades estabelecidas.

6.25. Caso o relatório indique que a solução tecnológica está em conformidade com as especificações exigidas, o licitante será declarado vencedor do processo licitatório e, caso indique a não conformidade, o licitante será desclassificado do processo licitatório.

6.26. Caso o relatório indique que a solução foi aprovada com ressalvas, as não conformidades serão listadas e o licitante terá prazo de 3 (três) dias úteis, não prorrogáveis, a contar da data de ciência do respectivo relatório, para proceder aos ajustes necessários na solução e disponibilizá-la, para a realização de testes complementares, para aferição da correção ou não das inconformidades indicada.

6.27. Poderá ser considerada aprovada com ressalva a solução que, embora possua todas as funcionalidades previstas na Prova de Conceito (PoC), venha a apresentar falha durante o teste.

6.28. Caso o novo relatório indique a não conformidade da solução ajustada às especificações técnicas exigidas, a licitante será desclassificada do processo licitatório.

6.29. Não será aceita a proposta da licitante que tiver a prova de conceito rejeitada, que não a realizar ou que não a realizar nas condições estabelecidas no Termo de Referência.

6.30. No caso de desclassificação do licitante, o pregoeiro convocará o próximo licitante, obedecida a ordem de classificação, sucessivamente, até que um licitante cumpra os requisitos e funcionalidades previstas na PoC.

6.31. Os resultados das avaliações serão divulgados por meio de mensagem no sistema.

7. DA FASE DE HABILITAÇÃO

7.1. 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.

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

7.2. 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.

7.3. 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.

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

7.5. 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.

7.6. 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 (art. 63, I, da Lei nº 14.133/2021).

7.7. 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.

7.8. 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.

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

7.9.1. 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. (IN nº 3/2018, art. 4º, §1º, e art. 6º, §4º).

7.10. 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. (IN nº 3/2018, art. 7º, *caput*).

7.10.1. A não observância do disposto no item anterior poderá ensejar desclassificação no momento da habilitação. (IN nº 3/2018, art. 7º, parágrafo único).

7.11. A verificação pelo pregoeiro, em sítios eletrônicos oficiais de órgãos e entidades emissores de certidões constitui meio legal de prova, para fins de habilitação.

7.11.1. 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.

7.11.2. 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.*

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

7.12.1. 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.

7.12.2. 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.

7.13. Após a entrega dos documentos para habilitação, não será permitida a substituição ou a apresentação de novos documentos, salvo em sede de diligência, para (Lei 14.133/21, art. 64, e IN 73/2022, art. 39, §4º):

7.13.1. complementação de informações acerca dos documentos já apresentados pelos licitantes e desde que necessária para apurar fatos existentes à época da abertura do certame; e

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

7.14. 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.

7.15. Na hipótese de o licitante não atender às exigências para habilitação, o pregoeiro 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 7.11.1.

7.16. 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.

7.17. 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 (art. 4º do Decreto nº 8.538/2015).

7.18. 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.

8. DOS RECURSOS

8.1. 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.

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

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

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

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

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

8.3.3. 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.

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

8.5. 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.

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

8.7. 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.

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

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

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

9. DAS INFRAÇÕES ADMINISTRATIVAS E SANÇÕES

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

9.1.1. deixar de entregar a documentação exigida para o certame ou não entregar qualquer documento que tenha sido solicitado pelo/a pregoeiro/a durante o certame;

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

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

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

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

9.1.2.4. deixar de apresentar amostra;

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

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

9.1.3.1. 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;

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

9.1.5. fraudar a licitação;

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

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

9.1.6.2. induzir deliberadamente a erro no julgamento;

9.1.6.3. apresentar amostra falsificada ou deteriorada;

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

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

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

9.2.1. advertência;

9.2.2. multa;

9.2.3. impedimento de licitar e contratar e

9.2.4. 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.

9.3. Na aplicação das sanções serão considerados:

9.3.1. a natureza e a gravidade da infração cometida.

9.3.2. as peculiaridades do caso concreto

9.3.3. as circunstâncias agravantes ou atenuantes

9.3.4. os danos que dela provierem para a Administração Pública

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

9.4. A multa será recolhida em percentual de 0,5% a 30% incidente sobre o valor do contrato licitado, recolhida no prazo máximo de 10(dez) dias úteis, a contar da comunicação oficial.

9.4.1. Para as infrações previstas nos itens 9.1.1, 9.1.2 e 9.1.3, a multa será de 0,5% a 15% do valor do contrato licitado.

9.4.2. Para as infrações previstas nos itens 9.1.4, 9.1.5, 9.1.6, 9.1.7 e 9.1.8, a multa será de 15% a 30% do valor do contrato licitado.

9.5. 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.

9.6. 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.

9.7. A sanção de impedimento de licitar e contratar será aplicada ao responsável em decorrência das infrações administrativas relacionadas nos itens 9.1.1, 9.1.2 e 9.1.3, 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.

9.8. Poderá ser aplicada ao responsável a sanção de declaração de inidoneidade para licitar ou contratar, em decorrência da prática das infrações dispostas nos itens 9.1.4, 9.1.5, 9.1.6, 9.1.7 e 9.1.8, bem como pelas infrações administrativas previstas nos itens 9.1.1, 9.1.2 e 9.1.3 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 n.º 14.133/2021.

9.9. 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 9.1.3, caracterizará o descumprimento total da obrigação assumida e o sujeitará às penalidades e à imediata perda 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.

9.10. 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.

9.11. 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.

9.12. 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.

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

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

10. DA IMPUGNAÇÃO AO EDITAL E DO PEDIDO DE ESCLARECIMENTO

10.1. 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.

10.2. 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.

10.3. 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: 70.070-010 – Serviço de Compras e Licitações – SELIC, 4° andar.

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

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

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

11. DAS DISPOSIÇÕES GERAIS

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

11.2. 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.

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

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

11.5. 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.

11.6. 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.

11.7. 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.

11.8. 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.

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

11.10. O Edital e seus anexos estão disponíveis, na íntegra, no Portal Nacional de Contratações Públicas (PNCP) e endereço eletrônico https://www.gov.br/compras/ptbr/ e http://www.cnpq.br/web/guest/licitacoes/ e também poderão ser lidos e/ ou obtidos no endereço Setor de Autarquias Sul (SAUS) Quadra 01, Lote 06, Bloco H, Edifício Telemundi II, Bairro Asa Sul, Brasília/DF – CEP: 70.070-010 – Serviço de Compras e Licitações – SELIC, 4° andar, nos dias úteis no horário das 9h30 ás 11h30 e das 14h30 ás 17h30.

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

11.12. ANEXO I - Termo de Referência;

11.12.1. ANEXO I do Termo de Referência – Termo de Compromisso de Manutenção de Sigilo e Termo de Confidencialidade e Sigilo;

11.12.2. ANEXO II do Termo de Referência – Níveis Mínimos de Serviço;

11.12.3. ANEXO III do Termo de Referência – Modelo do Termo de Vistoria Técnica;

11.12.4. ANEXO IV do Termo de Referência – Modelo de Recusa de Vistoria Técnica;

11.12.5. ANEXO V do Termo de Referência – Modelo da Ordem de Serviço;

11.12.6. ANEXO VI do Termo de Referência – Modelo dos Termos de Recebimento Provisório e Definitivo;

11.12.7. ANEXO VII do Termo de Referência – Requisitos Técnicos das Soluções;

11.12.8. ANEXO VIII do Termo de Referência – Modelo da Planilha de Custos e Formação de Preços;

11.12.8.1. Apêndice do Anexo I – Estudo Técnico Preliminar; e

11.12.9. ANEXO II – Minuta de Termo de Contrato.

Brasília, DF, 31 de outubro de 2024.

Victor Ferreira Dantas
Pregoeiro Oficial
Portaria CNPq n° 1.936/2024

CONSELHO NACIONAL DE DESENVOLVIMENTO CIENTÍFICO E TECNOLÓGICO
Setor de Autarquias Sul (SAUS), Quadra 01, Lote 06, Bloco H - Bairro Asa Sul - CEP 70070-010 - Brasília - DF - www.gov.br/cnpq
Edifício Telemundi II

TERMO DE REFERÊNCIA

Processo Administrativo n.º 01300.005789/2023-78

CONTRATAÇÃO DE SOLUÇÕES DE SEGURANÇA DE ENDPOINTS, SERVIDORES DE REDE, ANTISPAM, AMBIENTE DE COLABORAÇÃO, MOBILES, CONTAINERS E GERENCIAMENTO DE SUPERFÍCIE DE ATAQUE

Referência: Arts. 12 a 24 da Instrução Normativa SGD/ME n.º 94, de 2022

1 - CONDIÇÕES GERAIS DA CONTRATAÇÃO

1.1. Contratação de solução de segurança de *endpoints*, servidores de rede, *antispam,* ambiente de colaboração, *mobile,* ambiente de containers e gerenciamento de superfície de ataque com atualização contínua, garantia, implantação, suporte técnico e treinamento, nos termos da tabela abaixo, conforme condições e exigências estabelecidas neste instrumento.

GRUPO	ITEM	ESPECIFICAÇÃO	CATSER	UNIDADE	QUANTIDADE	VALOR UNITÁRIO	VALOR TOTAL
1	1	Solução de segurança para *endpoints Trend Vision One - Endpoint Security Essentials*	27502	Unidade	1.200	R$ 351,82	R$ 422.184,00
	2	Solução de segurança para servidores físicos, virtuais e em nuvem *Trend Vision One - Endpoint Security Pro*	27502	Unidade	500	R$ 3.000,46	R$ 1.500.230,00
	3	Solução de segurança para e-mails (*antispam*) e ambiente de colaboração *Trend Micro One Email and Collaboration Security - Pro*	27502	Unidade	1.200	R$ 939,43	R$ 1.127.316,00
	4	Solução de segurança para containers *Trend Cloud One Container*	27502	Unidade	10	R$ 11.553,99	R$ 115.539,90
	5	Solução de segurança para	27502	Unidade	50	R$ 116,51	R$ 5.825,50

		dispositivos *mobile Trend Micro Mobile Security*					
	6	Gerenciamento de risco e superfície de ataque *Attack Surface Risk Management (ASRM)*	27502	Unidade	1.700	R$ 238,02	R$ 404.634,00
	7	Instalação/configuração das soluções	26972	Unidade	1	R$ 79.166,66	R$ 79.166,66
	8	Suporte técnico, garantia e atualização 24x7	27332	Mês	24	R$ 9.450,00	R$ 226.800,00
	9	Treinamento das soluções de segurança	3840	Pessoa	2	R$ 20.854,27	R$ 41.708,54
TOTAL							**R$ 3.923.404,60**

1.2. Os serviços objeto desta contratação são caracterizados como comuns, uma vez que seus padrões de desempenho e qualidade são objetivamente definidos por este Termo de Referência, por meio de especificações usuais de mercado.
1.3. O prazo de vigência da contratação é de 24 (vinte e quatro) meses, contados da assinatura do contrato, prorrogável para até 10 anos, na forma dos artigos 106 e 107 da Lei n.º 14.133, de 2021.
1.3.1. O serviço é enquadrado como continuado tendo em vista que é essencial para o adequado funcionamento da instituição, sendo que sua interrupção pode comprometer a continuidade de atividades da Administração, além da necessidade da contratação dever se estender por mais de um exercício financeiro continuamente, dadas as ameaças de invasão, sequestro de dados e *malwares* que podem corromper dados e sistemas que impediriam o bom funcionamento do órgão, sendo a vigência plurianual mais vantajosa considerando o Estudo Técnico Preliminar.
1.4. O contrato oferece maior detalhamento das regras que serão aplicadas em relação à vigência da contratação.

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

2.1. A descrição da solução como um todo encontra-se pormenorizada em tópico específico dos Estudos Técnicos Preliminares, apêndice deste Termo de Referência.
2.2. O avanço acelerado da digitalização e da internet ampliou significativamente as vulnerabilidades e criou novas formas de ataques cibernéticos. Nesse cenário, é fundamental adotar soluções robustas de segurança para proteger ativos de TI e garantir a integridade, confidencialidade e disponibilidade dos dados.
2.3. Dados do Centro de Estudos, Resposta e Tratamento de Incidentes e Segurança no Brasil - CERT.br 2023 (*https://stats.cert.br/incidentes/*) apontam um aumento de 19% nos ataques a servidores web, destacando a necessidade de medidas de segurança proativas. Com o crescimento de ameaças como *ransomware*, SQL Injection e *malwares*, a proteção do ambiente de TI do CNPq, que presta serviços críticos à comunidade científica e à sociedade, deve ser aprimorada. Além disso, a Lei Geral de Proteção de Dados (LGPD) exige a adoção de soluções que garantam a segurança e privacidade dos dados, o que reforça a necessidade de atualizar a infraestrutura de cibersegurança da instituição.
2.4. O TCU, por meio do TC001.873/2020-2, também destaca a importância da implementação de controles críticos de segurança cibernética, conforme o *framework* do *Center for Internet Security* (CIS). O controle de defesa contra *malwares*, por exemplo, recomenda a utilização de ferramentas centralizadas que previnam, detectem e respondam rapidamente a ameaças em toda a infraestrutura de TI, incluindo *endpoints*, servidores, redes e ambientes de colaboração.
2.5. O controle 10 do CIS v8 - Defesas contra *malwares* - reforça a necessidade de se controlar ou impedir a instalação, disseminação e execução de aplicações, códigos ou scripts maliciosos em ativos corporativos prevenindo, detectando e corrigindo os pontos fracos de segurança antes que possam afetar, no caso, o CNPq.

Por essa razão, a proteção eficaz contra *malware* inclui conjuntos tradicionais de prevenção e detecção de *malware* de *endpoint*. Essas ferramentas são mais bem gerenciadas de forma centralizada para fornecer consistência em toda a infraestrutura. Quando tratamos de uma solução de segurança avançada integrada de prevenção, detecção e resposta esse controle se relaciona como uma abordagem holística para a detecção e resposta a ameaças, que envolve a integração e correlação de dados de várias fontes em uma única plataforma. Essa abordagem permite que as equipes de segurança monitorem e analisem as atividades de segurança em toda a infraestrutura de TI, incluindo redes, *endpoints* e aplicativos.

2.6. Dessa maneira uma solução de segurança avançada integrada de prevenção, detecção e resposta deve ser capaz de analisar os dados coletados em tempo real, utilizando algoritmos avançados para identificar comportamentos suspeitos, devendo ser capaz de compartilhar inteligência de ameaças com outras ferramentas de segurança, como soluções de SIEM/SOAR. Além disso, ela deverá ser capaz de automatizar a detecção e a resposta a incidentes, incluindo a remediação de ameaças, a isolação de sistemas comprometidos e a coleta de evidências forenses. Isso tudo sem esquecer que ela deverá dispor de uma oferta de relatórios detalhados e trilhas de auditoria para fins de conformidade e gerenciamento de riscos.

2.7. O Gartner prevê que, até 2027, 50% das organizações usarão uma solução desse tipo para melhorar a detecção e resposta a ameaças. O Gartner também destaca a importância da integração das soluções de segurança avançada integrada de prevenção, detecção e resposta com outras ferramentas de segurança, como soluções de gerenciamento de informações e eventos de segurança (SIEM), soluções de prevenção de intrusões (IPS) e soluções de gerenciamento de vulnerabilidades (VMS), para fornecer uma visão mais abrangente das atividades de segurança.

2.8. Diante dos desafios criados pelos processos de transformação digital das organizações públicas e pelos desafios de dependência tecnológica impostos pela Covid-19, acabou por forçar as organizações a expandir seu ambiente de trabalho em regime remoto. Dessa forma, os ambientes das organizações tornaram-se mais visíveis e vulneráveis a ataques com roubo de informações além da possibilidade de comprometimento do ambiente do CNPq, a exemplo o expressivo aumento dos casos de *ransomware*.

2.9. Em ataques cibernéticos recentes, grupos de hackers têm considerado sistemas de governo como alvos compensadores, no intuito de provocar diferentes impactos, como: o potencial dano à imagem do Governo perante seu público interno e perante a comunidade internacional, o descrédito da população nos serviços públicos, a desconfiança de investidores internacionais na capacidade da administração pública em proteger seus próprios sistemas, a desconfiança nos processos eleitorais e o descontentamento da população com relação à Administração Pública.

2.10. Uma vez que o CNPq não possui soluções dedicadas para gerar visibilidade centralizada de eventos de segurança, a pretensa contratação vai diretamente a encontro destas necessidades, contribuindo de forma considerável para o aumento do nível de maturidade em segurança da informação do ambiente tecnológico da Instituição em diversas camadas além do cumprimento aos requisitos legais.

3 - FUNDAMENTAÇÃO E DESCRIÇÃO DA NECESSIDADE DA CONTRATAÇÃO

3.1. A paisagem de ameaças cibernéticas tem se tornado cada vez mais complexa e diversificada. O contrato anterior, firmado em 2018 e que utiliza a solução da fabricante Trend Micro, cobria *endpoints* e servidores. Entretanto, essa cobertura não contempla os novos vetores de ataque. Apesar da solução implementada pelo CNPq estar em operação há mais de 10 (dez) anos e atender satisfatoriamente, ameaças mais sofisticadas, como *ransomware, phishing* e exploração de vulnerabilidades específicas em *containers* e dispositivos móveis, exigem uma abordagem mais ampla e integrada.

3.2. O uso de *containers*, como *Docker* e *Kubernetes*, vem crescendo significativamente devido à sua eficiência e escalabilidade. No entanto, eles também trazem novos desafios de segurança, como a gestão de imagens inseguras, vulnerabilidades em ambientes orquestrados e a falta de visibilidade em tempo real. Uma solução de segurança dedicada a *containers* permitirá monitoramento contínuo, correção de vulnerabilidades e proteção contra ameaças específicas a esse ambiente.

3.3. Em relação aos dispositivos móveis, observa-se um aumento expressivo na adoção dessas tecnologias no ambiente corporativo, tanto para fins de comunicação quanto para acesso a dados e sistemas. Isso, por sua vez, amplia os riscos de ataques cibernéticos. A falta de uma solução específica para a proteção desses dispositivos pode expor a organização a ameaças como *malwares* móveis, aplicativos maliciosos e ataques de *phishing* voltados especificamente para dispositivos móveis.

3.4. Ferramentas de colaboração, como e-mails corporativos, aplicativos de comunicação (Microsoft Teams, Slack, etc.) e plataformas de compartilhamento de arquivos, tornaram-se essenciais para a operação das organizações. Entretanto, esses ambientes são frequentemente alvo de ataques, como *phishing*, *malware* distribuído por anexos e tentativas de roubo de credenciais. A respeito do serviço de *antispam*, com a crescente dependência da comunicação eletrônica, as empresas tornaram-se mais vulneráveis a uma inundação constante de mensagens não solicitadas, conhecidas como *spam*. Esta avalanche de e-mails indesejados pode comprometer a eficiência operacional, desperdiçar tempo valioso dos funcionários e aumentar os riscos de segurança cibernética. A contratação de um software de *antispam* torna-se uma necessidade crítica para mitigar estes desafios, visto que atualmente o CNPq não dispõe de um contrato ativo deste tipo de solução, sendo não apenas uma medida preventiva, mas também uma parte essencial da estratégia de segurança cibernética e gestão de comunicações. Ao investir em tecnologias robustas, as organizações podem proteger seus ativos digitais e garantir uma operação suave e eficiente, livre das perturbações causadas pelo dilúvio constante de *spam*.

3.5. A superfície de ataque das organizações tem se expandido significativamente com o aumento da digitalização e do trabalho remoto. Sem uma solução abrangente que possibilite mapear, monitorar e mitigar vulnerabilidades em todos os pontos de contato digital, a organização se torna vulnerável a explorações não monitoradas, como brechas de segurança em dispositivos conectados, redes e aplicações em nuvem.

3.6. Diversas regulamentações, como a LGPD (Lei Geral de Proteção de Dados) e outras normas de proteção de dados, exigem que as organizações mantenham uma infraestrutura de segurança robusta e abrangente para proteger dados sensíveis. Uma cobertura limitada apenas a *endpoints* e servidores não é suficiente para atender a essas exigências, especialmente em setores que lidam com grandes volumes de dados pessoais e sensíveis.

3.7. Expandir a cobertura de segurança reduz consideravelmente a probabilidade e o impacto de incidentes cibernéticos. Brechas em ambientes não protegidos, como *containers*, dispositivos móveis e plataformas de colaboração, podem gerar custos significativos para a organização, tanto em termos financeiros quanto reputacionais. Investir em uma segurança proativa ajuda a mitigar esses riscos de forma eficaz.

3.8. Destaca-se que uma gestão centralizada das tecnologias permite uma administração mais eficiente e coerente de todos os recursos de segurança, facilitando a implementação de políticas, monitoramento e manutenção de toda a infraestrutura de TI, alinhando-se ao Decreto n.º 10.222, de 5 de fevereiro de 2020, referente à Estratégia Nacional de Segurança Cibernética - E-Ciber. Essa abordagem unificada permite uma resposta mais rápida e eficaz a incidentes de segurança, garantindo uma postura defensiva mais proativa e resiliente. Adotar uma única solução de segurança que cubra *endpoints*, servidores, e-mails, ambientes de colaboração, *containers*, dispositivos móveis, gerenciamento de risco e superfície de ataque oferece várias vantagens estratégicas e operacionais para o CNPq. Essa abordagem centralizada não apenas fortalece a postura de segurança, mas também simplifica a gestão e promove maior eficiência em toda a organização. Uma plataforma unificada proporciona visibilidade centralizada de todos os ativos e áreas de TI, permitindo o monitoramento contínuo e a gestão de ameaças em tempo real. Isso capacita a equipe de segurança a detectar, investigar e responder rapidamente a incidentes, reduzindo o tempo de resposta e minimizando o impacto das ameaças.

3.9. Uma pesquisa recente do Gartner (Gartner Survey Shows 75% of Organizations Are Pursuing Security Vendor Consolidation in 2022) mostrou que as organizações querem consolidar seus fornecedores de segurança para reduzir a complexidade e melhorar a postura a riscos. Longos processos de aquisição ou solicitações de propostas estão permitindo ofertas consolidadas, como XDR para *endpoints* e SASE para conectividade de ponta e segurança com integração no *backend*.

3.10. A consolidação de cibersergurança se apresenta como uma estratégia viável para enfrentar as crescentes ameaças do ambiente digital, especialmente em regiões emergentes como a América Latina. Em entrevista à Security Report (https://securityleaders.com.br/consolidacao-de-ciberseguranca-eficiencia-ou-risco/), o Diretor Global de Alianças em Segurança da Informação da Hitachi Vantara, BJ Deonarain, explica que a região segue vulnerável a ataques como *ransomware* e *phishing*. Na visão do executivo, a consolidação em uma solução pode ser uma solução para reduzir a complexidade das arquiteturas de segurança da informação, além de promover maior eficiência e controle de custos.

3.11. A utilização de diversas soluções de segurança de fornecedores diferentes tende a aumentar a complexidade de integração, gerenciamento e suporte. Por outro lado, uma solução única simplifica esses processos, facilitando a implementação de políticas de segurança consistentes e uniformes em todos os sistemas e dispositivos. Essa simplificação também alivia a carga de trabalho da equipe de TI, melhorando a eficiência operacional e permitindo que o foco seja direcionado para iniciativas mais estratégicas.

3.12. Além disso, a adoção de uma solução unificada favorece a conformidade com regulamentações de segurança e privacidade, como a LGPD e o GDPR. Com todos os dados e logs de segurança geridos em uma plataforma única, auditorias e verificações de conformidade tornam-se mais fáceis, garantindo que as políticas de segurança sejam aplicadas de maneira consistente em toda a organização.

3.13. Soluções de segurança integradas também oferecem um suporte superior para a automação de respostas a incidentes (SOAR) e a orquestração de processos. Isso permite a execução de ações automáticas para mitigar ameaças, muitas vezes sem a necessidade de intervenção humana. Como resultado, a resposta a incidentes é mais rápida, o que reduz o potencial de danos causados por ataques e otimiza o uso dos recursos humanos da equipe de segurança, permitindo que se concentrem em ameaças mais complexas.

3.14. Outra vantagem altamente significativa é a cobertura robusta e amplificada de grande parte de vetores de ataque. Uma solução unificada adota uma abordagem de "defesa em profundidade", onde várias camadas de segurança se complementam, fechando lacunas de proteção que poderiam ser exploradas por ameaças avançadas. Isso fortalece a resiliência da organização contra ataques sofisticados.

3.15. Para os usuários finais, o uso de uma solução integrada resulta em uma experiência mais fluida e menos invasiva. A redução da necessidade de múltiplos logins, notificações redundantes ou softwares distintos melhora a produtividade, sem comprometer a segurança, proporcionando um ambiente mais estável e seguro.

3.16. No aspecto operacional, a gestão de patches e atualizações de segurança também é simplificada em uma solução unificada. Áreas críticas podem ser atualizadas de forma coordenada, minimizando os riscos de vulnerabilidades decorrentes de falhas ou atrasos em atualizações.

3.17. Além disso, uma plataforma integrada facilita a identificação e o controle de ativos e sistemas não autorizados, conhecidos como "*shadow IT*". Isso melhora a governança da TI, reduzindo os riscos associados ao uso de ferramentas não aprovadas pela organização, garantindo maior controle e segurança sobre os recursos de TI. Destaca-se também que, quando diferentes soluções que trabalham "integradas" não é incomum o surgimento de algum problema e, em situações como estas, há uma disputa entre os fabricantes sobre quem é o responsável, interferindo na resolução do impedimento e impactando a instituição.

3.18. Por fim, a implementação e gestão de diversas soluções de segurança geralmente resultam em custos mais altos, tanto em licenciamento quanto em manutenção. Com uma única solução, esses custos são consolidados, permitindo que a organização aproveite economias de escala. Além disso, a redução da necessidade de integração personalizada entre ferramentas diferentes reduz o custo total de propriedade, já que os investimentos em treinamento, implantação e suporte também são centralizados e otimizados. Isso resulta em uma estratégia mais econômica e eficiente para o CNPq.

3.19. A contratação promoverá meios para se alcançar:

3.19.1. Eliminação de custos com manutenção dos hardwares e softwares, em razão de danos provocados por vírus e ataques de todos os gêneros.

3.19.2. Identificação e bloqueio, em tempo real, de ataques, invasões ou sabotagens.

3.19.3. Redução dos riscos relacionados à imagem institucional, perda de receita e descumprimento de normas e regulamentos.

3.19.4. Atualização tecnológica constante de soluções de segurança.

3.19.5. Aumento e manutenção de elevados níveis de segurança nos ambientes de TI protegidos.

3.19.6. Gestão da segurança da rede proporcionando o uso racional de recursos técnicos e financeiros.

3.19.7. Utilização de equipamentos e softwares com tecnologia de cibersegurança atualizada.

3.19.8. Redução dos custos operacionais, uma vez que o gerenciamento das ferramentas de segurança será único e integrado.

3.20. O objeto da contratação também está alinhado com a Estratégia de Governo Digital 2024-2027 e em consonância com o Plano Diretor de Tecnologia da Informação e Comunicação 2022-2024 do CNPq, conforme demonstrado abaixo:

ALINHAMENTO AOS PDTIC 2022-2024	
Necessidade de Contratação (NC)	
NC 017	Solução de Antivírus
NC 040	Solução de Antispam
Necessidades de Serviço (NS)	
NS 006	Disponibilidade dos recursos, soluções e serviços de TIC

NS 007	Monitoramento dos recursos, soluções e serviços de TIC
NS 014	Ambiente computacional corporativo seguro
NS 024	Modernização e atualização de recursos e soluções de TIC
Plano de Gerenciamento de Contratações (PGC)	
36/2024	Solução de segurança de endpoints, servidores de rede e antispam.
Estratégia de Governo Digital 2024-2027	
Objetivo 4	Ampliar a resiliência e a maturidade das estruturas tecnológicas governamentais com atenção à privacidade, proteção de dados pessoais, segurança da informação e segurança cibernética.

4 - REQUISITOS DA CONTRATAÇÃO

4.1. Requisitos de negócio

4.1.1. De maneira inicial e não exaustiva podemos listar as seguintes necessidades de negócio:

- **Solução de segurança para *endpoint*:** é um software projetado para proteger dispositivos finais, como computadores, laptops e dispositivos móveis, contra uma variedade de ameaças digitais, incluindo *malware*, *ransomware*, *phishing* e outras formas de ataques cibernéticos. Essas soluções geralmente incluem recursos como antivírus, firewall, detecção de intrusão, controle de aplicativos e proteção de dados, visando garantir a integridade, confidencialidade e disponibilidade dos dados armazenados nos dispositivos e na rede corporativa.
- **Solução de segurança para servidores físicos, virtuais e em nuvem:** é um conjunto integrado de medidas e ferramentas destinadas a proteger os ativos de uma organização em ambientes de TI diversos. Essas soluções devem adaptar-se às peculiaridades de cada tipo de infraestrutura, garantindo a proteção de servidores físicos contra acessos não autorizados e ataques físicos, a segurança de servidores virtuais contra ameaças digitais e a integridade dos dados e aplicações em ambientes de nuvem, onde a responsabilidade pela segurança é compartilhada entre o provedor de serviços e o usuário.
- **Solução de segurança para e-mails (*antispam*):** é um conjunto de tecnologias e medidas projetadas para filtrar e-mails indesejados e potencialmente perigosos, como *spam*, *phishing* e *malware*, antes que cheguem à caixa de entrada dos usuários. Essas soluções utilizam uma variedade de métodos, como listas negras, análise de conteúdo, verificação de reputação de remetentes, assinaturas de malware e aprendizado de máquina, para identificar e bloquear mensagens maliciosas, protegendo assim os usuários e a infraestrutura de TI contra ameaças cibernéticas relacionadas a e-mails.
- **Solução de segurança para ambiente de colaboração:** é um software projetado para proteger plataformas de colaboração online, como intranets, sistemas de mensagens instantâneas, compartilhamento de arquivos e espaços de trabalho colaborativos, contra uma variedade de ameaças cibernéticas. Essas soluções incluem recursos como controle de acesso, criptografia de dados, monitoramento de atividades suspeitas, prevenção contra vazamento de dados e integração com outras soluções de segurança, visando garantir a confidencialidade, integridade e disponibilidade das informações compartilhadas entre os colaboradores, enquanto mantém a conformidade regulatória e protege a reputação e os ativos da organização.
- **Solução de segurança para *containers*:** é um software especializado destinado a proteger ambientes baseados em contêineres, como Docker e Kubernetes, contra ameaças cibernéticas. Essas soluções abordam os desafios únicos apresentados pela natureza dinâmica e escalável dos contêineres, incluindo a segmentação de redes, monitoramento contínuo, detecção de vulnerabilidades, gerenciamento de identidades e acessos, proteção de APIs, e integração com plataformas de DevOps para garantir que os contêineres sejam implantados, gerenciados e executados de forma segura em toda a cadeia de desenvolvimento e implantação de software.
- **Solução de segurança para dispositivos *mobile***: é um software projetado para proteger smartphones, tablets e outros dispositivos móveis contra uma variedade de ameaças cibernéticas, como *malware*, *phishing*, roubo de dados e acesso não autorizado. Essas soluções incluem recursos

como antivírus, firewall, criptografia de dados, controle de acesso, detecção de ameaças em tempo real, gerenciamento de dispositivos móveis (MDM) e segurança de aplicativos, com o objetivo de garantir a integridade, confidencialidade e disponibilidade dos dados armazenados e transmitidos nos dispositivos móveis, além de proteger a privacidade e segurança dos usuários em ambientes corporativos e pessoais.

4.1.2. Os criminosos da internet (os atacantes/*hackers*) estão cada vez mais utilizando recursos de Inteligência Artificial (IA) para alavancar e acelerar, ainda mais, os ciclos de ataques. O uso de tecnologias de automação ofensiva resulta em menor latência para os atacantes ou em um tempo menor de violação (TTB), aumentando assim sua taxa de sucesso. As equipes de segurança precisam levar em consideração o fato de que os ataques estão ocorrendo em um ritmo muito mais rápido e ajustar suas estratégias defensivas. Isso requer tecnologia de automação avançada além de acompanhamento em tempo integral, com ferramentas de segurança avançadas e principalmente processos bem definidos.
4.1.3. O uso de uma ferramenta de segurança avançada integrada de prevenção, detecção e resposta possibilitará o aumento da estabilidade, disponibilidade e capacidade. O *core* desse tipo de ferramenta é dotado de módulos de IA (Inteligência Artificial) com enorme capacidade de detecção baseado em comportamento. Desta maneira, os riscos de alguma intercorrência são reduzidos visto que a modernização de ataques é acompanhada pela inteligência da ferramenta.
4.1.4. A reboque do já exposto, temos uma das principais necessidades de negócio que se trata de buscar fazer mais com menos, ou seja, reduzir o custo total de propriedade (TCO) de sua infraestrutura de segurança, fornecendo uma abordagem integrada para a detecção e resposta a ameaças, que elimine ou reduza minimamente a necessidade de investir em múltiplas soluções de segurança.
4.1.5. Ademais, é primordial aprimorar a atuação preventiva, elevar o grau de detecção de comportamentos anômalos e agilizar a resposta a incidentes de segurança para que possamos melhorar a percepção de segurança perante os usuários do CNPq. Estes objetivos serão perseguidos nesta contratação para que estes estejam condizentes com a importância que a segurança da informação possui para a Instituição. Abaixo identificamos 5 fases no ciclo de segurança cibernética que fazem parte da estratégia de segurança da informação. São elas:

1. **Prevenção:** é o esforço para impedir que ameaças maliciosas se infiltrem na rede e para classificar os tipos de ataques direcionados ao CNPq em tempo real. Nesta fase do ciclo, o objetivo é poder interromper os ataques antes que qualquer processo possa ser executado na rede;
2. **Detecção:** é o esforço para reconhecer e identificar ameaças na infraestrutura de segurança de TI do CNPq que conseguiram se infiltrar apesar dos esforços de prevenção. Durante essa fase, a solução precisa ser capaz de identificar processos maliciosos que estão sendo executados em um *endpoint*, na rede e/ou na nuvem;
3. **Contenção:** é o esforço para impedir a disseminação de uma ameaça cibernética, uma vez que ela tenha sido detectada e identificada na rede;
4. **Recuperação:** ocorre após a contenção da ameaça. Nesta fase, as equipes de segurança do CNPq e da Contratada trabalham em conjunto para restaurar a infraestrutura de TI ao seu estado anterior e estável;
5. **Remediação:** é esforço feito para garantir que processos e tecnologias sejam atualizados para mitigar futuros eventos cibernéticos. Isso inclui o reforço de programas de treinamento e conscientização de funcionários, pois os indivíduos desempenham um papel crucial na viabilização de violações de segurança cibernética.

4.2. Requisitos de capacitação

4.2.1. Os treinamentos deverão ser realizados e concluídos para até 2 (dois) servidores do CNPq, dentro de prazo máximo de 120 (cento e vinte) dias.
4.2.2. A CONTRATADA deverá fornecer treinamento específico sobre a instalação, operação, configuração e uso do console de gerenciamento, de caráter teórico e prático, da solução de segurança contratadas para 2 (dois) servidores da CONTRATANTE, em Brasília/DF.
4.2.3. O treinamento deverá ser sem custo adicional ao preço formulado em sua proposta, incluindo o material didático oficial.
4.2.4. O programa para o treinamento deverá ser previamente aprovado pela CONTRATANTE e eventuais mudanças de conteúdo solicitadas deverão constar no material didático.

4.2.5. No caso do treinamento fornecido não ser satisfatório, mediante avaliação tempestiva e fundamentada, tanto em relação à qualidade ou à carga horária efetiva, a CONTRATADA deverá realizar novo treinamento sem ônus adicional à CONTRATANTE.
4.2.6. Deverá ser emitido certificado de participação ao final do curso.
4.2.7. O escopo deste plano de treinamento para instalação, operação e configuração deve prever:
4.2.7.1. informativo global dos componentes tecnológicos envolvidos na prestação dos serviços contratados;
4.2.7.2. compreensão geral da filosofia de funcionamento e de operação da solução adotada;
4.2.7.3. conhecimento e usabilidade dos recursos (hardwares e softwares) envolvidos;
4.2.7.4. funcionalidades do sistema em seus respectivos módulos.
4.2.8. O plano de treinamento deve prever, para cada tema, a carga horária, recursos e condições imprescindíveis para o perfeito aproveitamento do treinamento incluindo a documentação didática a ser utilizada.
Os instrutores ou responsáveis pelos treinamentos, certificados pelo fabricante, são de responsabilidade da CONTRATADA e estes devem apresentar ao CNPq as respectivas agendas de treinamento.
4.2.9. Todo o material de apoio técnico necessário à realização dos treinamentos em ambiente da CONTRATADA, tais como os equipamentos, acessórios, ferramentas, etc. devem ser providos pela CONTRATADA em quantidade suficiente para permitir adequado aprendizado pelos treinados.

4.3. Requisitos legais

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

a. Constituição Federal;
b. Lei n.º 14.133, de 1º de abril de 2021;
c. Portaria SGD/MGI n.º 5.950, de 26 de outubro de 2023;
d. Instrução Normativa SGD/ME n.º 94, de 23 de dezembro de 2022;
e. Instrução Normativa SEGES/ME n.º 65, de 7 de julho de 2021;
f. Lei n.º 13.709, de 14 de agosto de 2018;
g. Lei n.º 8.248, de 23 de outubro de 1991;
h. Decreto n.º 11.260, de 22 de novembro de 2022;
i. Decreto n.º 9.637, de 26 de dezembro de 2018;
j. Decreto n.º 7.174, de 12 de maio de 2010;
k. Decreto n.º 7.579/2011, de 11 outubro de 2011.

4.4. Requisitos de suporte e manutenção

4.4.1. A CONTRATADA deverá acompanhar e ajustar os seguintes itens na atividade de monitoramento:
4.4.1.1. administração das configurações da solução oferecida;
4.4.1.2. desempenho da solução.
4.4.2. A CONTRATADA deverá emitir, no mínimo, mensalmente, os seguintes relatórios:
4.4.2.1. relatório de remoção de ameaças;
4.4.2.2. recomendações de ajustes de configuração;
4.4.2.3. vírus detectados;
4.4.2.4. top 10 vírus detectados;
4.4.2.5. vírus agrupado por dia;
4.4.2.6. total de arquivos verificados;
4.4.2.7. quantidade de arquivos bloqueados;
4.4.2.8. quantidade de vírus identificados;
4.4.2.9. quantidade de *phishing* identificados;
4.4.2.10. quantidade de falsos positivos identificados;
4.4.2.11. tentativas de ataques;
4.4.2.12. detalhamento das ameaças encontradas;
4.4.2.13. usuários que mais recebem e enviam códigos maliciosos;
4.4.2.14. amostragem de ameaças identificadas;
4.4.2.15. tipos de ações tomadas.

4.4.3. A CONTRATADA deverá prestar serviços de natureza continuada de suporte técnico *on-site* ou remotamente 24x7 em Brasília/DF relativos à prestação dos serviços de segurança das ferramentas implantadas, sem ônus para a CONTRATANTE, o qual será acionado por meio de abertura de chamados pela CONTRATANTE.
4.4.4. A CONTRATADA deverá disponibilizar para a CONTRATANTE uma Central de Atendimento (sítio na Internet, mensagem eletrônica e telefone) para consultas, aberturas de chamados técnicos e envio de arquivos para análise 24x7 durante a vigência do contrato.
4.4.5. A CONTRATADA deverá cumprir prazos máximos para resposta aos acionamentos, de acordo com o nível de severidade de cada chamado, conforme quadros a seguir:

Tabela 1: Níveis de severidade dos chamados

Categoria	Nível	Descrição
Urgente	1	Serviços totalmente indisponíveis. Falha comprometendo um ou mais serviços em produção ou que deixe indisponíveis os recursos do mesmo. Impacto a múltiplos usuários e/ou falha em servidor de produção que afete as operações críticas do CNPq.
Crítico	2	Serviços parcialmente indisponíveis ou com degradação de tempo de resposta no acesso aos aplicativos. Intermitente em serviços suportados que torne o ambiente inoperante. Impacto individual ou a pequenos grupos. Operação normal afetada, mas sem interrupção.
Não Crítico	3	Serviços disponíveis com ocorrência de alarmes de avisos, consulta sobre problemas, dúvidas gerais sobre a ferramenta de segurança. Manutenção e monitoramento de eventos de falhas ou de avisos relatados pelo cliente. Pequeno impacto a um ou mais usuários. A correção pode ser feita de forma agendada, em um momento futuro.

4.4.6. O nível de severidade será informado pela CONTRATANTE no momento da abertura de cada chamado.
4.4.7. O nível severidade poderá ser reclassificado a critério da CONTRATANTE. Caso isso ocorra haverá o início de nova contagem de prazo, conforme o novo nível de severidade.
4.4.8. Todas as solicitações de suporte técnico devem ser registradas pela CONTRATADA para acompanhamento e controle da execução do serviço descrito no item *Requisitos temporais.*
4.4.9. Para a execução de atendimento é necessário a autorização da CONTRATANTE para instalação ou desinstalação de quaisquer softwares ou equipamentos que não façam parte da solução antivírus CONTRATADA.
4.4.10. Em caso de interrupção ou indisponibilidade do serviço, a CONTRATADA se compromete a realizar as correções necessárias a reativação do serviço e à prevenção de novas interrupções, respeitados os prazos de atendimento.
4.4.11. Entende-se por interrupção ou indisponibilidade dos serviços de antivírus quando os ativos de TI protegidos não puderem ser atualizados devido a problemas de responsabilidade da CONTRATADA ou quando os servidores de atualização estiverem indisponíveis.

4.5. Requisitos temporais

4.5.1. Os serviços contratados deverão ser prestados pelo período de 24 (vinte e quatro) meses, prorrogáveis por até 10 anos, de acordo com os artigos 106 e 107 da Lei n.º 14.133. A justificativa para este período em vez de 12 (doze) meses é que as licitantes podem oferecer descontos ou condições financeiras mais favoráveis, o CNPq poderá ter acesso contínuo à solução sem interrupções frequentes para renovação, fortalecimento do relacionamento com o fornecedor, continuidade do negócio diante da criticidade da solução, além do menor esforço administrativo para procedimento de renovação contratual.
4.5.2. O prazo para a entrega dos itens é de 30 (dias) dias corridos, prorrogável por igual período, mediante aprovação da CONTRATANTE, após emissão da Ordem de Serviço.
4.5.3. Os componentes das soluções serão recebidos provisoriamente no prazo de até 15 (quinze) dias corridos, pelo(a) responsável pelo acompanhamento e fiscalização do contrato, para efeito de posterior verificação de sua conformidade com as especificações constantes neste Termo de Referência e na proposta.
4.5.4. Os componentes das soluções poderão ser rejeitados, no todo ou em parte, quando em desacordo com as especificações constantes neste Termo de Referência e na proposta, devendo ser substituídos no prazo de

30 (trinta) dias corridos, a contar da notificação à CONTRATADA, às suas custas, sem prejuízo da aplicação das penalidades.

4.5.5. Os componentes das soluções serão recebidos definitivamente no prazo de até 15 (quinze) dias corridos, contados do recebimento provisório, após a verificação de sua conformidade com as especificações constantes neste Termo de Referência e na proposta.

4.5.6. Na hipótese da verificação a que se refere o subitem anterior não ser procedida dentro do prazo fixado, reputar-se-á como realizada, consumando-se o recebimento definitivo no dia do esgotamento do prazo, exceto no caso de não conformidade dos itens fornecidos com as especificações constantes no Termo de Referência e na proposta.

4.5.7. O recebimento provisório ou definitivo do objeto não exclui a responsabilidade da CONTRATADA pelos prejuízos resultantes da incorreta execução do contrato.

4.5.8. Os serviços de console de gerenciamento deverão estar disponíveis 90% no mês.

4.5.9. A CONTRATADA deverá reinstalar ou substituir qualquer módulo da solução de antivírus por outro novo, no prazo de 5 (cinco) dias úteis, contados do recebimento de carta emitida pela CONTRATANTE, se:

4.5.9.1. ocorrerem 4 (quatro) ou mais defeitos que comprometam o seu uso normal, dentro de qualquer período de 30 (trinta) dias, ou;

4.5.9.2. a soma do tempo de paralisação do módulo ultrapassar 20 (vinte) horas, dentro de qualquer período de 30 (trinta) dias.

4.5.10. A solução da CONTRATADA deverá garantir a detecção e remoção programas maliciosos como *spyware*, programas de propaganda, ferramentas como *password crackers*, etc., para os servidores e para os desktops, de forma automática, em pelo menos 90,00% (noventa por cento) dos casos. Para os casos em que a solução não remova a infecção automaticamente, a CONTRATADA continua responsável pela remoção das infecções remanescentes, devendo a CNPq indicar o prazo para a solução do problema.

4.5.11. A solução da CONTRATADA deverá garantir a atualização automática das assinaturas de antivírus em pelo menos 90% (noventa por cento) das estações e servidores ativos e disponíveis na rede em até no máximo 24 (vinte e quatro) horas após o recebimento desta pelo servidor de antivírus. Para os casos em que a solução não atualize automaticamente as assinaturas de antivírus, a CONTRATADA continua responsável pelas atualizações remanescentes, devendo ao CNPq indicar o prazo para a solução do problema.

4.5.12. A solução da CONTRATADA deverá evitar a proliferação programas maliciosos, programas de propaganda, ferramentas como *password crackers* etc., de forma a evitar epidemias (*outbreaks*).

4.5.13. Os atendimentos de suporte técnico prestados à CONTRATANTE deverão pautar-se pelas instruções abaixo:

4.5.13.1. caso seja on-site, o atendimento deverá ser provido na sede do 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.

4.5.13.2. A CONTRATADA deverá cumprir prazos máximos para resposta aos acionamentos, de acordo com o nível de severidade de cada chamado, conforme quadros abaixo:

Tabela 2: Prazos de atendimento

Modalidade	Prazos de atendimento	Níveis de severidade		
		Urgente	Crítico	Não crítico
On-site, remoto, e-mail ou telefone	Início	1 hora	2 horas	24 horas
	Término	2 horas	4 horas	72 horas

4.6. Requisitos de segurança e privacidade

4.6.1. A CONTRATADA deverá manter sob sigilo as informações e comunicações de que tiver conhecimento, abstendo-se de divulgá-las, garantindo o sigilo e a inviolabilidade dos dados trafegados por meio dos enlaces eventualmente utilizados na execução das atividades, respeitando as hipóteses e condições constitucionais e legais de quebra de sigilo de telecomunicações.

4.6.2. A CONTRATADA deverá atender ao disposto na Política de Segurança da Informação e Comunicações do CNPq (POSIC), em suas normas integrantes e os profissionais que tiverem acesso ao ambiente computacional da instituição, deverão assinar o Termo de Responsabilidade de Acesso às Soluções de TI.

4.6.3. Compete à CONTRATANTE dar ciência à CONTRATADA da POSIC e demais normas do CNPq.

4.6.4. A CONTRATADA não poderá armazenar consigo qualquer documento técnico que contemple configurações aplicadas nos equipamentos implantados na rede da CONTRATANTE.
4.6.5. A CONTRATADA deverá informar à CONTRATANTE todas as senhas utilizadas para a configuração dos equipamentos, as quais deverão ser alteradas pela CONTRATANTE com o apoio técnico da CONTRATADA, logo após o encerramento do contrato ou sempre que a CONTRATANTE julgar necessário.
4.6.6. A CONTRATADA deverá prover segurança de acesso físico e lógico aos recursos da CONTRATANTE que estiverem sob sua guarda.
4.6.7. Os recursos de TI não poderão ser utilizados pela CONTRATADA ou seus prepostos para realização de atividades alheias aos serviços previstos ou englobados nesta contratação.
4.6.8. A CONTRATADA deverá guardar sigilo sobre dados e informações obtidos em razão da execução dos serviços contratados ou da relação contratual mantida com o CNPq, abstendo-se de divulgá-los a terceiros sob qualquer pretexto, a menos que prévia e formalmente autorizada pela CONTRATANTE.
4.6.9. Todos os perfis de acesso e caixas postais eventualmente concedidos à CONTRATADA deverão ser imediatamente excluídos após o término do contrato.
4.6.10. A CONTRATANTE terá propriedade sobre todos os documentos e procedimentos operacionais produzidos no escopo da presente contratação.
4.6.11. A CONTRATADA deverá respeitar as normas de segurança estabelecidas pela CONTRATANTE durante a realização de atividades no ambiente desta. Essa sujeição não caracteriza qualquer vínculo empregatício com a CONTRATANTE.
4.6.12. Deverão ser adotadas as versões mais recentes dos softwares básicos do ambiente da CONTRATANTE.

4.7. Requisitos sociais, ambientais e culturais

4.7.1. O atendimento aos chamados de assistência técnica, por qualquer meio de comunicação, deverão ser efetuados em língua portuguesa.
4.7.2. As pessoas envolvidas na execução das atividades deverão, durante sua permanência dentro das instalações do CNPq, se adequar às regras, costumes e normas internas que definem a conduta profissional e pessoal de servidores, colaboradores e visitantes da instituição.
4.7.3. Os profissionais deverão utilizar crachá de identificação ou documento de igual equivalência.
4.7.4. A CONTRATADA deverá observar o disposto na IN SLTI/MPOG n.º 01/2010, de 19 de janeiro de 2010, referente à sustentabilidade ambiental.
4.7.5. O descumprimento de normas ambientais constatadas durante a execução do contrato será comunicado pelo CNPq ao órgão de fiscalização do Distrito Federal ou da União.

4.8. Requisitos de arquitetura tecnológica

4.8.1. Os serviços deverão ser executados observando-se as diretrizes de arquitetura tecnológica estabelecidas pela área técnica da CONTRATANTE.
4.8.2. A adoção de tecnologia ou arquitetura diversa deverá ser autorizada previamente pela CONTRATANTE. Caso não seja autorizada, é vedado à CONTRATADA adotar arquitetura, componentes ou tecnologias diferentes daquelas definidas pela CONTRATANTE.

4.9. Requisitos de projeto e de implementação

4.9.1. CONTRATADA elaborará um plano de implantação e operação da solução caso seja necessário a alteração do licenciamento devido à atualização ou melhorias a serem realizadas nas configurações da solução, contendo, pelo menos:
4.9.1.1. cronograma de atividades;
4.9.1.2. lista de verificação de atividades/fases da execução dos serviços;
4.9.1.3. detalhamento das atividades a serem realizadas, contendo comandos, manuais de operação, guias do fabricante ou quaisquer documentações necessárias para a correta execução; e
4.9.1.4. plano de *rollback*.

4.9.2. A CONTRATADA deverá realizar todas as atividades necessárias à instalação, configuração e testes de funcionamento da solução, respeitando o horário de funcionamento da CONTRATANTE.
4.9.3. A critério da CONTRATANTE, as atividades necessárias à instalação, configuração e testes da solução poderão ser agendadas para os finais de semana e/ou fora do horário comercial.
4.9.4. A equipe técnica da CONTRATADA será acompanhada pelo(s) responsável(eis) técnico(s) da CONTRATANTE nas atividades necessárias à instalação, configuração e testes de solução.
4.9.5. A CONTRATANTE poderá determinar alterações no projeto e/ou no cronograma de implantação, desde que não implique custos adicionais à CONTRATADA.
4.9.6. A CONTRATADA deverá respeitar os requisitos técnicos e as informações sobre o ambiente computacional fornecidas pela CONTRATANTE, sendo de sua responsabilidade a correção de eventuais inconformidades, mesmo que a título oneroso e sem qualquer custo à CONTRATANTE.
4.9.7. A CONTRATANTE poderá realizar, a seu critério, reuniões técnicas e gerenciais com a CONTRATADA para alinhamento de expectativas e para definição/revisão de configurações.
4.9.8. A CONTRATADA deverá, sempre que solicitado, providenciar o registro das reuniões, contemplando os acertos e as definições estabelecidas em comum acordo com a CONTRATANTE. Toda a documentação originada a partir das reuniões técnicas, caso solicitado pela CONTRATANTE, deverá ser fornecida ao CNPq, via Sistema Eletrônico de Informações (SEI) ou outro meio indicado pela CONTRATANTE.
4.9.9. Ao final das etapas de implantação e testes da solução, a CONTRATADA deverá entregar relatório de conclusão contendo todas as informações relativas à implantação e testes da solução, de forma a comprovar o atendimento aos requisitos técnicos definidos no Termo de Referência, que deverá ser aprovado pela CONTRATANTE.

4.10. Requisitos de implantação

4.10.1. A CONTRATADA deverá providenciar a instalação da solução, a qual deve ocorrer em, no máximo, 15 (quinze) dias corridos após a emissão da autorização para instalação/configuração.
4.10.2. A autorização para instalação poderá ser emitida para cada componente da solução individualmente, sendo que cada autorização terá seu prazo diferenciado.
4.10.3. A contratada deverá disponibilizar 1 (um) técnico, certificado na solução para instalação e configuração do produto no ambiente do CNPq.
4.10.4. A CONTRATADA deverá elaborar um projeto executivo, contendo as fases de execução dos serviços com a especificação de cada fase, incluindo o cronograma dos serviços a serem realizados com respectivos prazos e datas.
4.10.5. A instalação deverá ser realizada em máquinas disponibilizadas pela CONTRATANTE, com infraestrutura de armazenamento em Storage, e deve garantir a alta disponibilidade da solução. Os recursos de hardware e sistema operacional para a instalação serão fornecidos pela CONTRATANTE.
4.10.6. A instalação deverá contemplar as seguintes fases:
4.10.6.1. avaliação da estrutura operacional para definir questões de funcionamento e desempenho da solução;
4.10.6.2. adequação do sistema operacional conforme requisitos da aplicação;
4.10.6.3. instalação do software em sua última versão disponível no momento da instalação, contemplando todas as funcionalidades disponíveis no produto, configurado para alta disponibilidade;
4.10.6.4. configuração de domínios, classes de serviços, gerenciamento hierárquico de armazenamento, *backup* e *restore* sem necessidade de parada do serviço, serviços de monitoramento via SNMP, listas de controle de acesso, e customização da interface web com o logotipo do CONTRATANTE, além de outras que o corpo técnico de informática da CONTRATANTE, de comum acordo com a CONTRATADA, possa vir a definir, respeitando as limitações técnicas do ambiente disponibilizado;
4.10.6.5. migração de todos os dados e configurações dos usuários, hoje instalados na solução de e-mail para o novo ambiente, sem qualquer prejuízo para os usuários;
4.10.6.6. fornecimento de documentação contendo informações detalhadas sobre todo o ambiente, procedimentos realizados no processo de instalação, descrição de todas as políticas adotadas (classe de serviço, HSM, backup etc.), procedimentos de backup e *disaster recovery*;
4.10.6.7. todo o processo da instalação deve ser realizado na sede da CONTRATANTE, por técnicos certificados pelo fabricante da solução.

4.11. Requisitos de garantia

4.11.1. O prazo de garantia contratual da solução, complementar à garantia legal, é de, no mínimo, 12 (doze) meses, contado a partir do primeiro dia útil subsequente à data do recebimento definitivo do objeto.
4.11.2. A garantia será prestada com vistas a manter o sistema de antivírus e antispam em perfeitas condições de uso com todas as licenças, configuradas e operantes, sem qualquer ônus ou custo adicional para a CONTRATANTE.
4.11.3. A garantia abrange a realização de configuração, instalação, atualização entre outros da solução, a ser realizado pela CONTRATADA, ou, se for ocaso, de acordo com as normas técnicas específicas.
4.11.4. Uma vez notificada, a CONTRATADA realizará a reparação ou reconfiguração da solução no prazo especificado nos *Requisitos Temporais*, contados a partir da data de abertura de chamado pela CONTRATANTE.
4.11.5. O prazo indicado no subitem anterior, durante seu transcurso, poderá ser prorrogado uma única vez, por igual período, mediante solicitação escrita e justificada da CONTRATADA, aceita pela CONTRATANTE.
4.11.6. Caso o prazo da garantia oferecida pelo fabricante seja inferior ao estabelecido nesta cláusula, o fornecedor deverá complementar a garantia do bem ofertado pelo período restante.
4.11.7. A garantia do fabricante dos produtos fornecidos deve obrigatoriamente prover:
4.11.7.1. atualização das versões dos softwares fornecidos, se novas versões forem disponibilizadas;
4.11.7.2. atualização dos softwares fornecidos se houver lançamento de novos softwares em substituição aos fornecidos, ou mesmo não sendo uma substituição, se ficar caracterizada uma descontinuidade dos softwares fornecidos;
4.11.7.3. acesso aos engenheiros do fabricante na modalidade de 24 (vinte e quatro) horas por dia e 7 (sete) dias por semana, durante o período contratado;
4.11.7.4. garantia de prioridade de atendimento na fila de chamados na central de suporte do fabricante;
4.11.7.5. gerente do fabricante dedicado para assuntos de incidentes.
4.11.7.5.1. este profissional deve ser apresentado pela CONTRATADA à CONTRATANTE no início da prestação dos serviços;
4.11.7.5.2. este profissional deverá realizar no mínimo 04 (quatro) visitas por ano de garantia para revisão do ambiente ou resolução de problemas técnicos.
4.11.7.6. envio de alertas preventivos durante o período do contrato.
4.11.7.7. A CONTRATADA deverá garantir o funcionamento das consoles de gerenciamento e atualização (inclusive na instalação ou atualização de versões/*releases*) ou problemas de incompatibilidade com outros softwares da CONTRATANTE.
4.11.7.7.1. os serviços de console de gerenciamento deverão estar disponíveis 90% no mês.
4.11.7.8. A CONTRATADA deverá reinstalar ou substituir qualquer módulo da solução de antivírus por outro novo, no prazo de 5 (cinco) dias úteis, contados do recebimento de carta emitida pela CONTRATANTE, se:
4.11.7.8.1. ocorrerem 4 (quatro) ou mais defeitos que comprometam o seu uso normal, dentro de qualquer período de 30 (trinta) dias, ou;
4.11.7.8.2. a soma do tempo de paralisação do módulo ultrapassar 20 (vinte) horas, dentro de qualquer período de 30 (trinta) dias.

4.12. Requisitos de experiência profissional

4.12.1. Os serviços de assistência técnica, suporte, garantia deverão ser prestados por técnicos devidamente capacitados nos produtos em questão, bem como com todos os recursos ferramentais necessários para a prestação dos serviços.
4.12.2. Para a prestação dos serviços de suporte técnico, garantia, atualização, implantação, configuração e treinamento das soluções de segurança, os profissionais da CONTRATADA deverão dispor de certificados expedidos pelo fabricante Trend Micro ou parceiros credenciados:
4.12.2.1. Apex One as a Service Certified Professional;
4.12.2.2. Deep Security 20 Certified Professional.

4.13. Requisitos de formação de equipe

4.13.1. A CONTRATADA deverá designar um responsável para contato direto com o CNPq, sem custo adicional para a CONTRATANTE. Além de ser o ponto focal da comunicação da CONTRATANTE, ele deverá assumir as responsabilidades da CONTRATADA perante o CNPq.
4.13.2. Deverá indicar um substituto para o preposto que, na ausência deste, deverá assumir integralmente todas as responsabilidades perante à CONTRATANTE.

4.14. Requisitos de metodologia de trabalho

4.14.1. A execução dos serviços está condicionada ao recebimento pelo CONTRATADO de Ordem de Serviço (OS) emitida pela CONTRATANTE.
4.14.2. A OS indicará o serviço, a quantidade, os prazos e a localidade na qual os deverão ser prestados.
4.14.3. O CONTRATADO deve fornecer meios para contato e registro de ocorrências.
4.14.4. A execução do serviço dever ser acompanhada pelo CONTRATADO, que dará ciência de eventuais acontecimentos à CONTRATANTE.
4.14.5. O fornecimento das licenças será feito por meio digital, conforme quantidade e tipos de licenças constantes em Ordem de Serviço.
4.14.6. A CONTRATADA deverá realizar a implantação da solução nos sites principal e secundário da CONTRATANTE.
4.14.7. Tanto o serviço de instalação quanto o de treinamento deverão ser agendados previamente com a equipe da CONTRATANTE.

4.15. Requisitos de Segurança da Informação e Privacidade

4.15.1. A CONTRATADA deverá manter sob sigilo as informações e comunicações de que tiver conhecimento, abstendo-se de divulgá-las, garantindo o sigilo e a inviolabilidade dos dados trafegados por meio dos enlaces eventualmente utilizados na execução das atividades, respeitando as hipóteses e condições constitucionais e legais de quebra de sigilo de telecomunicações.
4.15.2. A CONTRATADA deverá atender ao disposto na Política de Segurança da Informação da CONTRATANTE (POSIN), em suas normas integrantes e os profissionais que tiverem acesso ao ambiente computacional da instituição, deverão assinar o Termos de Responsabilidade e Sigilo.
4.15.3. Compete à CONTRATANTE dar ciência à CONTRATADA da POSIN e demais normas.
4.15.4. A CONTRATADA não poderá armazenar consigo qualquer documento técnico que contemple configurações aplicadas nos equipamentos implantados na rede da CONTRATANTE.
4.15.5. A CONTRATADA deverá informar à CONTRATANTE todas as senhas utilizadas para a configuração dos equipamentos, as quais deverão ser alteradas pela CONTRATANTE com o apoio técnico da CONTRATADA, logo após o encerramento do contrato ou sempre que a CONTRATANTE julgar necessário.
4.15.6. A CONTRATADA deverá prover segurança de acesso físico e lógico aos recursos da CONTRATANTE que estiverem sob sua guarda.
4.15.7. Os recursos de TI não poderão ser utilizados pela CONTRATADA ou seus prepostos para realização de atividades alheias aos serviços previstos ou englobados nesta contratação.
4.15.8. A CONTRATADA deverá guardar sigilo sobre dados e informações obtidos em razão da execução dos serviços contratados ou da relação contratual mantida com a CONTRATANTE, abstendo-se de divulgá-los a terceiros sob qualquer pretexto, a menos que prévia e formalmente autorizada pela CONTRATANTE.
4.15.9. Todos os perfis de acesso e caixas postais eventualmente concedidos à CONTRATADA deverão ser imediatamente excluídos após o término do contrato.
4.15.10. A CONTRATANTE terá propriedade sobre todos os documentos e procedimentos operacionais produzidos no escopo da presente contratação.
4.15.11. A CONTRATADA deverá respeitar as normas de segurança estabelecidas pela CONTRATANTE durante a realização de atividades no ambiente desta. Essa sujeição não caracteriza qualquer vínculo empregatício com a CONTRATANTE.
4.15.12. Deverão ser adotadas as versões mais recentes dos softwares básicos do ambiente da CONTRATANTE.

4.16. Vistoria

4.16.1. Não há necessidade de realização de avaliação prévia do local de execução dos serviços.

4.17. Sustentabilidade

4.17.1. Os critérios de sustentabilidade foram descritos no item *4.7. Requisitos sociais, ambientais e culturais*.

4.18. Requisitos técnicos das soluções

4.18.1. Os requisitos técnicos das soluções estão detalhados no Anexo VII - Requisitos técnicos das soluções.

4.19. Da subcontratação

4.19.1. Não é admitida a subcontratação do objeto contratual.

4.20. Garantia da contratação

4.20.1. Será exigida a garantia da contratação de que tratam os arts. 96 e seguintes da Lei n.º 14.133, de 2021, no percentual e condições descritas nas cláusulas do contrato.
4.20.2. Em caso de opção pelo seguro-garantia, a parte adjudicatária deverá apresentá-la, no máximo, até a data de assinatura do contrato.
4.20.3. A garantia, nas modalidades caução e fiança bancária, deverá ser prestada em até 10 dias úteis após a assinatura do contrato.
4.20.4. O contrato oferece maior detalhamento das regras que serão aplicadas em relação à garantia da contratação.

4.21. Informações relevantes para o dimensionamento da proposta

4.21.1. A demanda do órgão tem como base a análise realizada no Estudo Técnico Preliminar desta contratação.

5 - PAPÉIS E RESPONSABILIDADES

5.1. São obrigações da CONTRATANTE

5.1.1. Nomear Gestor e Fiscal(is) Técnico(s), Administrativo(s) e Requisitante(s) do contrato para acompanhar e fiscalizar a execução dos contratos.
5.1.2. Encaminhar formalmente a demanda por meio de Ordem de Serviço à CONTRATADA, de acordo com os critérios estabelecidos no Termo de Referência.
5.1.3. Receber o serviço fornecido pela CONTRATADA que esteja em conformidade com a proposta aceita, conforme inspeções realizadas.
5.1.4. Aplicar à CONTRATADA as sanções administrativas regulamentares e contratuais cabíveis.
5.1.5. Liquidar o empenho e efetuar o pagamento à CONTRATADA, dentro dos prazos preestabelecidos em contrato.
5.1.6. Comunicar à CONTRATADA todas e quaisquer ocorrências relacionadas com o fornecimento da solução de TIC.
5.1.7. Definir produtividade ou capacidade mínima de fornecimento da solução de TIC por parte da contratada, com base em pesquisas de mercado, quando aplicável.
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 da CONTRATADA

5.2.1. Indicar formalmente preposto idôneo, apto a representar a CONTRATADA 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 prontamente quaisquer danos diretamente causados à CONTRATANTE ou a terceiros por culpa ou dolo de seus representantes legais, prepostos ou empregados, em decorrência da relação contratual, não excluindo ou reduzindo a responsabilidade da fiscalização ou o acompanhamento da execução dos serviços pela CONTRATANTE.
5.2.4. Propiciar todos os meios necessários à fiscalização do contrato pela CONTRATANTE, cujo representante terá poderes para sustar o fornecimento, total ou parcial, em qualquer tempo, desde que motivadas as causas e justificativas desta decisão.
5.2.5. Manter, durante a execução do contrato, as mesmas condições de habilitação.
5.2.6. Quando especificada, manter, durante a execução do contrato, equipe técnica composta por profissionais devidamente habilitados, treinados e qualificados para fornecimento da solução de TIC.
5.2.7. Quando especificado, manter a produtividade ou a capacidade mínima de fornecimento da solução de TIC durante a execução do Contrato.
5.2.8. Ceder os direitos de propriedade intelectual e direitos autorais da solução de TIC sobre os diversos artefatos e produtos produzidos em decorrência da relação contratual, incluindo a documentação, os modelos de dados e as bases de dados à Administração.
5.2.9. Executar o objeto do certame em estreita observância dos ditames estabelecido pela Lei n.º 13.709, de 14 de agosto de 2018 (Lei Geral de Proteção de Dados Pessoais – LGPD).
5.2.10. Não fazer uso das informações prestadas pela CONTRATANTE para fins diversos do estrito e absoluto cumprimento do Contrato em questão.
5.2.11. Disponibilizar profissionais com habilidades para as ferramentas, tecnologias ou versões que vierem a ser adotadas pela CONTRATANTE durante a vigência do Contrato.
5.2.12. Relatar à CONTRATANTE toda e qualquer irregularidade verificada no decorrer da prestação dos serviços.
5.2.13. Realizar e manter atualizado o cadastro de seus representantes legais no Sistema Eletrônico de Informações da CONTRATANTE para fins de comunicação, assinatura de termos contratuais e aditivos.
5.2.14. Fazer a transição contratual, quando for o caso.

6 - MODELO DE EXECUÇÃO DO CONTRATO

6.1. Local e horário da prestação dos serviços

6.1.1. Os serviços serão realizados em ambiente da CONTRATADA ou remotamente, podendo, entretanto, serem realizados em ambiente da CONTRATANTE, a depender de sua natureza. A prestação dos serviços presenciais, quando necessários, deverão ser realizados nos seguinte endereço: Setor de Autarquias Sul (SAUS), Quadra 01, Lote 06, Bloco H - Edifício Telemundi II, Asa Sul, Brasília/DF, CEP 70070-010.
6.1.2. O deslocamento eventual de prestador de serviço da CONTRATADA para o CNPq e outras unidades do CNPq e suas parceiras, não implicará, de nenhuma forma, o acréscimo ou majoração nos valores dos serviços, bem como nenhum tipo de pagamento correspondente a deslocamentos, diárias, horas extras ou adicionais noturnos.
6.1.3. É possível a alteração destes endereços. Neste caso, o CNPq deverá informar a alteração por meio de correio eletrônico, dispensando alteração contratual.
6.1.4. Os serviços, quando presenciais, serão prestados no horário entre 8h30 e 18h30.

6.2. Formas de transferência de conhecimento

6.2.1. A CONTRATADA deverá apoiar a CONTRATANTE na migração reversa dos dados (da plataforma da contratada para os softwares substitutos utilizados no localmente ou em nuvem) em caso de descontinuidade contratual.
6.2.2. Em até um mês antes do encerramento do contrato ou sua eventual prorrogação, a CONTRATADA deverá providenciar a adaptação do ambiente a futuras tecnologias disponíveis na CONTRATANTE.
6.2.3. Ao final do contrato, a CONTRATADA fica obrigada a realizar a transferência de conhecimento tecnológico necessária à plena utilização da solução desenvolvida à equipe interna da CONTRATANTE e, se for o caso, à futura empresa CONTRATADA que for assumir os serviços escopo desta contratação. Esta transferência deverá ocorrer na sede do CONTRATANTE e às custas da CONTRATADA.
6.2.4. No caso de nova contratação, a CONTRATADA deverá participar de todas as reuniões marcadas pela CONTRATANTE com a nova CONTRATADA para apresentação dos documentos necessários e para a transição contratual. Conforme o caso, os documentos a serem utilizados deverão ser baseados em relatórios e informações técnicas necessárias à absorção pela nova empresa CONTRATADA.
6.2.5. A entrega final dos produtos gerados e de toda documentação não exime a CONTRATADA da obrigação de repasse mensal de conhecimento, ou a critério da CONTRATANTE.
6.2.6. A CONTRATADA deverá apresentar num prazo máximo de até 60 (sessenta) dias corridos antes do término de seu contrato, um plano para transferência de conhecimentos. Este plano deverá conter, pelo menos, a revisão de toda a documentação gerada, de todos os serviços prestados, acrescido de lista com credenciais administrativas, topologias, diagramas de rede, bases de conhecimento e quaisquer outros documentos que sejam adequados ao correto entendimento do serviço executado, dos procedimentos que o envolverem e de todo histórico de demandas, além de descrever a metodologia que será utilizada para transferir o conhecimento aos técnicos da CONTRATANTE e, se for o caso, à futura empresa CONTRATADA.
6.2.7. Nesta ocasião, deverão ser devolvidos todos os recursos disponibilizados pela CONTRATANTE de uso pela CONTRATADA durante a execução do contrato nas mesmas condições que foram disponibilizados, excetuando o desgaste natural do recurso, ou seja, aquele que não caracterize mau uso por parte da CONTRATADA. Na impossibilidade de devolução dos recursos nas mesmas condições, a CONTRATADA fará a reposição destes recursos sem qualquer ônus adicional à CONTRATANTE.
6.2.8. O fato de a CONTRATADA ou seus representantes não cooperarem ou reterem qualquer informação ou dado solicitado pela CONTRATANTE, que venha a prejudicar, de alguma forma, o andamento da transição contratual, constituirá quebra de contrato, sujeitando-a às penalidades previstas na Lei 14.133/2021 e na legislação vigente pertinente, no Contrato e no Termo de Referência.

6.3. Quantidade mínima de serviços para comparação e controle

6.3.1. Cada Ordem de Serviço conterá o volume de serviços demandados, incluindo a sua localização e o prazo, conforme modelo descrito no Anexo V.

6.4. Mecanismos formais de comunicação

6.4.1. A comunicação entre a CONTRATANTE e a CONTRATADA dar-se-á de forma escrita por meio dos seguintes instrumentos:
6.4.1.1. Ordem de Serviço;
6.4.1.2. sistema de gerenciamento de serviços de TIC (ITSM);
6.4.1.3. e-mails;
6.4.1.4. cartas;
6.4.1.5. ofício;
6.4.1.6. registros e atas de reunião;
6.4.1.7. plataforma eletrônica de comunicação aderida pela CONTRATANTE (por exemplo: rocket.chat, Microsoft Teams etc.).
6.4.2. A CONTRATADA deverá disponibilizar número de telefone por meio do qual seja possível contato direto com a CONTRATANTE.

6.5. Formas de Pagamento

6.5.1. Os critérios de medição e pagamento dos serviços prestados serão tratados em tópico próprio do Modelo de Gestão do Contrato.

6.6. Manutenção de sigilo e normas de segurança

6.6.1. A CONTRATADA deverá manter sigilo absoluto sobre quaisquer dados e informações contidos em quaisquer documentos e mídias, incluindo os equipamentos e seus meios de armazenamento, de que venha a ter conhecimento durante a execução dos serviços, não podendo, sob qualquer pretexto, divulgar, reproduzir ou utilizar, sob pena da lei, independentemente da classificação de sigilo conferida pela CONTRATANTE a tais documentos.
6.6.2. Deverá ser assinado Termo de Compromisso, contendo declaração de manutenção de sigilo e respeito às normas de segurança vigentes na entidade, a ser assinado pelo representante legal da CONTRATADA, no momento da assinatura do contrato (ANEXO I - Termo de Compromisso de Manutenção de Sigilo e Termo de Confidencialidade e Sigilo).
6.6.3. Deverá ser assinado Termo de Ciência por todos os empregados da CONTRATADA diretamente envolvidos na contratação, independente de prestarem serviço presencial ou remotamente (ANEXO I - Termo de Compromisso de Manutenção de Sigilo e Termo de Confidencialidade e Sigilo).

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 n.º 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 a CONTRATADA 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 representante da empresa para adoção de providências que devam ser cumpridas de imediato.

7.5. Preposto

7.5.1. A CONTRATADA designará formalmente o preposto da empresa, antes do início da prestação dos serviços, indicando no instrumento os poderes e deveres em relação à execução do objeto contratado.
7.5.2. A CONTRATANTE poderá recusar, desde que justificadamente, a indicação ou a manutenção do preposto da empresa, hipótese em que a CONTRATADA designará outro para o exercício da atividade.

7.6. Reunião Inicial

7.6.1. 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 dos serviços.
7.6.2. A reunião será realizada em conformidade com o previsto no inciso I do Art. 31 da IN SGD/ME n.º 94, de 2022, e ocorrerá em até 10 (dez) dias úteis da assinatura do Contrato, podendo ser prorrogada a critério da CONTRATANTE.
7.6.3. A pauta desta reunião observará, pelo menos:
7.6.3.1. Presença do representante legal da contratada, que apresentará o seu preposto;
7.6.3.2. Entrega, por parte da CONTRATADA, do Termo de Compromisso e dos Termos de Ciência;
7.6.3.3. Esclarecimentos relativos a questões operacionais, administrativas e de gestão do Contrato;

7.6.4. 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;
7.6.5. Apresentação das declarações/certificados do fabricante, comprovando que o produto ofertado possui a garantia solicitada neste Termo de Referência.

7.7. Fiscalização

7.7.1. A execução do contrato deverá ser acompanhada e fiscalizada pelo(s) fiscal(is) do contrato, ou pelos respectivos substitutos (Lei n.º 14.133, de 2021, art. 117, caput), nos termos do art. 33 da IN SGD n.º 94, de 2022, observando-se, em especial, as rotinas a seguir.

7.7.2. Fiscalização Técnica.
7.7.2.1. O fiscal técnico do Contrato, além de exercer as atribuições previstas no art. 33, II, da IN SGD n.º 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.
7.7.2.2. 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.
7.7.2.3. Identificada qualquer inexatidão ou irregularidade, o fiscal técnico do Contrato emitirá notificações para a correção da execução do Contrato, determinando prazo para a correção.
7.7.2.4. 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.
7.7.2.5. 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.
7.7.2.6. 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.

7.7.3. Fiscalização Administrativa.
7.7.3.1. O fiscal administrativo do contrato, além de exercer as atribuições previstas no art. 33, IV, da IN SGD n.º 94, de 2022, verificará a manutenção das condições de habilitação do contratado, acompanhará o empenho, o pagamento, as garantias, as glosas e a formalização de apostilamento e termos aditivos, solicitando quaisquer documentos comprobatórios pertinentes, caso necessário.
7.7.3.2. 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.

7.7.4. Fiscalização Requisitante.
7.7.4.1. O fiscal requisitante do Contrato, além de exercer as atribuições previstas no art. 33, II, da IN SGD n.º 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.
7.7.4.2. O fiscal requisitante do Contrato apoiará o fiscal técnico na anotação do histórico de gerenciamento do Contrato de todas as ocorrências relacionadas à execução do Contrato, com a descrição do que for necessário para a regularização das faltas ou dos defeitos observados. Identificada qualquer inexatidão ou irregularidade, o fiscal requisitante do Contrato emitirá notificações para a correção da execução do Contrato, determinando prazo para a correção.
7.7.4.3. O fiscal requisitante 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.
7.7.4.4. No caso de ocorrências que possam inviabilizar a execução do Contrato nas datas aprazadas, o fiscal requisitante do Contrato comunicará o fato imediatamente ao gestor do Contrato.

7.7.5. Gestor do Contrato.

7.7.5.1. O gestor do contrato, além de exercer as atribuições previstas no art. 33, I, da IN SGD n.º 94, de 2022, coordenará 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.
7.7.5.2. O gestor do contrato acompanhará 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.
7.7.5.3. O gestor do contrato acompanhará a manutenção das condições de habilitação do contratado, 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.
7.7.5.4. O gestor do contrato emitirá 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.
7.7.5.5. O gestor do contrato tomará 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 n.º 14.133, de 2021, ou pelo agente ou pelo setor com competência para tal, conforme o caso.
7.7.5.6. O gestor do contrato deverá elaborará 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.
7.7.5.7. O gestor do contrato deverá 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.

8 - CRITÉRIOS DE MEDIÇÃO E PAGAMENTO

8.1. A avaliação da execução do objeto utilizará o Indicador de Nível Mínimo de Serviço (INMS), conforme previsto no Anexo II - Níveis Mínimos de Serviço.
8.2. Será indicada a retenção ou glosa no pagamento, proporcional à irregularidade verificada, sem prejuízo das sanções cabíveis, caso se constate que a CONTRATADA:
8.2.1. não produzir os resultados acordados;
8.2.2. deixar de executar, ou não executar com a qualidade mínima exigida as atividades contratadas; ou
8.2.3. deixar de utilizar materiais e recursos humanos exigidos para a execução do serviço, ou utilizá-los com qualidade ou quantidade inferior à demandada.
8.3. A utilização do INMS não impede a aplicação concomitante de outros mecanismos para a avaliação da prestação dos serviços.
8.4. A aferição da execução contratual para fins de pagamento considerará os seguintes critérios:

8.5. Do recebimento

8.5.1. Os serviços serão recebidos provisoriamente, no prazo de 15 (quinze) dias corridos, pelos fiscais técnico e administrativo, mediante termos detalhados, quando verificado o cumprimento das exigências de caráter técnico e administrativo.
8.5.2. O fiscal técnico do contrato realizará o recebimento provisório do objeto do contrato mediante Relatório Técnico que comprove o cumprimento das exigências de caráter técnico.
8.5.3. Para efeito de recebimento provisório, ao final de cada período de faturamento, o fiscal técnico do contrato irá apurar o resultado das avaliações da execução do objeto e, se for o caso, a análise do desempenho e qualidade da prestação dos serviços realizados em consonância com os indicadores previstos, que poderá resultar no redimensionamento de valores a serem pagos à contratada, registrando em relatório a ser encaminhado ao gestor do contrato.
8.5.3.1. Será considerado como ocorrido o recebimento provisório com a entrega do Relatório Técnico ou, em havendo mais de um a ser feito, com a entrega do último.

8.5.4. A CONTRATADA fica obrigada a reparar, corrigir, remover, reconstruir ou substituir, às suas expensas, no todo ou em parte, o objeto em que se verificarem vícios, defeitos ou incorreções resultantes da execução ou materiais empregados, cabendo à fiscalização não atestar a última e/ou única medição de serviços até que sejam sanadas todas as eventuais pendências que possam vir a ser apontadas no Recebimento Provisório.
8.5.5. A fiscalização não efetuará o ateste da última e/ou única medição de serviços até que sejam sanadas todas as eventuais pendências que possam vir a ser apontadas no Recebimento Provisório.
8.5.6. Os serviços poderão ser rejeitados, no todo ou em parte, quando em desacordo com as especificações constantes neste Termo de Referência e na proposta, sem prejuízo da aplicação das penalidades.
8.5.7. Quando a fiscalização for exercida por um único servidor, o Relatório Técnico deverá conter o registro, a análise e a conclusão acerca das ocorrências na execução do contrato, em relação à fiscalização técnica e administrativa e demais documentos que julgar necessários, devendo encaminhá-los ao gestor do contrato para recebimento definitivo.
8.5.8. Os serviços serão recebidos definitivamente no prazo de 15 (quinze) dias úteis, contados do recebimento provisório, por servidor ou comissão designada pela autoridade competente, após a verificação da qualidade e quantidade do serviço e consequente aceitação mediante Relatório Técnico, obedecendo os seguintes procedimentos:
8.5.8.1. Emitir documento comprobatório da avaliação realizada pelos fiscais técnico, requisitante e administrativo, quando houver, no cumprimento de obrigações assumidas pela CONTRATADA, com menção ao seu desempenho na execução contratual, baseado em indicadores objetivamente definidos e aferidos, e a eventuais penalidades aplicadas, devendo constar do cadastro de atesto de cumprimento de obrigações, conforme regulamento.
8.5.8.2. Realizar a análise dos relatórios e de toda a documentação apresentada pela fiscalização e, caso haja irregularidades que impeçam a liquidação e o pagamento da despesa, indicar as cláusulas contratuais pertinentes, solicitando à CONTRATADA, por escrito, as respectivas correções.
8.5.8.3. Emitir Relatório Técnico para efeito de recebimento definitivo dos serviços prestados, com base nos relatórios e documentações apresentadas; e
8.5.8.4. Comunicar a empresa para que emita a Nota Fiscal ou Fatura, com o valor exato dimensionado pela fiscalização.
8.5.8.5. Enviar a documentação pertinente ao setor de contratos para a formalização dos procedimentos de liquidação e pagamento, no valor dimensionado pela fiscalização e gestão.
8.5.9. 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 n.º 14.133, de 2021, comunicando-se à empresa para emissão de Nota Fiscal no que concerne à parcela incontroversa da execução do objeto, para efeito de liquidação e pagamento.
8.5.10. Nenhum prazo de recebimento ocorrerá enquanto pendente a solução, pela CONTRATADA, de inconsistências verificadas na execução do objeto ou no instrumento de cobrança.
8.5.11. O recebimento provisório ou definitivo não excluirá a responsabilidade civil pela solidez e pela segurança do serviço nem a responsabilidade ético-profissional pela perfeita execução do contrato.
8.5.12. Os serviços prestados pela CONTRATADA só poderão ser faturados após o seu recebimento definitivo e autorizada a emissão da Nota Fiscal pelo Gestor do Contrato.

8.6. Procedimentos de teste e inspeção

8.6.1. A Metodologia de Avaliação da Qualidade será realizada pela CONTRATANTE, de acordo com a avaliação das seguintes condições que deverão ser cumpridas pela CONTRATADA:
8.6.1.1. o cumprimento dos prazos e outras obrigações assumidas pela contratada;
8.6.1.2. entrega da documentação exigida;
8.6.1.3. atendimento dos critérios de aceitação;
8.6.1.4. execução dos procedimentos corretos para que haja o recebimento dos bens e a atestação dos serviços prestados durante a garantia e;
8.6.1.5. a Metodologia de Avaliação da Qualidade dos serviços prestados ocorrerá através do acompanhamento e avaliação dos atendimentos aos chamados de suporte técnico especializado junto com as solicitações de garantia de funcionamento da Solução de segurança de *endpoints* e servidores de rede.
8.6.2. Durante a vigência da garantia, a fiscalização técnica do contrato avaliará constantemente a prestação do serviço e usará como indicador os índices de severidades e atendimentos descritos na tabela 1, no

subitem 4.5.5.

8.6.3. A CONTRATANTE reserva-se o direito de efetuar inspeções e diligências para sanar quaisquer dúvidas existentes, podendo efetuá-las de maneira presencial ou através de documentação, em qualquer momento da contratação.

8.6.3.1. As inspeções e diligências servirão para embasamento e elaboração dos Termos de Recebimento Provisório e Definitivo, TRP e TRD, respectivamente.

8.6.3.2. Com mesmo efeito para procedimentos de teste e inspeção, a CONTRATANTE também reserva-se o direito de verificar o atendimento aos índices dos níveis mínimos aceitáveis definidos no Anexo II - Níveis Mínimos de Serviço como forma de verificação da conformidade dos serviços contratados.

8.7. Sanções administrativas e procedimentos para retenção ou glosa no pagamento

8.7.1. Nos termos do art. 19, inciso III da Instrução Normativa SGD/ME n.º 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:

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

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

8.7.2. A licitante que, convocada dentro do prazo de validade da sua proposta, não assinar o Contrato ou a Ata, deixar de entregar documentação exigida no Edital, apresentar documentação falsa, não mantiver a proposta, fraudar na execução do contrato, comportar-se de modo inidôneo, fizer declaração falsa ou cometer fraude fiscal ficará impedida de licitar e de contratar com a União e será descredenciada no SICAF, pelo prazo de até 5 (cinco) anos, sem prejuízo das multas e demais cominações legais.

8.7.3. Pela recusa em assinar a Ata, o Contrato ou retirar a Nota de Empenho, no prazo máximo de 5 (cinco) dias úteis, após a regular convocação, a licitante poderá ser penalizada com multa no percentual de 5% (cinco por cento), calculada sobre o valor total estimado do Contrato, sem prejuízo da aplicação de outras sanções previstas no parágrafo anterior.

8.7.4. Comete infração administrativa a Contratada que:

8.7.4.1. não executar total ou parcialmente qualquer das obrigações assumidas em decorrência da contratação;

8.7.4.2. ensejar o retardamento da execução do objeto;

8.7.4.3. falhar ou fraudar na execução do contrato;

8.7.4.4. comportar-se de modo inidôneo; ou

8.7.4.5. cometer fraude fiscal.

8.7.5. Pela inexecução total ou parcial do objeto deste contrato, a CONTRATANTE pode aplicar à CONTRATADA as seguintes sanções:

8.7.5.1. Advertência por escrito, quando do não cumprimento de quaisquer das obrigações contratuais consideradas faltas leves, assim entendidas aquelas que não acarretam prejuízos significativos para o serviço contratado;

8.7.5.2. Multa, quando do não cumprimento de quaisquer das obrigações contratuais consideradas faltas moderadas ou graves, assim entendidas aquelas que acarretam prejuízos para o serviço contratado;

8.7.5.3. As penalidades de multa decorrentes de fatos diversos serão consideradas independentes entre si.

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

8.7.5.5. Sanção de impedimento de licitar e contratar com órgãos e entidades da União, com o consequente descredenciamento no SICAF pelo prazo de até cinco anos;

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

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

8.7.6.1. não atingir os valores mínimos aceitáveis fixados nos critérios de aceitação, não produzir os resultados

ou deixar de executar as atividades contratadas; ou

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

8.7.7. A aplicação de qualquer das penalidades previstas realizar-se-á em processo administrativo que assegurará o contraditório e a ampla defesa à CONTRATADA, observando-se o procedimento previsto na Lei n.º 14.133/2021 e, subsidiariamente, a Lei n.º 9.784, de 1999.

8.7.8. As multas devidas e/ou prejuízos causados à CONTRATANTE serão deduzidos dos valores a serem pagos, ou recolhidos em favor da União, ou deduzidos da garantia, ou ainda, quando for o caso, serão inscritos na Dívida Ativa da União e cobrados judicialmente.

8.7.9. Caso a CONTRATANTE determine, a multa deverá ser recolhida no prazo máximo de 10 (dez) dias úteis, a contar da data do recebimento da comunicação enviada pela autoridade competente.

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

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

8.7.12. Se, durante o processo de aplicação de penalidade, se houver indícios de prática de infração administrativa tipificada pela Lei n.º 12.846, de 2013, como ato lesivo à Administração Pública nacional ou estrangeira, cópias do processo administrativo necessárias à apuração da responsabilidade da empresa deverão ser remetidas à autoridade competente, com despacho fundamentado, para ciência e decisão sobre a eventual instauração de investigação preliminar ou Processo Administrativo de Responsabilização - PAR.

8.7.13. A apuração e o julgamento das demais infrações administrativas não consideradas como ato lesivo à Administração Pública nacional ou estrangeira nos termos da Lei n.º 12.846, de 1º de agosto de 2013, seguirão seu rito normal na unidade administrativa.

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

8.7.15. As penalidades serão obrigatoriamente registradas no SICAF.

8.7.16. Nos casos de inadimplemento na prestação dos serviços, as ocorrências serão registradas pela CONTRATANTE que notificará a CONTRATADA, conforme tabela a seguir:

ID	Ocorrência	Glosa/Sanção
1	Não comparecer injustificadamente à reunião inicial.	Advertência. Em caso de reincidência, multa 1% sobre o valor total do Contrato.
2	Quando convocado dentro do prazo de validade da sua proposta, não celebrar o Contrato, deixar de entregar ou apresentar documentação falsa exigida para o certame, ensejar o retardamento da execução de seu objeto, não manter a proposta, falhar ou fraudar na execução do Contrato, comportar-se de modo inidôneo ou cometer fraude fiscal.	A Contratada ficará impedida de licitar e contratar com a União, Estados, Distrito Federal e Municípios e, será descredenciada no SICAF, ou nos sistemas de cadastramento de fornecedores pelo prazo de até 5 (cinco) anos, sem prejuízo das demais cominações legais, e multa de 5% do valor da contratação.
3	Ter praticado atos ilícitos visando frustrar os objetivos da licitação.	A Contratada será declarada inidônea para licitar e contratar com a Administração Pública.
4	Demonstrar não possuir idoneidade para contratar com a Administração em virtude de atos ilícitos praticados.	Suspensão temporária de 6 (seis) meses para licitar e contratar com a Administração Pública, sem prejuízo da Rescisão Contratual.
5	Não executar total ou parcialmente os serviços previstos no objeto da contratação.	Multa de até 10% sobre o valor total do Contrato.
6	Suspender ou interromper, salvo motivo de força maior ou caso fortuito, os serviços solicitados,	Multa de até 5% sobre o valor total do Contrato.

	por até de 30 dias, sem comunicação formal ao gestor do Contrato.	
7	Não prestar os esclarecimentos imediatamente, referente à execução dos serviços, salvo quando implicarem em indagações de caráter técnico, hipótese em que serão respondidos no prazo máximo de 5 dias úteis.	Advertência. Em caso de reincidência, multa de 1% sobre o valor total do Contrato por dia útil de atraso em prestar as informações por escrito, ou por outro meio quando autorizado pela Contratante, até o limite de 10 dias úteis.
		Após o limite de 10 dias úteis, aplicar-se-á multa de 5% do valor total do Contrato.
8	Provocar intencionalmente a indisponibilidade da prestação dos serviços quanto aos componentes de software (sistemas, portais, funcionalidades, banco de dados, programas, relatórios, consultas etc.).	A Contratada será impedida de licitar e contratar com órgãos e entidades da União, com o consequente descredenciamento no SICAF pelo prazo de até cinco anos, sem prejuízo às penalidades de correntes da inexecução total ou parcial do contrato, o que poderá acarretar a rescisão do Contrato, sem prejuízo das demais penalidades previstas na Lei n.º 14.133/2021.
9	Permitir intencionalmente o funcionamento dos sistemas de modo adverso ao especificado na fase de levantamento de requisitos e às cláusulas contratuais, provocando prejuízo aos usuários dos serviços.	A Contratada será impedida de licitar e contratar com órgãos e entidades da União, com o consequente descredenciamento no SICAF pelo prazo de até cinco anos, sem prejuízo às penalidades decorrentes da inexecução total ou parcial do contrato, o que poderá acarretar a rescisão do Contrato, sem prejuízo das demais penalidades previstas na Lei n.º 14.133/2021.
10	Comprometer intencionalmente a integridade, disponibilidade ou confiabilidade e autenticidade das bases de dados dos sistemas.	A Contratada será impedida de licitar e contratar com órgãos e entidades da União, com o consequente descredenciamento no SICAF pelo prazo de até cinco anos, sem prejuízo às penalidades decorrentes da inexecução total ou parcial do contrato, o que poderá acarretar a rescisão do Contrato, sem prejuízo das demais penalidades previstas na Lei n.º 14.133/2021.
11	Comprometer intencionalmente o sigilo das informações armazenadas nos sistemas da contratante.	A Contratada será impedida de licitar e contratar com órgãos e entidades da União, com o consequente descredenciamento no SICAF pelo prazo de até cinco anos, sem prejuízo às penalidades decorrentes da inexecução total ou parcial do contrato, o que poderá acarretar a rescisão do Contrato, sem prejuízo das demais penalidades previstas na Lei n.º 14.133/2021.
12	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 5% (dois por cento) do valor total do Contrato.

8.8. Liquidação

8.8.1. Recebida a Nota Fiscal ou documento de cobrança equivalente, correrá o prazo de 10 (dez) dias úteis para fins de liquidação, na forma desta seção, prorrogáveis por igual período, nos termos do art. 7º, §2º da

Instrução Normativa SEGES/ME n.º 77/2022.

8.8.2. 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 n.º 14.133, de 2021.

8.8.3. 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:

8.8.3.1. o prazo de validade;

8.8.3.2. a data da emissão; os dados do Contrato e do órgão contratante;

8.8.3.3. o período respectivo de execução do Contrato;

8.8.3.4. o valor a pagar; e

8.8.3.5. eventual destaque do valor de retenções tributárias cabíveis.

8.8.4. 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.

8.8.5. 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 n.º 14.133, de 2021.

8.8.6. A Administração deverá realizar consulta ao SICAF para:

8.8.6.1. verificar a manutenção das condições de habilitação exigidas no edital;

8.8.6.2. identificar possível razão que impeça a participação em licitação, no âmbito do órgão ou entidade, que implique proibição de contratar com o Poder Público, bem como ocorrências impeditivas indiretas (INSTRUÇÃO NORMATIVA n.º 3, DE 26 DE ABRIL DE 2018).

8.8.7. 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 da CONTRATANTE.

8.8.8. Não havendo regularização ou sendo a defesa considerada improcedente, a 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.

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

8.8.10. 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.

8.9. Prazo de pagamento

8.9.1. 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 n.º 77, de 2022.

8.9.2. No caso de atraso pela 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 ICTI de correção monetária.

8.10. Forma de pagamento

8.10.1. O pagamento será realizado por meio de ordem bancária, para crédito em banco, agência e conta corrente indicados pela CONTRATADA.

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

8.10.3. Quando do pagamento, será efetuada a retenção tributária prevista na legislação aplicável.

8.10.4. 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.

8.11. Cessão de crédito

8.11.1. É admitida a cessão fiduciária de direitos creditícios com instituição financeira, nos termos e de acordo com os procedimentos previstos na Instrução Normativa SEGES/ME n.º 53, de 8 de Julho de 2020, conforme as regras deste presente tópico.
8.11.1.1. As cessões de crédito não fiduciárias dependerão de prévia aprovação do contratante.
8.11.2. A eficácia da cessão de crédito, de qualquer natureza, em relação à Administração, está condicionada à celebração de termo aditivo ao contrato administrativo.
8.11.3. 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 n.º 8.429, de 1992, nos termos do Parecer JL-01, de 18 de maio de 2020.
8.11.4. 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 (Instrução Normativa n.º 53, de 8 de julho de 2020).
8.11.5. A cessão de crédito não afetará a execução do objeto contratado, que continuará sob a integral responsabilidade do contratado.

8.12. Da alteração subjetiva

8.12.1. É admissível a fusão, cisão ou incorporação da CONTRATADA com/em outra pessoa jurídica, desde que sejam observados pela nova pessoa jurídica todos os requisitos de habilitação exigidos na licitação original; sejam mantidas as demais cláusulas e condições do contrato; não haja prejuízo à execução do objeto pactuado; e haja a anuência expressa da Administração à continuidade do contrato.

9 - FORMA E CRITÉRIOS DE SELEÇÃO DO FORNECEDOR E REGIME DE EXECUÇÃO

9.1. Forma de seleção e critério de julgamento da proposta

9.1.1. 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 por grupo.

9.2. Regime de execução

9.2.1. O regime de execução do Contrato será o de empreitada por preço global.
9.2.2. O parcelamento da solução de TIC se mostrou inviável, pois as licenças, serviços de instalação, configuração, garantia, suporte do fabricante e repasse de conhecimento formam uma solução unificada. É essencial que esses itens sejam fornecidos em conjunto, sem parcelamento, para garantir a implantação efetiva da solução. Essa abordagem está em conformidade com a alínea "a", inciso V do artigo 40 da Lei nº 14.133, de 1º de abril de 2021, que estabelece o princípio "*da padronização, considerando a compatibilidade de especificações estéticas, técnicas ou de desempenho*". Dessa forma, a aquisição dos itens em um lote único assegura que todos os componentes sejam compatíveis entre si, garantindo a harmonia e o desempenho adequado da solução. Além de promover maior facilidade na manutenção, suporte técnico e garantia, uma vez que todos os elementos estão integrados e fornecidos por um único provedor. O propósito é alcançar uma solução única, gerenciada de forma centralizada, para atender tanto quantitativa como qualitativamente às

necessidades atuais da Pasta, proporcionando garantias adicionais à Administração de que não haverá ambiguidades em relação às responsabilidades por possíveis falhas na execução do contrato.

9.2.3. O parcelamento dos itens em vários lotes comprometeria consideravelmente os custos, a uniformidade e a padronização da solução. Além, do mais, ao se adotar soluções de diferentes fabricantes, os serviços de implantação, treinamento e suporte seriam multiplicados para atender cada uma das soluções, claramente ferindo o princípio de economicidade da contratação. Ressalta-se também que é fundamental para o aumento da eficiência administrativa do setor público otimizar a gestão de seus contratos de fornecimento. Essa eficiência administrativa é também uma obrigação constitucional que deve ser perseguida pela administração pública. A unicidade da solução é o requisito que assegura a capacidade de integração dos serviços e impulsiona o potencial de compartilhamento de recursos pela Contratada. Essas características formam a essência do objeto da pretensão contratual em relação aos seus aspectos intrínsecos (ciclo de vida de serviços).

9.3. Da aplicação da margem de preferência

9.3.1. Não será aplicada margem de preferência na presente contratação.

9.4. Exigências de Habilitação

9.4.1. Para fins de habilitação, deverá o licitante comprovar os seguintes requisitos:

9.5. Habilitação jurídica

9.5.1. 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.

9.5.2. Empresário individual: inscrição no Registro Público de Empresas Mercantis, a cargo da Junta Comercial da respectiva sede.

9.5.3. 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.

9.5.4. 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.

9.5.5. 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.

9.5.6. Sociedade simples: inscrição do ato constitutivo no Registro Civil de Pessoas Jurídicas do local de sua sede, acompanhada de documento comprobatório de seus administradores.

9.5.7. 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.

9.5.8. 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 n.º 5.764, de 16 de dezembro de 1971.

9.5.9. Os documentos apresentados deverão estar acompanhados de todas as alterações ou da consolidação respectiva.

9.6. Habilitação fiscal, social e trabalhista

9.6.1. Prova de inscrição no Cadastro Nacional de Pessoas Jurídicas ou no Cadastro de Pessoas Físicas, conforme o caso.

9.6.2. 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 n.º 1.751, de 02 de outubro de 2014, do Secretário da Receita Federal do Brasil e da Procuradora-Geral da Fazenda Nacional.
9.6.3. Prova de regularidade com o Fundo de Garantia do Tempo de Serviço (FGTS).
9.6.4. 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 n.º 5.452, de 1º de maio de 1943.
9.6.5. Prova de inscrição no cadastro de contribuintes Municipal/Distrital relativo ao domicílio ou sede do fornecedor, pertinente ao seu ramo de atividade e compatível com o objeto contratual.
9.6.6. Prova de regularidade com a Fazenda Municipal/Distrital do domicílio ou sede do fornecedor, relativa à atividade em cujo exercício contrata ou concorre.
9.6.7. Caso o fornecedor seja considerado isento dos tributos Municipal/Distrital 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.
9.6.8. O fornecedor enquadrado como microempreendedor individual que pretenda auferir os benefícios do tratamento diferenciado previstos na Lei Complementar n.º 123, de 2006, estará dispensado da prova de inscrição nos cadastros de contribuintes estadual e municipal.

9.7. Qualificação Econômico-Financeira

9.7.1. Certidão negativa de falência expedida pelo distribuidor da sede do fornecedor - Lei n.º 14.133, de 2021, art. 69, caput, inciso II.
9.7.2. Balanço patrimonial, demonstração de resultado de exercício e demais demonstrações contábeis dos 2 (dois) últimos exercícios sociais, comprovando:
9.7.2.1. índices de Liquidez Geral (LG), Liquidez Corrente (LC), e Solvência Geral (SG) superiores a 1 (um);
9.7.2.2. As empresas criadas no exercício financeiro da licitação deverão atender a todas as exigências da habilitação e poderão substituir os demonstrativos contábeis pelo balanço de abertura; e
9.7.2.3. 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.
9.7.2.4. 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.
9.7.3. Caso a empresa licitante 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% do valor total estimado da contratação.
9.7.4. As empresas criadas no exercício financeiro da licitação deverão atender a todas as exigências da habilitação e poderão substituir os demonstrativos contábeis pelo balanço de abertura (Lei n.º 14.133, de 2021, art. 65, §1º).
9.7.5. O atendimento dos índices econômicos previstos neste item deverá ser atestado mediante declaração assinada por profissional habilitado da área contábil, apresentada pelo fornecedor.

9.8. Qualificação Técnica

9.8.1. Declaração de que o licitante tomou conhecimento de todas as informações e das condições locais para o cumprimento das obrigações objeto da licitação.
9.8.1.1. A declaração poderá ser substituída por declaração formal assinada pelo responsável técnico da licitante acerca do conhecimento pleno das condições e peculiaridades da contratação.
9.8.2. Comprovação de aptidão para execução de serviço de complexidade tecnológica e operacional equivalente ou superior com o objeto desta contratação, ou com o item pertinente, por meio da apresentação de certidões ou atestados, por pessoas jurídicas de direito público ou privado, ou regularmente emitido(s) pelo conselho profissional competente, quando for o caso.
9.8.3. Para comprovação de que a empresa LICITANTE possui capacitação técnica e experiência na execução de serviços correlatos aos do objeto deste Termo de Referência, a empresa deverá, no termos do art. 67 da Lei n.º

14.133/2021, juntamente com a documentação de habilitação necessária, comprovar aptidão para a prestação dos serviços em características, quantidades e prazos compatíveis com o objeto desta licitação, por período não inferior a 12 (doze) meses, por meio de Atestado Técnico em nome da LICITANTE, expedido(s) por pessoa(s) jurídica(s) de direito público ou privado, que comprove ter a empresa LICITANTE executado ou que esteja executando serviços de características técnicas semelhantes ao objeto desta contratação, nos termos da lei.

9.8.4. Para fins da comprovação de que trata este subitem, os atestados deverão dizer respeito a contratos executados com as seguintes características técnicas:

9.8.4.1. Atestado de capacidade técnica de soluções Trend Micro de segurança para *endpoints:* 600 subscrições;

9.8.4.2. Atestado de capacidade técnica de soluções Trend Micro de segurança para servidores: 250 subscrições;

9.8.4.3. Atestado de capacidade técnica de soluções Trend Micro de segurança para e-mails (*antispam*) e/ou ambiente de colaboração: 600 subscrições.

9.8.4.4. para a prestação dos serviços de suporte técnico, garantia, atualização, implantação, configuração e treinamento das soluções de segurança, a CONTRATADA deverá demonstrar, no mínimo, que dispõe de profissionais certificados expedidos pelo fabricante Trend Micro, ou parceiros credenciados pela fabricante:

9.8.4.4.1. Apex One as a Service Certified Professional;

9.8.4.4.2. Deep Security 20 Certified Professional.

9.8.5. Será admitida, para fins de comprovação de quantitativo mínimo, a apresentação e o somatório de diferentes atestados executados de forma concomitante.

9.8.6. Os atestados de capacidade técnica poderão ser apresentados em nome da matriz ou da filial do fornecedor.

9.8.7. O fornecedor disponibilizará todas as informações necessárias à comprovação da legitimidade dos atestados, apresentando, quando solicitado pela CONTRATANTE, cópia do Contrato que deu suporte à contratação, endereço atual da CONTRATANTE e local em que foi executado o objeto contratado, dentre outros documentos.

10 - ESTIMATIVAS DO VALOR DA CONTRATAÇÃO

10.1. O custo estimado total da contratação é de **R$ 3.923.404,60 (três milhões, novecentos e vinte e três mil quatrocentos e quatro reais e sessenta centavos) para 24 (vinte e quatro) meses.**

GRUPO	ITEM	ESPECIFICAÇÃO	CATSER	UNIDADE	QUANTIDADE	VALOR UNITÁRIO	VALOR TOTAL
1	1	Solução de segurança para *endpoints Trend Vision One - Endpoint Security Essentials*	27502	Unidade	1.200	R$ 351,82	R$ 422.184,00
	2	Solução de segurança para servidores físicos, virtuais e em nuvem *Trend Vision One - Endpoint Security Pro*	27502	Unidade	500	R$ 3.000,46	R$ 1.500.230,00
	3	Solução de segurança para e-mails (*antispam*) e ambiente de colaboração *Trend Micro One Email and Collaboration Security - Pro*	27502	Unidade	1.200	R$ 939,43	R$ 1.127.316,00
	4	Solução de segurança para *containers Trend*	27502	Unidade	10	R$ 11.553,99	R$ 115.539,90

		Cloud One Container					
	5	Solução de segurança para dispositivos *mobile Trend Micro Mobile Security*	27502	Unidade	50	R$ 116,51	R$ 5.825,50
	6	Gerenciamento de risco e superfície de ataque *Attack Surface Risk Management (ASRM)*	27502	Unidade	1.700	R$ 238,02	R$ 404.634,00
	7	Instalação/configuração das soluções	26972	Unidade	1	R$ 79.166,66	R$ 79.166,66
	8	Suporte técnico, garantia e atualização 24x7	27332	Mês	24	R$ 9.450,00	R$ 226.800,00
	9	Treinamento das soluções de segurança	3840	Pessoa	2	R$ 20.854,27	R$ 41.708,54
TOTAL							**R$ 3.923.404,60**

10.2. Em caso de licitação para Registro de Preços, os preços registrados poderão ser alterados ou atualizados em decorrência de eventual redução dos preços praticados no mercado ou de fato que eleve o custo dos bens, das obras ou dos serviços registrados, nas seguintes situações:
10.2.1. em caso de força maior, caso fortuito ou fato do príncipe ou em decorrência de fatos imprevisíveis ou previsíveis de consequências incalculáveis, que inviabilizem a execução da ata tal como pactuada, nos termos do disposto na alínea "d" do inciso II do caput do art. 124 da Lei n.º 14.133, de 2021;
10.2.2. em caso de criação, alteração ou extinção de quaisquer tributos ou encargos legais ou superveniência de disposições legais, com comprovada repercussão sobre os preços registrados;
10.2.3. serão reajustados os preços registrados, respeitada a contagem da anualidade e o índice previsto para a contratação; ou
10.2.4. poderão ser repactuados, a pedido do interessado, conforme critérios definidos para a contratação.

11 - ADEQUAÇÃO ORÇAMENTÁRIA

11.1. As despesas decorrentes da presente contratação correrão à conta de recursos específicos consignados no Orçamento Geral da União.
11.2. A contratação será atendida pela seguinte dotação:

- **AÇÃO:** 2000
- **PTRES:** 173704
- **FONTE DE RECURSOS:** 1000000000
- **NATUREZA DA DESPESA:** 339040
- **PI-PLANO INTERNO:** 20000234021

11.3. A dotação relativa aos exercícios financeiros subsequentes será indicada após aprovação da Lei Orçamentária respectiva e liberação dos créditos correspondentes, mediante apostilamento.

11.4. Cronograma Físico-Financeiro

Item		Prazo estimado	2024	2025	2026
1	Trend Vision One - Endpoint Security Essentials	15 dias após emissão das Ordens de Serviço	R$ 211.092,00	R$ 211.092,00	R$ 0,00

2	Trend Vision One - Endpoint Security Pro	15 dias após emissão das Ordens de Serviço	R$ 750.115,00	R$ 750.115,00	R$ 0,00
3	Trend Micro One Email and Collaboration Security - Pro	15 dias após emissão das Ordens de Serviço	R$ 563.658,00	R$ 563.658,00	R$ 0,00
4	Trend Cloud One Container	15 dias após emissão das Ordens de Serviço	R$ 57.769,95	R$ 57.769,95	R$ 0,00
5	Trend Micro Mobile Security	15 dias após emissão das Ordens de Serviço	R$ 2.912,75	R$ 2.912,75	R$ 0,00
6	Attack Surface Risk Management (ASRM)	15 dias após emissão das Ordens de Serviço	R$ 202.317,00	R$ 202.317,00	R$ 0,00
7	Instalação/configuração das soluções	15 dias após emissão das Ordens de Serviço	R$ 79.166,66	R$ 0,00	R$ 0,00
8	Suporte técnico, garantia e atualização 24x7	Mensal, durante 24 (vinte e quatro) meses	R$ 37.800,00	R$ 113.400,00	R$ 75.600,00
9	Treinamento das soluções de segurança	Até 120 dias após emissão da Ordem de Serviço	R$ 41.708,54	R$ 0,00	R$ 0,00
			R$ 1.946.539,90	**R$ 1.901.264,70**	**R$ 75.600,00**

12 - ANEXOS

- Anexo I - Termo de Compromisso de Manutenção de Sigilo e Termo de Confidencialidade e Sigilo (2033249).
- Anexo II - Níveis Mínimos de Serviço (2033254).
- Anexo III - Modelo do Termo de Vistoria Técnica (2033292).
- Anexo IV - Modelo de Recusa de Vistoria Técnica (2033294).
- Anexo V - Modelo da Ordem de Serviço (2085484).
- Anexo VI - Modelo dos Termos de Recebimento Provisório e Definitivo (2086295).
- Anexo VII - Requisitos técnicos das soluções (2086730).
- Anexo VIII - Planilha de Custos e Formação de Preços (2151557).

13 - DA EQUIPE DE PLANEJAMENTO DA CONTRATAÇÃO

13.1. A equipe de planejamento da contratação foi instituída pela Portaria DADM/CNPq n.º 1.881, de 23 de julho de 2024.
13.2. Conforme o § 6º do art. 12 da IN SGD/ME n.º 94/2022, o Termo de Referência será assinado pela equipe de planejamento da contratação e pela autoridade máxima da área de TIC e aprovado pela área competente.

Integrante Requisitante	Integrante Técnico	Integrante Administrativo
(Assinado eletronicamente) **Emerson da Motta Willer** Analista em C&T 15380671	*(Assinado eletronicamente)* **Paulo Rodrigues da Costa** Assistente em C&T 06718345	*(Assinado eletronicamente)* **Cícero Manoel Veríssimo Gomes** Assistente em C&T 06717209

Brasília, na data da assinatura

Autoridade máxima da área de TIC
(Assinado eletronicamente) ***Geraldo Sorte*** Coordenador-Geral de Tecnologia da Informação – CGETI/DASD Portaria DASD/CNPq n.º 1219, de 26 de janeiro de 2023 06719546

Autoridade máxima da área administrativa
(Assinado eletronicamente) ***Débora Peres Menezes*** Diretora de Análise de Soluções Digitais - DASD Portaria Casa Civil n.º 2.003/2023 1159726

Documento assinado eletronicamente por **EMERSON DA MOTTA WILLER**, **Fiscal Requisitante do Contrato**, em 30/10/2024, às 18:49, conforme o art. 6º do Decreto nº 8.539, de 08 de outubro de 2015.

Documento assinado eletronicamente por **PAULO RODRIGUES DA COSTA**, **Integrante técnico da contratação**, em 31/10/2024, às 09:18, conforme o art. 6º do Decreto nº 8.539, de 08 de outubro de 2015.

Documento assinado eletronicamente por **GERALDO SORTE**, **Coordenador-Geral de Tecnologia da Informação PORTARIA Nº 217, DE 3 DE MARÇO DE 2022**, em 31/10/2024, às 11:52, conforme o art. 6º do Decreto nº 8.539, de 08 de outubro de 2015.

Documento assinado eletronicamente por **CICERO MANOEL VERISSIMO GOMES**, **Integrante Administrativo**, em 31/10/2024, às 15:02, 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 **2188650** e o código CRC **9022F886**.

CONSELHO NACIONAL DE DESENVOLVIMENTO CIENTÍFICO E TECNOLÓGICO

COORDENAÇÃO DE INFRAESTRUTURA DE TECNOLOGIA DA INFORMAÇÃO - COINT/CGETI/DASD

ANEXO I

TERMO DE COMPROMISSO DE MANUTENÇÃO DE SIGILO E TERMO DE CONFIDENCIALIDADE E SIGILO

1. TERMO DE COMPROMISSO DE MANUTENÇÃO DE SIGILO

O CONSELHO NACIONAL DE DESENVOLVIMENTO CIENTÍFICO E TECNOLÓGICO – CNPq, Fundação Pública Federal criada pela Lei nº 1.310, de 15 de janeiro de 1951, vinculado ao Ministério da Ciência, Tecnologia e Inovação – MCTI, com Inscrição no CNPJ/MJ sob nº 33.654.831/0001-36, sediado no <ENDEREÇO DO CNPq>, CEP <CEP DO CNPq>, na cidade de Brasília-DF, Telefone: <TELEFONE>, doravante denominado CONTRATANTE, e, de outro lado, a <NOME DA EMPRESA>, sediada em <ENDEREÇO>, CNPJ n.° <CNPJ>, doravante denominada CONTRATADA; CONSIDERANDO que, em razão do CONTRATO n.º XX/20XX doravante denominado CONTRATO PRINCIPAL, a CONTRATADA poderá ter acesso a informações sigilosas da CONTRATANTE; CONSIDERANDO a necessidade de ajustar as condições de revelação destas informações sigilosas, bem como definir as regras para o seu uso e proteção; CONSIDERANDO o disposto na Política de Segurança da Informação da CONTRATANTE; resolvem celebrar o presente TERMO DE COMPROMISSO DE MANUTENÇÃO DE SIGILO, doravante TERMO, vinculado ao CONTRATO PRINCIPAL, mediante as seguintes cláusulas e condições:

Cláusula Primeira – DO OBJETO
Constitui objeto deste TERMO o estabelecimento de condições específicas para regulamentar as obrigações a serem observadas pela CONTRATADA, no que diz respeito ao trato de informações sigilosas, disponibilizadas pela CONTRATANTE, por força dos procedimentos necessários para a execução do objeto do CONTRATO PRINCIPAL celebrado entre as partes e em acordo com o que dispõem a Lei 12.527, de 18/11/2011 e os Decretos 7.724, de 16/05/2012 e 7.845, de 14/11/2012, que regulamentam os procedimentos para acesso e tratamento de informação classificada em qualquer grau de sigilo.

Cláusula Segunda – DOS CONCEITOS E DEFINIÇÕES
Para os efeitos deste TERMO, são estabelecidos os seguintes conceitos e definições: INFORMAÇÃO: dados, processados ou não, que podem ser utilizados para produção e transmissão de conhecimento, contidos em qualquer meio, suporte ou formato. INFORMAÇÃO SIGILOSA: aquela submetida temporariamente à restrição de acesso público em razão de sua imprescindibilidade para a segurança da sociedade e do Estado. CONTRATO PRINCIPAL: contrato celebrado entre as partes, ao qual este TERMO se vincula.

Cláusula Terceira – DA INFORMAÇÃO SIGILOSA
Serão consideradas como informação sigilosa, toda e qualquer informação classificada ou não nos graus de sigilo ultrassecreto, secreto e reservado. O TERMO abrangerá toda informação escrita, verbal, ou em linguagem computacional em qualquer nível, ou de qualquer outro modo apresentada, tangível ou intangível, podendo incluir, mas não se limitando a: *know-how*, técnicas, especificações, relatórios, compilações, código fonte de programas de computador na íntegra ou em partes, fórmulas, desenhos, cópias, modelos, amostras de ideias, aspectos financeiros e econômicos, definições, informações sobre as

atividades da CONTRATANTE e/ou quaisquer informações técnicas/comerciais relacionadas/resultantes ou não ao CONTRATO PRINCIPAL, doravante denominados INFORMAÇÕES, a que diretamente ou pelos seus empregados, a CONTRATADA venha a ter acesso, conhecimento ou que venha a lhe ser confiada durante e em razão das atuações de execução do CONTRATO PRINCIPAL celebrado entre as partes.

Cláusula Quarta – DOS LIMITES DO SIGILO

As obrigações constantes deste TERMO não serão aplicadas às INFORMAÇÕES que:

I. Sejam comprovadamente de domínio público no momento da revelação, exceto se tal fato decorrer de ato ou omissão da CONTRATADA;

II. Tenham sido comprovadas e legitimamente recebidas de terceiros, estranhos ao presente TERMO;

III. Sejam reveladas em razão de requisição judicial ou outra determinação válida do Governo, somente até a extensão de tais ordens, desde que as partes cumpram qualquer medida de proteção pertinente e tenham sido notificadas sobre a existência de tal ordem, previamente e por escrito, dando a esta, na medida do possível, tempo hábil para pleitear medidas de proteção que julgar cabíveis.

Cláusula Quinta – DOS DIREITOS E OBRIGAÇÕES

As partes se comprometem a não revelar, copiar, transmitir, reproduzir, utilizar, transportar ou dar conhecimento, em hipótese alguma, a terceiros, bem como a não permitir que qualquer empregado envolvido direta ou indiretamente na execução do CONTRATO PRINCIPAL, em qualquer nível hierárquico de sua estrutura organizacional e sob quaisquer alegações, faça uso dessas INFORMAÇÕES, que se restringem estritamente ao cumprimento do CONTRATO PRINCIPAL.

Parágrafo Primeiro – A CONTRATADA se compromete a não efetuar qualquer tipo de cópia da informação sigilosa sem o consentimento expresso e prévio da CONTRATANTE.

Parágrafo Segundo – A CONTRATADA compromete-se a dar ciência e obter o aceite formal da direção e empregados que atuarão direta ou indiretamente na execução do CONTRATO PRINCIPAL sobre a existência deste TERMO bem como da natureza sigilosa das informações.

I. A CONTRATADA deverá firmar acordos por escrito com seus empregados visando garantir o cumprimento de todas as disposições do presente TERMO e dará ciência à CONTRATANTE dos documentos comprobatórios.

Parágrafo Terceiro – A CONTRATADA obriga-se a tomar todas as medidas necessárias à proteção da informação sigilosa da CONTRATANTE, bem como evitar e prevenir a revelação a terceiros, exceto se devidamente autorizado por escrito pela CONTRATANTE.

Parágrafo Quarto – Cada parte permanecerá como fiel depositária das informações reveladas à outra parte em função deste TERMO.

I. Quando requeridas, as INFORMAÇÕES deverão retornar imediatamente ao proprietário, bem como todas e quaisquer cópias eventualmente existentes.

Parágrafo Quinto – A CONTRATADA obriga-se por si, sua controladora, suas controladas, coligadas, representantes, procuradores, sócios, acionistas e cotistas, por terceiros eventualmente consultados, seus empregados, contratados e subcontratados, assim como por quaisquer outras pessoas vinculadas à CONTRATADA, direta ou indiretamente, a manter sigilo, bem como a limitar a utilização das informações disponibilizadas em face da execução do CONTRATO PRINCIPAL.

Parágrafo Sexto - A CONTRATADA, na forma disposta no parágrafo primeiro, acima, também se obriga a:

I. Não discutir perante terceiros, usar, divulgar, revelar, ceder a qualquer título ou dispor das INFORMAÇÕES, no território brasileiro ou no exterior, para nenhuma pessoa, física ou jurídica, e para nenhuma outra finalidade que não seja exclusivamente relacionada ao objetivo aqui referido,

cumprindo-lhe adotar cautelas e precauções adequadas no sentido de impedir o uso indevido por qualquer pessoa que, por qualquer razão, tenha acesso a elas;

II. Responsabilizar-se por impedir, por qualquer meio em direito admitido, arcando com todos os custos do impedimento, mesmo judiciais, inclusive as despesas processuais e outras despesas derivadas, a divulgação ou utilização das INFORMAÇÕES por seus agentes, representantes ou por terceiros;

III. Comunicar à CONTRATANTE, de imediato, de forma expressa e antes de qualquer divulgação, caso tenha que revelar qualquer uma das INFORMAÇÕES, por determinação judicial ou ordem de atendimento obrigatório determinado por órgão competente; e

IV. Identificar as pessoas que, em nome da CONTRATADA, terão acesso às informações sigilosas.

Cláusula Sexta – DA VIGÊNCIA

O presente TERMO tem natureza irrevogável e irretratável, permanecendo em vigor desde a data de sua assinatura até expirar o prazo de classificação da informação a que a CONTRATADA teve acesso em razão do CONTRATO PRINCIPAL.

Cláusula Sétima – DAS PENALIDADES

A quebra do sigilo e/ou da confidencialidade das INFORMAÇÕES, devidamente comprovada, possibilitará a imediata aplicação de penalidades previstas conforme disposições contratuais e legislações em vigor que tratam desse assunto, podendo até culminar na rescisão do CONTRATO PRINCIPAL firmado entre as PARTES. Neste caso, a CONTRATADA, estará sujeita, por ação ou omissão, ao pagamento ou recomposição de todas as perdas e danos sofridos pela CONTRATANTE, inclusive as de ordem moral, bem como as de responsabilidades civil e criminal, as quais serão apuradas em regular processo administrativo ou judicial, sem prejuízo das demais sanções legais cabíveis, conforme Art. 87 da Lei nº. 8.666/93.

Cláusula Oitava – DISPOSIÇÕES GERAIS

Este TERMO de Confidencialidade é parte integrante e inseparável do CONTRATO PRINCIPAL.

Parágrafo Primeiro – Surgindo divergências quanto à interpretação do disposto neste instrumento, ou quanto à execução das obrigações dele decorrentes, ou constatando-se casos omissos, as partes buscarão solucionar as divergências de acordo com os princípios de boa-fé, da equidade, da razoabilidade, da economicidade e da moralidade.

Parágrafo Segundo – O disposto no presente TERMO prevalecerá sempre em caso de dúvida e, salvo expressa determinação em contrário, sobre eventuais disposições constantes de outros instrumentos conexos firmados entre as partes quanto ao sigilo de informações, tal como aqui definidas.

Parágrafo Terceiro – Ao assinar o presente instrumento, a CONTRATADA manifesta sua concordância no sentido de que:

I. A CONTRATANTE terá o direito de, a qualquer tempo e sob qualquer motivo, auditar e monitorar as atividades da CONTRATADA;

II. A CONTRATADA deverá disponibilizar, sempre que solicitadas formalmente pela CONTRATANTE, todas as informações requeridas pertinentes ao CONTRATO PRINCIPAL.

III. A omissão ou tolerância das partes, em exigir o estrito cumprimento das condições estabelecidas neste instrumento, não constituirá novação ou renúncia, nem afetará os direitos, que poderão ser exercidos a qualquer tempo;

IV. Todas as condições, termos e obrigações ora constituídos serão regidos pela legislação e regulamentação brasileiras pertinentes;

V. O presente TERMO somente poderá ser alterado mediante TERMO aditivo firmado pelas partes;

VI. Alterações do número, natureza e quantidade das informações disponibilizadas para a CONTRATADA não descaracterizarão ou reduzirão o compromisso e as obrigações pactuadas neste TERMO, que permanecerá válido e com todos seus efeitos legais em qualquer uma das situações tipificadas neste instrumento;

VII. O acréscimo, complementação, substituição ou esclarecimento de qualquer uma das informações disponibilizadas para a CONTRATADA, serão incorporados a este TERMO, passando a fazer dele parte integrante, para todos os fins e efeitos, recebendo também a mesma proteção descrita para as informações iniciais disponibilizadas, sendo necessário a formalização de TERMO aditivo 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.

Cláusula Nona – DO FORO

A CONTRATANTE elege o foro da Seção Judiciária do Distrito Federal, onde está localizada a sede da CONTRATANTE, para dirimir quaisquer dúvidas originadas do presente TERMO, com renúncia expressa a qualquer outro, por mais privilegiado que seja. E, por assim estarem justas e estabelecidas as condições, o presente TERMO DE COMPROMISSO DE MANUTENÇÃO DE SIGILO é assinado pelas partes em 2 vias de igual teor e um só efeito.

Brasília, _____ de _____ de 20__

De acordo,

Contratante	**Contratada**
_____	_____
<nome> <qualificação>	<nome> <qualificação>

Testemunhas

_____	_____
<nome> <qualificação> <rg> <CPF>	<nome> <qualificação> <rg> <CPF>

2. TERMO DE CONFIDENCIALIDADE E SIGILO

Eu _____, nacionalidade, estado civil, profissão, CPF, abaixo firmado, assumo o compromisso de manter confidencialidade e sigilo sobre todos os dados e informações a que tiver acesso como autoridade, servidor, prestador de serviço, consultor ou estagiário, nos termos da Portaria CNPq nº 1.019/2022, de 30 de agosto de 2022, que instituiu a Política de Segurança da Informação – PoSIN do Conselho Nacional de Desenvolvimento Científico e Tecnológico – CNPq.

Por este termo de confidencialidade e sigilo comprometo-me a:

1. não utilizar dados e informações institucionais a que tiver acesso, para gerar benefício próprio exclusivo e/ou unilateral, presente ou futuro, ou para o uso de terceiros;

2. não efetuar nenhuma gravação ou cópia de arquivos físicos ou eletrônicos com dados e informações institucionais a que tiver acesso;
3. não me apropriar de material, dados e informações institucionais, sejam esses com ou sem confidencialidade e/ou sigilo que venha a ser a mim disponibilizados para atividades da Fundação; e
4. não repassar o conhecimento de quaisquer dados e informações, responsabilizando-me por todas as pessoas que vierem a ter acesso às informações, por meu intermédio, e obrigando-me, assim, a ressarcir a ocorrência de qualquer dano e/ou prejuízo oriundo de uma eventual publicação com quebra de confidencialidade ou sigilo das informações por mim fornecidas.

Neste Termo, as seguintes expressões são assim definidas:

- Dado institucional é aquele que permite obter a informação gerada, custodiada, manipulada, utilizada ou armazenada no CNPq compõe o seu ativo da informação e deve ser protegida conforme a PoSIN, normas complementares e procedimentos em vigor, incluídas as referências legais e normativas citadas nesta Portaria.
- Dado pessoal é aquele que possibilita a identificação, direta ou indireta, da pessoa natural.
- Informação institucional significa todo conhecimento revelado sob a forma escrita, verbal ou por quaisquer outros meios a partir de dado institucional.

Pelo descumprimento do presente Termo de Confidencialidade e Sigilo, fica o abaixo assinado ciente de todas as sanções administrativas, judiciais e penais que poderão advir como resultado de seu ato.

Brasília, ____ de _____ de 20___

_____

<nome>
<Cargo / Função / Setor>
<CPF>

Referência: Processo nº 01300.005789/2023-78 SEI nº 2033249

Documento assinado eletronicamente por **PAULO RODRIGUES DA COSTA**, **Integrante técnico da contratação**, em 24/07/2024, às 10:04, conforme o art. 6º do Decreto nº 8.539, de 08 de outubro de 2015.

Documento assinado eletronicamente por **EMERSON DA MOTTA WILLER**, **Integrante requisitante da contratação**, em 24/07/2024, às 10:24, conforme o art. 6º do Decreto nº 8.539, de 08 de outubro de 2015.

Documento assinado eletronicamente por **CICERO MANOEL VERISSIMO GOMES**, **Gestor do Contrato**, em 24/07/2024, às 18:47, 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 **2033249** e o código CRC **3A7D96CB**.

CONSELHO NACIONAL DE DESENVOLVIMENTO CIENTÍFICO E TECNOLÓGICO

COORDENAÇÃO DE INFRAESTRUTURA DE TECNOLOGIA DA INFORMAÇÃO - COINT/CGETI/DASD

ANEXO II

NÍVEIS MÍNIMOS DE SERVIÇO

1. Os níveis mínimos de serviço representam um compromisso assumido por um prestador de serviços perante um cliente para que se possa medir como estão se comportando as “entregas” programadas dos serviços.
2. Por se tratarem de níveis “mínimos”, entende-se que a CONTRATADA deverá entregar, no mínimo, os resultados definidos, para que não esteja sujeita a glosas ou descontos nos seus vencimentos.
3. Os indicadores descritos neste Anexo aplicam-se para todos os serviços prestados.

IAP - ÍNDICE DE ATENDIMENTO NO PRAZO	
FINALIDADE	Medir o tempo de atraso na entrega dos produtos e serviços constantes nas Ordens de Serviço.
META A CUMPRIR	IAP <= 0
INSTRUMENTO DE MEDIÇÃO	Ordem de Serviço, Termo de Recebimento Provisório e Termo de Recebimento Definitivo.
FORMA DE ACOMPANHAMENTO	A avaliação será realizada por meio da verificação da data de entrega constante na Ordem de Serviço e da data de recebimento provisório do produto ou serviço.
PERIODICIDADE	Por Ordem de Serviço
MECANISMOS DE CÁLCULO	TEX = (DEE - DDE) Onde: TEX = Tempo de execução (quantidade de dias entre o envio da OS e o recebimento provisório). DDE = Data definida para entrega dos produtos/serviços constantes na Ordem de Serviço. DEE = Data efetiva da entrega das licenças.
INÍCIO DA VIGÊNCIA	A partir da emissão da Ordem de Serviço.

FAIXA DE AJUSTE	• Para valores iguais ou inferiores a 0 (zero) – Pagamento integral da OS; • De 1 a 15 dias de atraso – Glosa de 5% sobre o valor da OS; • De 16 a 20 dias de atraso – Glosa de 10% sobre o valor da OS; • De 21 a 30 dias de atraso - Glosa de 15% sobre o valor da OS; • Acima de 30 dias de atraso – Será aplicada a multa de 3% sobre o valor do Contrato, sem prejuízo da glosa anterior.
OBSERVAÇÃO	A meta definida visa garantir a entrega dos produtos e serviços constantes nas Ordens de Serviço dentro do prazo previsto.

SAP - INDICADOR DE SUPORTE ATENDIDO DENTRO DO PRAZO			
FINALIDADE	Assegurar que os chamados estejam dentro dos prazos acordados de início e fim de atendimento.		
META A CUMPRIR	**Severidade**	**Tempo de resolução do chamado**	
	1 - Urgente	6 horas	
	2 - Crítico	12 horas	
	3 - Não crítico	24 horas	
INSTRUMENTO DE MEDIÇÃO	Registro/resolução de cada solicitação/incidente de suporte técnico (chamado).		
FORMA DE ACOMPANHAMENTO	Cálculo do prazo de registro/resolução de cada solicitação/incidente de suporte técnico (chamado) em relação ao Nível de Serviço.		
PERIODICIDADE	Mensal.		
MECANISMOS DE CÁLCULO	**Severidade**	**Descrição**	**Penalidades**
	1 - Urgente	Até 2 horas corridas de atraso, além do prazo indicado no subitem "Meta a cumprir" desta tabela.	**1** – Advertência; **2** – Havendo recorrência, multa de 0,8% (zero vírgula oito por cento) por hora de atraso, calculada sobre o valor mensal do item de licença; considerando-se o item de licença como sendo o valor anual pago por todas as licenças do item em questão, por exemplo, o item "Solução de Segurança para Privilégios e Acessos – Proteção e Monitoração de Acessos a Ativos e Sistemas", ou seja, o valor total anual para as 20 licenças desse item.
		Superior a 2 horas e inferior ou igual a 8 horas corridas de atraso, além do prazo definido no subitem "Meta a cumprir" desta tabela.	**3** – Multa de 1,0% (um por cento) por hora de atraso, calculada sobre o valor mensal do item de licença, sem prejuízo ao item anterior; considerando-se o item de licença como sendo o valor anual pago por todas as licenças do item em

			questão, por exemplo, o item "Solução de Segurança para Privilégios e Acessos – Proteção e Monitoração de Acessos a Ativos e Sistemas", ou seja, o valor total anual para as 20 licenças desse item.
		Superior a 8 horas corridas de atraso, além do prazo definido no subitem "Meta a cumprir" desta tabela.	**4** – Multa de 1,2% (um vírgula dois por cento) por hora de atraso, calculada sobre o valor mensal do item de licença, sem prejuízo ao item anterior, e outras sanções administrativas a critério da Contratante; considerando-se o item de licença como sendo o valor anual pago por todas as licenças do item em questão, por exemplo, o item "Solução de Segurança para Privilégios e Acessos – Proteçãoe Monitoração de Acessos a Ativos e Sistemas", ou seja, o valor total anual para as 20 licenças desse item.
	2 - Crítico	Até 4 horas corridas de atraso, além do prazo indicado no subitem "Meta a cumprir" desta tabela.	**5** – Advertência; **6** – Para as demais ocorrências, multa de 0,6% (zero vírgula seis por cento) por hora de atraso, calculada sobre o valor mensal do item de licença; considerando-se o item de licença como sendo o valor anual pago por todas as licenças do item em questão, por exemplo, o item "Solução de Segurança para Privilégios e Acessos – Proteção e Monitoração de Acessos a Ativos e Sistemas", ou seja, o valor total anual para as 20 licenças desse item.
		Superior a 4 horas e inferior ou igual a 24 horas corridas de atraso, além do prazo indicado no subitem "Meta a cumprir" desta tabela.	**7** – Multa de 0,8% (zero vírgula oito por cento) por hora de atraso, calculada sobre o valor mensal do item de licença, sem prejuízo ao item anterior; considerando-se o item de licença como sendo o valor anual pago por todas as licenças do item em questão, por exemplo, o item "Solução de Segurança para Privilégios e Acessos – Proteção e Monitoração de Acessos a Ativos e Sistemas", ou seja, o valor total anual para as 20 licenças desse item.

		Superior a 24 horas corridas de atraso, além do prazo indicado no subitem "Meta a cumprir" desta tabela.	**8** – Multa de 1.0% (um por cento) por hora de atraso, calculada sobre o valor mensal do item de licença, sem prejuízo ao item anterior, e outras sanções administrativas a critério da Contratante; considerando-se o item de licença como sendo o valor anual pago por todas as licenças do item em questão, por exemplo, o item "Solução de Segurança para Privilégios e Acessos – Proteção e Monitoração de Acessos a Ativos e Sistemas", ou seja, o valor total anual para as 20 licenças desse item.
	3 - Não crítico	Até 48 horas corridas de atraso, além do prazo indicado no subitem "Meta a cumprir" desta tabela.	**9** – Advertência; **10** – Para as demais ocorrências, multa de 0,5% (zero vírgula cinco por cento) por hora de atraso, calculada sobre o valor mensal do item de licença; considerando-se o item de licença como sendo o valor anual pago por todas as licenças do item em questão, por exemplo, o item "Solução de Segurança para Privilégios e Acessos – Proteção eMonitoração de Acessos a Ati vos e Sistemas", ou seja, o valor total anual para as 20 licenças desse item. **11** – Se o somatório das multas aplicadas com relação às obrigações relativas a um mesmo item de licença ultrapassar 20% do seu valor de aquisição, poderá ensejar a rescisão do Contrato, independentemente de aplicação das sanções administrativas cabíveis.

a. Havendo qualquer interrupção no funcionamento da solução, a CONTRATANTE efetuará abertura de chamado reportando todos os sintomas.
b. Os chamados serão classificados conforme as severidades Urgente, Crítico e Não crítico.
c. Todos os prazos especificados no item "Meta a cumprir" são contados a partir da abertura do respectivo número de identificação do chamado.
d. A abertura do chamado com fornecimento do seu número de identificação (protocolo de atendimento) deve ocorrer no prazo máximo de 15 minutos a partir do contato pela Contratante com o número fornecido pela CONTRATADA.
e. O atendimento aos chamados pode ocorrer remotamente ou de forma presencial. Atendimentos remotos não resolvidos que ultrapassem 24 horas devem ser continuados de forma presencial.
f. Após a conclusão do suporte, a CONTRATADA comunicará à CONTRATANTE e solicitará autorização para o fechamento do chamado. Caso a CONTRATANTE não confirme a solução definitiva do

problema, o chamado permanecerá aberto até que seja efetivamente solucionado pela CONTRATADA. Neste caso, a CONTRATANTE informará as pendências relativas ao chamado aberto.

g. Sempre que a meta deste indicador não for cumprida, a CONTRATANTE emitirá notificação à CONTRATADA, que terá o prazo de, no máximo, 5 (cinco) dias úteis, contados a partir do recebimento da notificação, para apresentar as justificativas para as falhas verificadas.
h. Caso não haja manifestação dentro desse prazo ou caso a CONTRATANTE entenda serem improcedentes as justificativas apresentadas, será iniciado processo de aplicação das penalidades previstas, conforme a severidade e o respectivo tempo de atendimento não cumprido.

Referência: Processo nº 01300.005789/2023-78 SEI nº 2033254

Documento assinado eletronicamente por **PAULO RODRIGUES DA COSTA**, **Integrante técnico da contratação**, em 24/07/2024, às 10:04, conforme o art. 6º do Decreto nº 8.539, de 08 de outubro de 2015.

Documento assinado eletronicamente por **EMERSON DA MOTTA WILLER**, **Integrante requisitante da contratação**, em 24/07/2024, às 10:24, conforme o art. 6º do Decreto nº 8.539, de 08 de outubro de 2015.

Documento assinado eletronicamente por **CICERO MANOEL VERISSIMO GOMES**, **Gestor do Contrato**, em 24/07/2024, às 18:47, 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 **2033254** e o código CRC **D47C846E**.

CONSELHO NACIONAL DE DESENVOLVIMENTO CIENTÍFICO E TECNOLÓGICO

COORDENAÇÃO DE INFRAESTRUTURA DE TECNOLOGIA DA INFORMAÇÃO - COINT/CGETI/DASD

ANEXO III

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

Referência: Processo nº 01300.005789/2023-78 SEI nº 2033292

Documento assinado eletronicamente por **PAULO RODRIGUES DA COSTA**, **Integrante técnico da contratação**, em 24/07/2024, às 10:05, conforme o art. 6º do Decreto nº 8.539, de 08 de outubro de 2015.

Documento assinado eletronicamente por **EMERSON DA MOTTA WILLER**, **Integrante requisitante da contratação**, em 24/07/2024, às 10:24, conforme o art. 6º do Decreto nº 8.539, de 08 de outubro de 2015.

Documento assinado eletronicamente por **CICERO MANOEL VERISSIMO GOMES**, **Gestor do Contrato**, em 24/07/2024, às 18:47, 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 **2033292** e o código CRC **69B2D7DD**.

CONSELHO NACIONAL DE DESENVOLVIMENTO CIENTÍFICO E TECNOLÓGICO

COORDENAÇÃO DE INFRAESTRUTURA DE TECNOLOGIA DA INFORMAÇÃO - COINT/CGETI/DASD

ANEXO IV

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 01300.005789/2023-78 SEI nº 2033294

Documento assinado eletronicamente por **PAULO RODRIGUES DA COSTA**, **Integrante técnico da contratação**, em 24/07/2024, às 10:05, conforme o art. 6º do Decreto nº 8.539, de 08 de outubro de 2015.

Documento assinado eletronicamente por **EMERSON DA MOTTA WILLER**, **Integrante requisitante da contratação**, em 24/07/2024, às 10:24, conforme o art. 6º do Decreto nº 8.539, de 08 de outubro de 2015.

Documento assinado eletronicamente por **CICERO MANOEL VERISSIMO GOMES**, **Gestor do Contrato**, em 24/07/2024, às 18:47, 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 **2033294** e o código CRC **C9A04A02**.

CONSELHO NACIONAL DE DESENVOLVIMENTO CIENTÍFICO E TECNOLÓGICO

COORDENAÇÃO DE PROJETOS E DESENHO DE SERVIÇOS DE TECNOLOGIA DA INFORMAÇÃO - COPDS/CGETI/DASD

ANEXO V

MODELO DA ORDEM DE SERVIÇO

1. IDENTIFICAÇÃO	
Contrato	
Contratada	
Objeto contratado	
Ordem de Serviço	
Data de emissão	
Área requisitante	

2. ESPECIFICAÇÃO DOS PRODUTOS/SERVIÇOS E VOLUMES

ID	PRODUTO/SERVIÇO	MÉTRICA	QUANTIDADE	VALOR
1				R$
2				R$
3				R$

3. INSTRUÇÕES COMPLEMENTARES

4. CRONOGRAMA

ID	PRODUTO/SERVIÇO	INÍCIO	ENTREGA	PRAZO GARANTIA
1				
2				

5. DOCUMENTOS/PRODUTOS A SEREM ENTREGUES

6. CIÊNCIA

CONTRATANTE
(Assinado eletronicamente) **NOME** Portaria de nomeação do gestor
CONTRATADA
(Assinado eletronicamente) **NOME** Preposto da contratada

Referência: Processo nº 01300.005789/2023-78 SEI nº 2085484

Documento assinado eletronicamente por **PAULO RODRIGUES DA COSTA**, **Integrante técnico da contratação**, em 24/07/2024, às 10:05, conforme o art. 6º do Decreto nº 8.539, de 08 de outubro de 2015.

Documento assinado eletronicamente por **EMERSON DA MOTTA WILLER**, **Integrante requisitante da contratação**, em 24/07/2024, às 10:26, conforme o art. 6º do Decreto nº 8.539, de 08 de outubro de 2015.

Documento assinado eletronicamente por **CICERO MANOEL VERISSIMO GOMES**, **Gestor do Contrato**, em 24/07/2024, às 18:51, 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 **2085484** e o código CRC **7BA4E362**.

CONSELHO NACIONAL DE DESENVOLVIMENTO CIENTÍFICO E TECNOLÓGICO

COORDENAÇÃO DE PROJETOS E DESENHO DE SERVIÇOS DE TECNOLOGIA DA INFORMAÇÃO - COPDS/CGETI/DASD

ANEXO VI

MODELO DOS TERMOS DE RECEBIMENTO PROVISÓRIO E DEFINITIVO

1. TERMO DE RECEBIMENTO PROVISÓRIO

1. TERMO DE RECEBIMENTO PROVISÓRIO					
Ordem de Serviço	-------	**Data de emissão da OS**	-------	**Número do contrato**	-------
2. INFORMAÇÕES DA CONTRATADA					
Razão Social	-------				
CNPJ	-------				
Endereço	-------				
3. INFORMAÇÕES DA CONTRATANTE					
Razão Social	-------				
CNPJ	-------				
Endereço	-------				

4. IDENTIFICAÇÃO DO SERVIÇO

Grupo	Item	Descrição do Serviço	Unidade	Valor
1	1			R$
	2			R$
TOTAL:				**R$**

5. RECEBIMENTO

6. ASSINATURA

(*Assinado eletronicamente*) **NOME DO FISCAL TÉCNICO** Portaria de nomeação do fiscal técnico	(*Assinado eletronicamente*) **NOME DO PREPOSTO** Preposto do contrato n.º 001/2024

2. TERMO DE RECEBIMENTO DEFINITIVO

1. TERMO DE RECEBIMENTO DEFINITIVO

Ordem de Serviço	-------	Data de emissão da OS	-------	Número do contrato	-------

2. INFORMAÇÕES DA CONTRATADA	
Razão Social	-------
CNPJ	-------
Endereço	-------

3. INFORMAÇÕES DA CONTRATANTE	
Razão Social	-------
CNPJ	-------
Endereço	-------

4. IDENTIFICAÇÃO DO SERVIÇO

Grupo	Item	Descrição do Serviço	Unidade	Valor
1	1			R$
	2			R$
TOTAL:				**R$**

5. RECEBIMENTO

6. ASSINATURA	
(*Assinado eletronicamente)* **NOME DO FISCAL TÉCNICO** Portaria de nomeação do fiscal técnico	(*Assinado eletronicamente)* **NOME DO PREPOSTO** Preposto do contrato n.º XX/2024

Referência: Processo nº 01300.005789/2023-78 SEI nº 2086295

Documento assinado eletronicamente por **PAULO RODRIGUES DA COSTA**, **Integrante técnico da contratação**, em 24/07/2024, às 10:05, conforme o art. 6º do Decreto nº 8.539, de 08 de outubro de 2015.

Documento assinado eletronicamente por **EMERSON DA MOTTA WILLER**, **Integrante requisitante da contratação**, em 24/07/2024, às 10:25, conforme o art. 6º do Decreto nº 8.539, de 08 de outubro de 2015.

Documento assinado eletronicamente por **CICERO MANOEL VERISSIMO GOMES**, **Gestor do Contrato**, em 24/07/2024, às 18:51, 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 **2086295** e o código CRC **1B264128**.

CONSELHO NACIONAL DE DESENVOLVIMENTO CIENTÍFICO E TECNOLÓGICO

COORDENAÇÃO DE PROJETOS E DESENHO DE SERVIÇOS DE TECNOLOGIA DA INFORMAÇÃO - COPDS/CGETI/DASD

ANEXO VII

REQUISITOS TÉCNICOS DAS SOLUÇÕES

Solução de segurança de *endpoints* e Solução de segurança de servidores físicos, virtuais e em nuvem	
ID	**DESCRIÇÃO**
1	**Funcionalidades gerais**
1.1	Deve permitir a programação de atualizações automáticas das listas de definições de vírus, a partir de local predefinido da rede, ou de site seguro da internet, com frequência (no mínimo diária) e horários definidos pelo administrador da solução.
1.2	Deve permitir atualização incremental da lista de definições de vírus.
1.3	Deve permitir a atualização automática do *engine* do programa de proteção a partir de localização na rede local ou na internet, a partir de fonte autenticável.
1.4	Deve permitir o *rollback* das atualizações das listas de definições de vírus e *engines*.
1.5	Deve permitir a indicação de agentes para efetuar a função de replicador de atualizações e configurações, de forma que outros agentes possam utilizá-los como fonte de atualizações e configurações, não sendo necessária a comunicação direta com o servidor de *anti-malware* para essas tarefas.
1.6	Deve permitir que os agentes de atualização possam replicar os componentes de vacinas, motores de escaneamento, versão de programas, *hotfix* e configurações específicas de domínios da árvore de gerenciamento.
1.7	Deve permitir proteção das configurações da solução instalada na estação de trabalho através de senha ou controle de acesso, em ambos os casos, controlada por política gerenciada pelo console de administração da solução completa.
1.8	Deve possibilitar instalação "silenciosa".
1.9	Deve possuir firewall integrado.
1.10	Deve possuir EDR - Detecção e Resposta a Ameaças.
1.11	Deve possuir XDR - Extended Detection and Response.
1.12	Deve possuir *machine learning* e *behavioral analysis* para detecção de ameaças.
1.13	Deve possuir console de gerenciamento centralizado.
1.14	Deve possuir recursos de prevenção de perda de dados (DLP).
1.15	Deve possuir *whitelisting* de aplicações pré-aprovadas para execução.
1.16	Deve permitir integração com sistemas de gerenciamento de eventos de segurança (SIEM).
1.17	Deve permitir *rollback* de ações maliciosas.
1.18	Deve possuir capacidades de *threat hunting*.

1.19	Deve possui capacidade de executar arquivos suspeitos em ambiente isolado (sandbox).
2	**Proteção anti-malware para estações de trabalho Microsoft Windows**
2.1	A solução deve atender a estações de trabalho com solução de virtualização de desktops com o Sistema Operacional Windows.
2.2	Deve ser capaz de realizar a proteção a códigos maliciosos nos sistemas operacionais: • Microsoft Windows 8 e versões superiores.
2.3	Suportar as seguintes plataformas virtuais: • VMware Vsphere ESXi 7 e versões superiores.
2.4	Deve detectar, analisar e eliminar, automaticamente e em tempo real, programas maliciosos em: • Processos em execução em memória principal (RAM); • Arquivos executados, criados, copiados, renomeados, movidos ou modificados, inclusive em sessões de linha de comando (DOS ou Shell); • Arquivos compactados automaticamente, em pelo menos nos seguintes formatos: zip, exe, arj, mime/uu, Microsoft cab; • Arquivos recebidos por meio de programas de comunicação instantânea tais como Whatsapp, Telegram, Facebook Messenger, Microsoft Teams, Zoom, Google Meet; • Arquivos recebidos a partir de sites Web; • Arquivos acessados ou recebidos por e-mail.
2.5	Deve permitir diferentes configurações de detecção (varredura ou rastreamento): • Em tempo real de arquivos acessados pelo usuário; • Em tempo real dos processos em memória, para a captura de programas maliciosos executados em memória, sem a necessidade de escrita de arquivo; • Manual, imediato ou programável, com interface gráfica em janelas, personalizável, com opção de limpeza; • Por linha de comando parametrizável.
2.6	Deve possuir funcionalidade de "*Machine Learning*" utilizando como fonte de aprendizado a rede de inteligência do fabricante, identificando os aspectos maliciosos, características de boa pontuação e correlacionando, no mínimo, com as seguintes técnicas de proteção a vetores de ataque: • Reputação de URL para exploração de navegadores, websites infectados e Office Exploits; • Reputação de arquivos para downloads de arquivos e anexos de e-mail.
2.7	Execução do instalador de software com classificação comportamental do instalador.
2.8	Execução do malware de software com classificação comportamental do instalador.
3	**Proteção *anti-malware* para estações de trabalho Linux**
3.1	A solução deve atender a estações de trabalho Linux.
3.2	Deve ser capaz de realizar a proteção a códigos maliciosos nos seguintes sistemas operacionais, no mínimo: • Ubuntu Linux 20.04 e versões superiores; • Suse Linux Enterprise.
3.3	Deve possuir integração com a solução de Detecção e Resposta Avançada de Ataques (XDR).

3.4	A console de gerenciamento deve permitir o gerenciamento das políticas de segurança através da Internet.
4	**Solução de segurança para proteção para Data Center**
4.1	A solução de deve atender a um ambiente de aproximadamente 500 sockets e 30 hosts.
4.2	Deve ser compatível com pelo menos os seguintes sistemas operacionais nas versões indicadas e versões superiores: • CentOS 7 e superiores; • Debian GNU/Linux 10 e superiores; • Windows Server 2008 e superiores; • Oracle Linux 7 e superiores; • Red Hat Enterprise Linux 7 e superiores; • VMWare ESXi 7 e superiores.
4.3	Suportar as seguintes plataformas virtuais: • VMware Vsphere ESXi 7 e versões superiores.
4.4.	O console de gerenciamento deve ser on-premises, permitindo o gerenciamento das políticas de segurança através da Internet.
4.5.	Deve possuir integração com a solução de Detecção e Resposta Avançada de Ataques (XDR).
4.6	Deve ser gerenciada por console Web, compatível com pelo menos os browsers Microsoft Edge, Firefox e Google Chrome.
4.7	Deve suportar certificado digital para gerenciamento.
4.8	O console de administração deve permitir o envio de notificações via SMTP.
4.9	Todos os eventos e ações realizadas no console de gerenciamento precisam ser gravados, visando a auditoria.
4.10	Deve permitir a criação de widgets para facilitar a administração e visualização dos eventos.
4.11	A funcionalidade de anti-malware deve possuir as seguintes características: • Deve permitir a proteção contra códigos maliciosos através da instalação de agentes, permitindo rastrear ameaças em tempo real, varredura sob demanda e agendamento, com possibilidade de tomada de ações distintas para cada tipo de ameaça; • Deve possibilitar a criação de listas de exclusão, para que o processo do antivírus não execute a varredura em determinados diretórios ou arquivos do sistema operacional; • Deve possuir listas de exclusão separadas por módulo da proteção anti-malware como exclusão das detecções por comportamento, exclusão por machine learning e exclusão por assinatura; • Em plataforma Windows, deve permitir criar exclusões de escaneamento a partir do certificado digital das aplicações; • Deve possibilitar a verificação de ameaças dentro de arquivos compactados, efetuando a limpeza apenas de arquivos maliciosos em casos de detecção. A limpeza deve ocorrer sem a descompactação do arquivo; • O scan de arquivos comprimidos deve ser de no mínimo 6 camadas de compressão; • O scan de arquivos comprimidos do tipo OLE deve ser de no mínimo 20 camadas de compressão.

4.12	A funcionalidade de Proteção Contra URLs Maliciosas deve possuir as seguintes características: • Deve permitir a proteção contra acesso a websites ou URLs consideradas maliciosas ou de baixa reputação; • A lista de URLs deve ser fornecida e atualizada automaticamente pelo fabricante, permitindo a consulta em uma base local ou na nuvem da reputação das URLs acessadas;
4.13	O módulo de Firewall deve possuir as seguintes características: • Operar como firewall de host, através da instalação de agente nos servidores protegidos; • Deve possuir a capacidade de controlar o tráfego baseado nos tipos de protocolos, endereços IP e intervalo de portas.
5	**Detecção e Resposta Avançada de Ataques (XDR)**
5.1	Deve suportar a coleta de dados de diversas fontes, incluindo *endpoints*, rede, filtros da web e sensores de nuvem, para acelerar a detecção e resposta a incidentes e reduzir os tempos de resposta.
5.2	Deve permitir a integração com plataformas de segurança via API.
5.3	Deve ser capaz de ingerir diversas fontes de dados, entre elas *Network Intrusion Detection Systems* (NIDS), *Endpoint Protection Platforms* (EPP), E*ndpoint Detection and Response* (EDR), com objetivo de aprimorar o processo de detecção de ameaças e tornar ágil processo de correlação e investigação de alertas.
5.4	Deve permitir a integração com a ferramenta de gerenciamento de tickets CA Service Desk e GLPI possibilitando a gestão unificada de incidentes.
5.5	A quantidade de coletores necessários para a total ingestão de eventos do ambiente não deve onerar ou gerar custos adicionais de licenciamento;
5.6	Deve fornecer ambiente gráfico para criação de fluxos de interação.
5.7	Deve permitir a automação das atividades de resposta a incidentes com base nas necessidades e processos mapeados.
5.8	Deve fornecer visibilidade de possíveis vazamentos de contas de usuário.
5.9	Deve fornecer informações de elevação de privilégio das contas nos dispositivos.
5.10	Deve ser compatível com a solução NSX da VMware para permitir integração com os ambientes virtualizados do CNPq.
5.11	Deve realizar a coleta e análise dos dados de atividade de endpoints de desktop e servidor.
5.12	Deve realizar a coleta e análise dos dados de atividade de contas de e-mail.
5.13	Deve fornecer insights sobre a postura de segurança baseado em um índice geral de risco, exposição de dispositivos, ataques em andamento e outros fatores relacionados.
5.14	Deve realizar a descoberta dos ativos organizacionais expostos a ataques, incluindo dispositivos e ativos voltados para a Internet, contas, aplicativos em nuvem e ativos em nuvem.
5.15	Deve realizar a avaliação das comunicações com destino a internet relacionadas a atividades ou endereços maliciosos ou vulneráveis, identificando os usuários e dispositivos envolvidos, fornecendo informações de mitigação do risco detectado.
5.16	Possuir console Web para gerenciamento e administração da ferramenta.
5.17	Possuir modelos pré-definidos pelo fabricante de atividades suspeitas e maliciosas para identificação e categorização de ameaças no ambiente.
5.18	Deve fornecer um índice de risco com base nas configurações de produtos integrados do fornecedor para reduzir o risco induzido por erros humanos.
5.19	Permitir criação de listas de exceção de objetos para redução de falso-positivo.

5.20	Os modelos de detecção deverão possuir níveis de severidade (score) individuais para cada modelo em pelo menos os seguintes níveis: crítico; alto; médio; baixo.
5.21	Deve prover relatórios de inteligência de ameaças avançadas mais recentes e indicadores de comprometimento para ajudar sua organização a se defender proativamente contra ameaças.
5.22	Deve integrar relatórios de inteligência criados por especialistas em ameaças do fabricante e terceiros para ajudar na identificação de ameaças.
5.23	Os relatórios de ameaças do fabricante deverão gerar alertas de detecção caso sejam identificadas atividades presentes nos relatórios dentro do ambiente.
5.24	Deve ser possível identificar individualmente cada relatório de ameaça.
5.25	Deve permitir adicionar bases de inteligência terceiras de forma manual, por API, importando arquivos com base CSV ou STIX através de assinatura de feeds de inteligência de ameaças terceiros.
5.26	Deve ser possível realizar buscas através de *strings* parciais, exatas, valores nulos, *wildcards* e caracteres especiais.
5.27	O campo de busca deve permitir o uso de múltiplos operadores lógicos para no mínimo: E; Ou; Não.
5.30	Deve permitir indexar múltiplas buscas utilizando operadores lógicos.
5.31	Deve permitir salvar pesquisas com os critérios de busca e operadores lógicos utilizados para futuras consultas.
5.32	Deve permitir pesquisar por atividades de cada um dos contextos, mesmo que não tenham gerado qualquer tipo de detecção pelos modelos de detecção de ameaça.
5.33	Deve permitir investigar os alertas gerados pelos modelos de detecção por meio de uma análise impacto e análise de causa raiz.
5.34	Deve consolidar e correlacionar diferentes modelos de ameaça relacionados a um único evento.
5.35	Deve somar as pontuações (*score*) de cada modelo durante a correlação das atividades para melhor categorização do incidente.
5.36	Deve exibir todos os detalhes do incidente em uma única página, contendo no mínimo: • Status do incidente; • Score; • Quantidade de contas de e-mail impactadas; • Data e hora da detecção; • Técnica do MITRE utilizada; • Modelo(s) de detecção acionado(s); • Objetos detectados dentro de cada modelo; • Deve permitir alterar o status de cada evento, para no mínimo Novo, Em progresso/análise e Fechado ou escala equivalente.
5.37	Permitir adicionar comentários e notas a cada evento pelos analistas da ferramenta.
5.38	Durante o processo de análise da cadeia de processos deve ser possível verificar todos os objetos relacionados à esta análise, as atividades executadas pelos objetos e sua reputação conforme categorização do fabricante.
5.39	Deve ser possível interagir com cada um dos objetos relacionados ao evento para análise avançada e resposta.
5.40	Deve destacar e organizar as atividades relacionadas a cada modelo de detecção por ordem cronológica, permitindo identificar a relação de cada atividade com os modelos de detecção.
5.41	Permitir adicionar um comentário junto a cada ação tomada para registro e contextualização das ações.
5.42	Deve permitir remover arquivos SHA-1, URLs, IPs ou domínios a lista de bloqueio dos sensores.
5.43	Permitir coletar e fazer o download de um arquivo para investigação local detalhada.

5.44	Permitir adicionar o remetente (*sender*) de um e-mail na lista de bloqueio, impedindo o mesmo de enviar novos e-mails os usuários da sua empresa.
5.45	Mover o e-mail selecionado para a área de quarentena de um específico usuário ou todos os usuários que contenham este e-mail em suas caixas.
5.46	Deletar o e-mail selecionado das caixas selecionadas.
5.47	Deve permitir verificar todas as ações de respostas executadas no console ou por API.
5.48	Deve exibir os seguintes painéis de controle: • Índice de risco da empresa; • MITRE ATT&CK® Mapping for Enterprise; • Visão geral de alertas; • Top 10 vulnerabilidades em risco; • Top 10 usuários em risco; • Top 10 dispositivos em risco;
5.49	Deve permitir a geração e o download de relatórios únicos e/ou agendados.
5.50	Deve possuir a capacidade de sugerir termos de busca, de acordo com o conteúdo já buscado numa investigação, para agilizar a obtenção do resultado.
5.51	Deve permitir exportar sob demanda os logs em texto puro (CSV ou PDF).
5.52	Deve permitir investigação por palavras-chave customizadas para facilitar a busca de eventos.
5.53	Deve permitir recebimento e encaminhamento de logs via syslog.
5.54	Deve permitir receber logs de diferentes dispositivos.
6	**Proteção Host IPS e Host Firewall**
6.1	Deve ser capaz de realizar a proteção a códigos maliciosos nos seguintes sistemas operacionais e superiores: • Microsoft Windows 8; • CentOS 7; • Windows Server 2008; • Ubuntu 18; • Red Hat Enterprise Linux Server.
6.2	Deve possuir módulo para proteção de vulnerabilidades com as funcionalidades de host IPS e host firewall.
6.3	O módulo deve ser integrado como solução do *endpoint* e ser gerenciado pelo mesmo console, sem que haja custo de licença adicional.
6.4	Todas as regras das funcionalidades de *firewall* e IPS de host devem permitir apenas detecção (log) ou prevenção (bloqueio).
6.5	Deve permitir ativar e desativar o produto sem a necessidade de remoção.
6.6	Deve possuir capacidade de identificar e bloquear, no mínimo, os seguintes tipos de ataques: • *Denial of Service* (DOS); • *Port scanning;* • *Network Flooding*.
6.7	Deve permitir a emissão de alertas via SMTP e SNMP.
7	**Controle de aplicações de *endpoints***
7.1	Deve ser capaz de realizar a proteção a códigos maliciosos nos seguintes sistemas operacionais e superiores:

	• Microsoft Windows 8; • CentOS 7; • Windows Server 2008; • Ubuntu 18; • Red Hat Enterprise Linux Server.
7.2	O módulo deve ser integrado como solução do *endpoint* e ser gerenciado pelo mesmo console, sem que haja custo de licença adicional.
7.3	Deve permitir a criação de políticas de segurança personalizadas.
7.4	As políticas de segurança devem permitir a seleção dos alvos baseados nos seguintes critérios: • Nome parcial ou completo das estações de trabalho, permitindo a utilização de caractere coringa para identificação do nome parcial da máquina; • Range de endereços IPS; • Sistema operacional; • Grupos de máquinas espelhados do Active Directory e LDAP; • Usuários ou grupos do Active Directory e LDAP.
7.5	As políticas de segurança devem permitir a combinação lógica dos critérios para identificação do(s) alvo(s) de cada política.
7.6	As políticas de segurança devem permitir o controle do intervalo de envio dos logs.
7.7	As políticas de segurança devem permitir o controle do intervalo para envio de atualização de cada política.
7.8	As políticas de segurança devem permitir a definição de qual servidor de gerenciamento o agente de segurança deve comunicar-se.
7.9	As políticas de segurança devem permitir a ocultação do ícone do agente, que reside da barra de tarefas, e de notificações ao usuário.
7.10	As políticas de segurança devem permitir o controle através de regras de aplicação.
7.11	As regras de controle de aplicação devem permitir as seguintes ações: • Permissão de execução; • Bloqueio de execução; • Bloqueio de novas instalações.
7.12	As regras de controle de aplicação devem permitir o modo de apenas coleta de eventos (logs), sem a efetivação da ação regra.
8	**Proteção contra vazamento de informações (DLP) de *Endpoints***
8.1	Deve ser capaz de realizar a proteção contra vazamento de informações nos seguintes sistemas operacionais e versões superiores: • Microsoft Windows 8; • CentOS 7; • Windows Server 2008; • Ubuntu 18; • Red Hat Enterprise Linux Server.
8.2	O módulo deve ser integrado como solução do *endpoint* e ser gerenciado pelo mesmo console, sem que haja custo de licença adicional.
8.3	Deve possuir nativamente *templates* para atender as seguintes regulamentações: • LGPD (Lei nº 13.709/2018);

	• Lei do Sigilo Bancário (Lei Complementar nº 105/2001); • Lei do Prontuário Eletrônico (Lei nº 13.787/2018); • Marco Civil da Internet (Lei nº 12.965/2014); • Código de Defesa do Consumidor (Lei nº 8.078/1990).
8.4	Deve ser capaz de detectar informações, em documentos nos formatos: • Documentos: Microsoft office (doc, docx, xls, xlsx, ppt, pptx) openoffice, rtf, wordpad, text; xml, html; • Gráficos: visio, postscript, pdf, tiff; • Comprimidos: win zip, rar, tar, jar, arj, 7z, rpm, cpio, gzip, bzip2, unix/linux zip, lzh; • Códigos: c/c++, java, verilog, autocad.
8.5	Deve ser capaz de detectar informações, com base em: • Dados estruturados, como dados de cartão de crédito, dados pessoais, endereços de e-mail, CPF, entre outros, através de palavras ou frases exatas, padrão de documentos conhecidos e formato pré-definido de identificação de dados; • Dados não-estruturados, como documentos exportados, reformatados ou sem estrutura de dados definida, através de expressões regulares ou descoberta de dados por aprendizado de padrões e criação de *fingerprinting*.
8.6	Deve ser capaz de detectar em arquivos compactados.
8.7	Deve permitir a configuração de quantas camadas de compressão serão verificadas.
8.8	Deve permitir a criação de modelos personalizados para identificação de informações.
8.9	Deve permitir a criação de modelos com base em regras e operadores lógicos.
8.10	Deve possuir modelos padrões.
8.11	Deve permitir a importação e exportação de modelos.
8.12	Deve permitir a criação de políticas personalizadas.
8.13	Deve permitir a criação de políticas baseadas em múltiplos modelos.
8.14	Deve permitir mais de uma ação para cada política, como: • Apenas registrar o evento da violação; • Bloquear a transmissão; • Gerar alertar para o usuário; • Gerar alertar na central de gerenciamento; • Capturar informação para uma possível investigação da violação.
8.15	Deve permitir criar regras distintas com base se a estação está fora ou dentro da rede.
9	**MacOS**
9.1	Deve ser compatível com as seguintes versões do MacOS 10.13 e subsequentes.
9.2	Deve trabalhar de forma híbrida, fazendo uso de assinaturas, *machine learning* e detecção de comportamento para identificar *malwares* no *endpoint*.
9.3	Deve possuir uma regra pré-definida para análise de *malware* consultando extensões comumente utilizadas para otimizar o uso de recurso do *endpoint.*
9.4	A solução deve possuir uma regra pré-definida para análise de *malware* consultando somente arquivos Mach-O ou permitir ler todos os arquivos.
9.5	Deve permitir scanear compartilhamentos de rede, arquivos comprimidos e *Time Machine*.
9.6	Em caso de detecção a solução deve tomar uma das seguintes ações:

	• Liberar acesso; • Quarentenar; • Limpar; • Deletar.
9.7	Deve permitir colocar programa, extensões ou arquivos em exclusão para evitar falso positivos e otimizar o uso de recurso.
9.8	Deve possuir a função *Scan Cache*, otimizando o *scan* nas máquinas, armazenando informações dos arquivos que já são conhecidos como bons.
9.9	Deve possuir módulo de proteção contra alteração dos arquivos.
9.10	Deve ser capaz de liberar ou bloquear os seguintes dispositivos: • CD/DVD; • Compartilhamentos de rede; • SD card; • Dispositivos *thunderbolt* de armazenamento; • Dispositivos de armazenamento USB; • Deve ser possível adicionar dispositivos de armazenamento USB a lista de dispositivos permitidos utilizando nome do fabricante, ID do dispositivo e número de serial.
9.11	Deve ser possível configurar ao menos as seguintes ações: • Acesso total; • Somente leitura; • Bloqueio.

Solução de segurança para e-mails (*antispam*)	
ID	**DESCRIÇÃO**
1.1	A solução deverá atender, no mínimo, os serviços abaixo: • Disponibilidade do serviço; • Proteção contra vírus; • Efetividade no bloqueio de SPAM; • Ocorrência de falsos-positivos; • Latência máxima na entrega de mensagens.
1.2	Deve ser compatível com Zimbra e Microsoft 365.
2	**Características gerais da solução**
2.1	A solução deverá possuir *Single Sign-On* para acessar o console de administração.
2.2	A solução deverá permitir a criação de regras para entrada (*inbound*) e saída (*outbound*) de e-mails.
2.3	A solução deverá possuir console de gerenciamento web.
2.4	A solução deverá possuir console centralizada, incluindo: • Configurações de administração; • Objetos de política; • Objetos suspeitos; • Gerenciamento de usuário final; • Gerenciamento de diretório; • Informações sobre licenciamento;

	• Logs; • Relatórios; • Visualização de mensagens quarentenadas; • Gerenciamento de domínio; • *Dashboard* baseado em gráficos; • Rastreamento de e-mails, eventos e logs.
2.5	A solução deverá possuir *dashboards* possibilitando no mínimo a visualização de ameaças, *ransomwares*, detalhes de autenticação baseada em domínio, *sandbox*, BEC, SPAM, principais violações, eventos de DLP, consumo de banda, proteção *time-of-click*.
2.6	A solução deverá possuir configurações de *dashboard* sendo possível selecionar: • Direção do tráfego: entrada e saída de e-mails (*inbound/outbound*); • Período: data, semana e mês.
2.7	A solução deve suportar sistema ARC (*Authenticated Received Chain*), preservando os resultados da autenticação de e-mail.
2.8	A solução deve ser capaz de remover conteúdos ativos encontrados em documentos anexos como Microsoft Word, Excel e PowerPoint. Se caso o conteúdo ativo não puder ser removido, deve possuir a opção de excluir o anexo que contém o conteúdo ativo.
2.9	A solução deve possuir a funcionalidade de validação de DNS reverso do remetente, tendo a capacidade de criar listas de domínios PTR (Pointer Record) que serão bloqueados; (*New Feature Available on March* 28, 2022).
2.10	A solução deverá ser capaz de permitir a filtragem baseada em reputação IP para no mínimo: • Remetentes permitidos com base no endereço IP e país; • Remetentes bloqueados com base no endereço IP, país e região.
2.11	A solução deverá ser capaz de permitir a filtragem de remetente e destinatários para no mínimo: remetentes aprovados por endereço de e-mail ou domínio, remetentes bloqueados por endereço de e-mail ou domínio.
2.12	A solução deverá possibilitar incluir X-Header no cabeçalho da mensagem para mensagens de e-mail correspondentes a remetentes aprovados.
2.13	A lista de remetentes aprovados e remetentes bloqueados deverão exibir no mínimo as seguintes informações: • Remetente; • Domínio do destinatário; • Data.
2.14	Deverá possuir correspondência de IP do remetente, possibilitando especificar um IP ou um intervalo de endereços IP em um domínio do remetente identificado pelo endereço do cabeçalho da mensagem para permitir mensagens de e-mail apenas desses endereços.
2.15	Deverá detectar *malwares*, *worms*, e outras ameaças baseadas em assinatura e padrões.
2.16	Deverá ser capaz de detectar *spam* baseado em assinatura e padrões.
2.17	Deverá identificar e-mails marketing como redes sociais, fóruns e boletins de informações.
2.18	Deverá permitir criar exceções para e-mails marketing.
2.19	A configuração de spam deverá possuir no mínimo três níveis: baixo, meio e alto.
2.20	Deverá detectar ataques de comprometimento de e-mail.
2.21	Deverá possuir detectar *phishing* e conteúdos suspeitos.

2.22	Deverá detectar mensagens de *graymail.*
2.23	Deverá realizar varreduras em arquivos JSE e VBE para identificar ameaças de macro.
2.24	Deverá detectar ameaças desconhecidas utilizando *machine learning.*
2.25	Deverá permitir visualizar relatório detalhado para cada detecção *machine learning.*
2.26	Deverá possuir *engine* própria para detecção de explorações de documentos, ameaças de dia zero, vulnerabilidades conhecidas e outras ameaças usadas em ataques direcionados.
2.27	Deverá possuir proteção *anti-ransomware*.
2.28	Deverá possuir análise de URLs no corpo do e-mail.
2.29	Deverá possuir o recurso para analisar as URLs no momento do clique do usuário e as bloquear se forem maliciosas.
2.30	Deve possuir ações de bloqueio, liberação e alerta para as seguintes categorias ou equivalentes: perigoso, altamente suspeito, não testado e suspeito.
2.31	Deverá possuir proteção contra comprometimento de e-mail.
2.32	Deverá permitir adicionar usuários de alto perfil, possibilitando exportar a lista em CSV.
2.33	Deverá possibilitar importar usuários de alto perfil através de arquivo CSV.
2.34	Deverá fornecer informações detalhadas bem como razões para mensagens de e-mail detectadas como possíveis ataques analisados ou prováveis do *Business e-mail Compromise* (BEC).
2.35	Deverá possuir proteção contra-ataques de engenharia social.
2.36	Deverá fornecer informações detalhadas bem como razões para mensagens de e-mail detectadas como possíveis ataques de engenharia social.
2.37	Deverá ser capaz utilizar no mínimo os seguintes bancos de dados de reputação que: • Tenham uma lista de endereços IP de servidores de correio que são conhecidos por serem fontes de *spam*; • Tenham uma lista de endereços IP identificados como envolvidos em *ransomware* ativos, *malware* ou outras campanhas de ameaças por e-mail; • Tenham uma lista de IPs atribuídos dinamicamente.
2.38	Deverá possibilitar configurar diferentes tipos de exceções de varredura em um e-mail através de definições de condições e possibilitando executar as ações ou equivalentes de *bypass*, deleção do e-mail incluindo anexos e quarentenar ~~quando:~~ • ~~O número de arquivos em um arquivo compactado excede 350MB;~~ • ~~A taxa de descompactação de um arquivo compactado excede 90MB;~~ • ~~O número de camadas de descompactação em um arquivo compactado excede 20MB;~~ • ~~O tamanho de um único arquivo descompactado excede 60MB;~~ • ~~Um arquivo do Office contém mais de 350 subarquivos.~~
2.39	As ações de verificação configuradas para cada exceção deverão ser aplicadas a todos os remetentes e destinatários.
2.40	Deverá possibilitar incluir *tag*.
2.41	Deverá possuir regras de varredura avançadas que permitam especificar as condições que a regra se aplica às mensagens verificadas pela solução.
2.42	Deverá possuir as seguintes condições: • Tamanho da mensagem; • Assunto; • Corpo do e-mail; • Cabeçalho;

	• Conteúdo do anexo; • Nome e/ou Extensão: ◦ .386, .ACM,.ASP,.AVP, .BAT,.CGI, .CHM,.CLA,.CLASS,.CMD, .CNV, .COM, .CS, .DLL, .DRV, .EXE, .HLP, .HTA, .HTM, .JS*, .LNK, .OCX, .OPO, .PHP, .PL. .SH, .SYS, .VBS, VBE, VXD, .WBS, .WIZ. WSH, .DOC, .DOCM, DOCX, .DOT, .DOTM, .DOTX, .DVB, .EML, .MD*, .PPA, .PPAM, .PPS, .PPSM, .PPSX, .PPT, .PPTM, .PPTX, XL,XLA, XLAM, .XLC, .XLK, XLL,.XLM, .XLR, .XLS, .XLSB, .XLSM, XLSX, .XLT, .XLTM, XLTX; MIME. • Content-type: vídeo, áudio, imagens, documentos e outros; • Tamanho do anexo; • Anexo protegido por senha: .7z, .ace, .arj, .docx, .pptx, .rar, .xlsx, .zip; • Quantidade de anexos; • Número de destinatários.
2.43	Deverá possuir ações através das regras permitindo definir o que acontecerá com as mensagens que atendem às condições dos critérios da regra: • Criptografar mensagem de e-mail; • Monitorar, permitindo os administradores o monitoramento das mensagens. As ações de monitoramento incluem o envio de uma mensagem de notificação para outras pessoas ou o envio de um cópia oculta (Cco) da mensagem para outras pessoas; • Bloqueio, deverá interceptar a mensagem, impedindo que ela atinja o destinatário original. As ações de bloqueio incluem excluir a mensagem inteira, colocar em quarentena e enviar para um destinatário diferente; • Modificar, permitindo alterar a mensagem e/ou seus anexos. As ações de modificação incluem limpeza de vírus que podem ser limpos, exclusão de anexos de mensagens, inserção de um carimbo no corpo da mensagem ou TAG de assunto.
2.44	Deverá possibilitar selecionar de todas as correspondências ou equivalentes para acionar a regra somente quando todos os critérios configurados selecionados fizerem correspondência.
2.45	Deverá possibilitar selecionar de qualquer correspondências ou equivalentes para acionar a regra quando qualquer critério configurado fizerem correspondência.
2.46	Deve ser possível criar políticas de *malwares*, *spam* e filtragem de conteúdo com: • Definição do destinatário, possibilitando selecionar domínios cadastrados, domínios específicos e grupos de usuários; • Especificação de endereços de remetente; • Exceções.
2.47	A solução deverá possibilitar importar e exportar os destinatários, remetentes e listas de exceções.
2.48	Deve ser possível criar políticas que executem ações em mensagens que contêm *malware*, *worms* ou outros códigos maliciosos.
2.49	Deve ser possível realizar a limpeza de *malwares* ou códigos maliciosos, onde o *malware* pode ser removido com segurança do conteúdo do arquivo infectado, resultando em uma cópia não infectada da mensagem ou anexo original.
2.50	Deverá possuir o serviço de banner para customização do portal com a logo.
2.51	Deverá possuir integração com o Active Directory ou com LDAP.
2.52	Deverá permitir o gerenciamento de múltiplos domínios.
2.53	Deverá permitir a integração com Microsoft Office 365, Google G-Suite, Zimbra e outros servidores de e-mail.
2.54	O uso das REST APIs deve permitir executar operações para no mínimo: criação, leitura, atualização e exclusão.

3	**Criptografia de e-mail**
3.1	Deverá ser capaz de criptografar e-mails baseado em políticas.
3.2	Deverá assegurar a comunicação através da utilização do protocolo TLS.
3.3	Deverá permitir a configuração da checagem do TLS.
3.4	Deverá suportar: TLS 1.0 e subsequentes.
4	**Rastreamento de e-mail e auditoria**
4.1	Deve permitir o rastreamento de mensagens de forma centralizada e por meio da interface de gerenciamento, não sendo aceito pesquisa via linha de comando.
4.2	Deverá possuir permitir o rastreamento de mensagens enviadas e recebidas.
4.3	Deverá possibilitar pesquisas de log de rastreamento de e-mail por até 30 dias.
4.4	Deverá fornecer buscas para rastreamento de e-mail por: período, direção do tráfego, remetente, destinatário, tipo (bloqueado/liberado), ação, assunto, ID da mensagem e *hash* do anexo SHA256.
4.5	Deverá possibilitar exportar a busca no formato .CSV.
4.6	Deverá permitir a consulta de eventos com os logs das políticas aplicadas por até 30 dias.
4.7	Deverá fornecer consulta de eventos com os logs das políticas por: período, direção do tráfego, remetente, destinatário, nome da regra, tipo de ameaça, anexo, BEC, conteúdo, DLP, *Graymail, ransomware, phishing, spam*, *malware, web reputation*, ID da mensagem e ação.
4.8	Deverá permitir rastrear os cliques de URL por até 30 dias.
4.9	Deverá fornecer permitir rastrear os cliques de URL por: data, direção do tráfego, remetente, destinatário, ID da mensagem, URL, ação e a hora em que um URL foi clicada.
4.10	Deverá ser possível consultar os logs de auditoria da console da solução por até 30 dias.
4.11	Deverá ser possível encaminhar os logs para *syslog*.
5	**Relatórios**
5.1	Deverá fornecer relatórios com base em uma programação diária, semanal, mensal e trimestral.
5.2	Os relatórios deverão ser, pelo menos, no formato PDF.
5.3	Deverá ser possível criar relatórios agendados e manuais.
5.4	Deverá possibilitar obter relatório sobre com resumo do tráfego de e-mail de todos os domínios e por domínio, detecções de ameaças, detecções de arquivos da *sandbox*, detecções de URL da *sandbox* e os principais destinatários comprometidos por e-mail (BEC).
6	**Notificações**
6.1	Deverá suportar notificação via e-mail.
6.2	Deverá possuir modelos de notificação pré-definidas para violação de políticas.
6.3	Deverá notificar quando o e-mail possuir um anexo compactado.
6.4	Deverá notificar quando o tamanho da mensagem excedido.
6.5	Deverá notificar quando uma regra for desencadeada.
6.6	Deverá notificar quando houver uma configuração de violação de segurança.
6.7	Deverá notificar quando um vírus ou spam for identificado.
7	**Prevenção contra vazamento de dados**
7.1	Deverá permitir gerenciar as mensagens de e-mail com dados confidenciais e proteger contra perda de dados, monitorando as mensagens de e-mail de saída.
7.2	Deverá possibilitar criar regras por expressões regulares, palavras chaves e atributos do arquivo.
7.3	Deverá possuir *templates* pré-definidos.
7.4	Deverá possuir *templates* customizados.

7.5	Deverá possuir uma base com no mínimo 200 modelos para criação de regras.
7.6	Deverá permitir a customização de modelos aderência a LGPD.
8	**Da quarentena**
8.1	Deverá permitir visualizar as mensagens quarentenadas por data, direção do tráfego, remetente, destinatários e conteúdo.
8.2	Deverá permitir o gerenciamento da quarentena para múltiplos domínios.
8.3	Deverá permitir a customização da notificação de quarentena pelo menos semanalmente, uma vez ou mais vezes durante o dia.
8.4	A notificação de quarentena deverá permitir a customização.
8.5	A notificação de quarentena deverá ser, no mínimo, em inglês e português.
8.6	A solução deverá possibilitar a gestão de quarentena de forma que seja possível que o administrador possa visualizar: a razão de um determinado bloqueio, o remetente, o destinatário, a data, o assunto, o IP do host de destino, a mensagem original, o tamanho da mensagem original.
8.7	Com base nos requisitos acima, deve ainda permitir as ações liberar e/ou excluir a mensagem.
8.8	A solução deverá permitir realizar o download da mensagem quarentenada.
8.9	Caso uma mensagem seja bloqueada ou rejeitada, a solução deverá informar também a razão do bloqueio e quais as regras foram ativadas.
8.10	Deverá possuir *single sign-on* (SSO) para a quarentena de usuário.
8.11	Deverá possibilitar utilizar duplo fator de autenticação.
8.12	Deverá possibilitar que usuário tome as seguintes ações ou similar em sua própria quarentena: • Excluir e bloquear o remetente: possibilitando excluir permanentemente a mensagem e adicionar o endereço aos remetentes bloqueados; • Excluir, possibilitando excluir permanentemente a mensagem; • Entregar e aprovar o remetente, permitindo liberar a mensagem da quarentena e adicionar o endereço aos remetentes aprovados, para que mensagens futuras de remetentes aprovados não sejam mantidas em quarentena; • Entregar, permitindo assim liberar a mensagem da quarentena.
8.13	Deverá possibilitar que o usuário criar listas remetentes aprovados e remetentes bloqueados.

Solução de segurança para ambiente de colaboração	
ID	**DESCRIÇÃO**
1	A solução deve permitir a identificação e proteção contra ameaças no Microsoft Office 365 (Exchange Online, Sharepoint Online, Onedrive for Business e Microsoft Teams), Gsuite e Zimbra.
2	Identificar e bloquear arquivos maliciosos carregados para o Google Drive, Onedrive, Zimbra, Sharepoint e Microsoft Teams. Por exemplo, se um usuário tentar carregar um determinado arquivo malicioso ou proibido em uma das plataformas citadas, a solução deve fazer o bloqueio.
3	Bloquear upload de arquivos por tipo definido em política para as soluções supracitadas.
4	Identificar e bloquear URLs maliciosas em arquivos e URLs, incluindo URLs dentro de anexos.
5	Realizar escaneamentos de ameaças em tempo real nos serviços integrados, identificando componentes maliciosos.
6	Permitir realizar escaneamento retroativo de ameaças (sob demanda), isto é, em busca de ameaças já armazenadas nas caixas de e-mail dos usuários ou em diretórios do Google Drive, Onedrive e Sharepoint.

7	O nível de sensibilidade das URLs maliciosas deve ser configurável através de políticas.
8	Deve possuir capacidade de cadastro dos usuários importantes para focar a análise de ataques de Comprometimento de E-mail (BEC).
9	Deve permitir que os administradores configurem a periodicidade das notificações para, no mínimo, URLs maliciosas identificadas, SPAMs maliciosos, *phishing*, *ransomware*, arquivos analisados na *sandbox* e identificados como baixo, médio e alto risco.
10	Identificar tentativas de comprometimento de e-mail baseado em uma análise dos estilos de escrita de cada usuário cadastrado como importante.
11	Deve permitir a visualização das estatísticas no dashboard por serviço integrado (Gmail, Google Drive, Exchange Online, Zimbra, Teams, Onedrive, Sharepoint) e alterar o período dos logs para, no mínimo, 24 horas, 7 dias e 30 dias.
12	Deve permitir a exibição da tendência para cada um dos tipos de serviço integrado em relação ao mesmo período anterior. Por exemplo, exibir aumento ou redução das ameaças no Exchange Online ou Zimbra nos últimos 30 dias, comparando com os 30 dias anteriores.
13	Deve ter a capacidade de analisar arquivos e URLs em *sandbox* para identificação de ameaças desconhecidas (sem assinatura).
14	Deve utilizar mecanismos de proteção que contemplem, pelo menos, malwares conhecidos por assinatura, malwares desconhecidos por *Machine Learning*, bloqueio de conteúdo (por tipo de arquivo, por exemplo), reputação de URLs.
15	A solução deve permitir compartilhamento de informações através de SIEM via API ou através da gerência centralizada.
16	A solução deve prover relatórios que contemplem, pelo menos, riscos de segurança (ameaças), *ransomware*, arquivos analisados em *sandbox*, auditoria e sobre a API.
17	Os relatórios devem ser exportáveis para, pelo menos, PDF.
18	Os relatórios devem ser enviados por e-mail, mediante configuração do administrador.
19	A verificação *anti-malware* deverá permitir a customização das ações a serem tomadas, por exemplo: quarentenar, deletar e passar.
20	Realizar integração nuvem-a-nuvem, através de API da Microsoft e Google.
21	As ações configuráveis nas políticas do serviço de e-mail devem contemplar, no mínimo, etiquetar a mensagem (inserir *tag*), quarentenar, deletar, ignorar e mover para lixeira.
22	Os demais serviços devem possuir ações pré-definidas e configuráveis para eliminar, quarentenar e ignorar os arquivos identificados.
23	Deve empregar o uso de análise em ambiente virtual (sandbox) do próprio fabricante para detecção de malwares avançados, com objetivo de diminuir seu risco de violação.
24	As políticas deverão ser aplicáveis por usuário ou grupo sincronizado da estrutura de serviço online (Microsoft ou Google).
25	Possuir um dashboard com as principais ameaças detectadas, a exemplo dos tipos *ransomware*, *phishing*, comprometimento de e-mail.
26	Deverá ser capaz de implementar políticas com base no filtro de conteúdo das mensagens.
27	Deverá ter a capacidade de compartilhar objetos suspeitos identificados através da análise em *sandbox* com a gerência centralizada do fabricante.
28	Cada política de serviço deve ser configurável para apenas monitorar ou tomar ação de proteção.
29	As notificações enviadas para o administrador e para os usuários devem ser customizáveis, permitindo tradução, inclusão ou exclusão de campos.
30	Deverá permitir a configuração dos níveis de detecção para SPAM.

31	Deverá permitir o administrador criar exceções para permitir ou bloquear determinados endereços de e-mail e URLs manualmente.
32	A solução deve possuir capacidade de ignorar e-mails já enviados para a lixeira do serviço de e-mail.
33	Deve permitir ao administrador bloquear mensagens de *graymail* por tipo (mensagens de marketing, notificações de fóruns e redes sociais, etc).
34	Os logs devem ser interativos, permitindo ao administrador montar consultas baseadas nos parâmetros como serviço detectado, tipo/categoria da ameaça, usuários afetados, política acionada, nome da ameaça, dentre outros.
35	Os resultados das consultas de logs deverão ter opção de salvar como um relatório exportável.
36	Deve permitir que o administrador realize buscas pontuais nos logs, a partir de parâmetros previamente definidos.
37	Deve possuir áreas de quarentena distintas para cada um dos serviços integrados, permitindo a restauração, download ou exclusão de arquivos/e-mails quarentenados pela política.
38	Deve permitir a criação de exceções para detecções por *Machine Learning* e por *Sandbox*.
39	Deve ter a capacidade de integração com serviços de autenticação para logon único (*single sign-on*) com, pelo menos, Okta, ADFS, Keycloak e Azure AD.
40	Deve possuir capacidade de configuração de contas de administração com permissões granulares por administrador, permitindo visualização ou controle total dos itens de menu.
41	Deve suportar a integração com serviço de gerenciamento de incidentes do próprio fabricante através da plataforma de investigação.
42	O recurso de detecção e resposta para e-mails deverá ser integrado à solução da Microsoft Office 365 ou Zimbra sem a necessidade de alterar configurações dos serviços de e-mail, ou configurações dos usuários.
43	Possuir modelos pré-definidos pelo fabricante de atividades suspeitas e/ou maliciosas para identificação e categorização de ameaças no ambiente.
44	A solução deve ser capaz de associar diferentes modelos de ameaças e associá-los a um único incidente/evento.
45	Deve ter capacidade de apresentar informações relacionadas ao MITRE para cada um dos eventos detectados no ambiente, caso possuam.
46	Utilizar bases de inteligência de ameaças integrando relatórios de inteligência do fabricante e de terceiros para ajudar a identificar ameaças no ambiente.
47	Em caso de ameaça avançada por e-mail, a solução deve permitir tomar diferentes ações de resposta no ambiente, contemplando, no mínimo.
48	Deve permitir adicionar o remetente (*sender*) de um e-mail na lista de bloqueio, impedindo o mesmo de enviar novos e-mails os usuários internos.
49	Deve mover o e-mail selecionado para a área de quarentena de um específico usuário ou todos os usuários que contenham este e-mail em suas caixas.
50	Deve deletar o e-mail selecionado das caixas selecionadas.

Solução de segurança para containers	
ID	**DESCRIÇÃO**
1	**Módulo de proteção contínua e automatizada de imagens de containers no pipeline**

1.1	A solução deverá utilizar sensores para escanear imagens de container localizadas no datacenter *on-premises* e em nuvem.
1.2	A console de gerenciamento deve ter suporte a múltiplo fator de autenticação (MFA).
1.3	Deverá escanear imagens e containers durante a fase de desenvolvimento, no processo *deploy*, após o *deploy* e em tempo de execução.
1.4	Durante a fase de desenvolvimento a solução deve ter a capacidade de identificar vulnerabilidades, códigos maliciosos, chaves privadas e segredos, além de violação de conformidade, antes da imagem ir para a produção.
1.5	Na fase de *deployment* a solução deverá ter a capacidade de controle de admissão baseado em políticas, o qual deverá bloquear imagens que estejam fora do padrão definido pela organização.
1.6	Durante a execução em produção, a solução deverá ser capaz de fazer uma verificação contínua da conformidade e das regras aplicadas na fase de admissão.
1.7	A solução deve detectar tanto ameaças instaladas via gerenciador de pacote quanto aplicações instaladas diretamente.
1.8	Os escaneamentos realizados pelos sensores locais (*on-premises*) devem ser enviados para a plataforma centralizada para fins de reporte e correlação.
1.9	Quando em execução, os containers deverão ser monitorados por ações que violem as regras pré-definidas e mapeadas no framework MITRE ATT&CK, focado em técnicas para containers.
1.10	Em caso de violação da política durante a execução, a solução deverá permitir isolar ou encerrar o *pod* em questão;
1.11	A solução deve ser compatível com soluções de cluster *Kubernetes* em nuvem, incluindo: *Amazon Kubernetes Service* (EKS), *Google Kubernetes Engine* (GKE) e *Azure Kubernetes Service* (AKS);
1.12	Deverá ter compatibilidade com *Kubernetes* 1.14 ou superior (incluindo *OpenShift*).
1.13	As políticas devem ser segmentadas de acordo com a fase de desenvolvimento, contemplando ao menos: desenvolvimento, verificação contínua e tempo de execução.
1.14	Durante a fase de implantação, a solução deve permitir apenas monitorar as atividades dos containers e, caso o administrador deseje, a solução deve permitir realizar bloqueio da ação e isolamento do *pod*, de acordo com a fase;
1.15	A solução deve exibir os eventos que ocorreram nos containers, contemplando ao menos: ação, data/hora, cluster, política e regra que gerou o evento, severidade, nome da imagem do container, nome do *pod*;
1.16	Deve ter a capacidade de criar regras de proteção e *compliance* baseadas nas propriedades do *pod*, da imagem e do container, baseadas resultados do escaneamento da imagem e acesso ao *kubectl*;
1.17	A solução deve permitir criar exceções para as regras.
1.18	As regras de proteção devem incluir, no mínimo: • Containers que executam com permissão de root; • Containers com permissão para escalar privilégios; • Containers que podem escrever em sistemas de arquivos root; • Imagens de container com malware; • Imagens de container com vulnerabilidades.
1.19	A solução para proteção de containers em tempo de execução, deve ser compatível com os seguintes sistemas: • Amazon Linux 2 4.14.x, 5.4.x e 5.10.x; • RHCOS 4.18.x;

	• Ubuntu 4.15.x (generic), 5.4.x (generic, aws, azure e GKE), 5.11.x (generic, azure e aws); • Google Container-Optimized OS (COS) 5.4.x e 5.10.x; • Debian 5.10.x (generic).
2	**Sensor de escaneamento de imagens**
2.1	O sensor deve ser implantado como uma arquitetura de microsserviços.
2.2	Deve ser integrado na esteira de desenvolvimento da organização para analisar imagens de containers antes que elas possam ir para a produção.
2.3	Deve ser compatível com pelo menos as seguintes distribuições: RHEL, CentOS, Oracle Linux, Ubuntu, Debian, Alpine e Amazon Linux (2018 e 2).
2.4	Deve suportar a varredura de imagens do Docker em qualquer registro que suporte a API do Docker Registry V2.
2.5	A integração via registro deve ser compatível com: Docker Trusted Registry (DTR), Google Container Registry (GCR), Amazon Elastic Container Registry (ECR), Azure Container Registry (ACR), VMware Harbor, jFrog Artifactory, Sonatype Nexus e Quay Container Registry.
2.6	O console de gerenciamento do sensor deve oferecer suporte à implantação no Kubernetes 1.10.0 ou superior em uma plataforma certificada Kubernetes (ou equivalente como Red Hat Openshift).
2.7	A solução deve ter na API um recurso de webhook que permita que os componentes de CI / CD se registrem para receber notificações de eventos de verificação, incluindo 'verificação concluída', permitindo automatizar fluxos de trabalho.
2.8	Deve possuir APIs com o detalhamento das funções que podem ser utilizadas para a integração da solução com softwares de terceiros.
2.9	Deve possuir console de gerenciamento local no host, via linha de comando, que inclua a possibilidade de iniciar a varredura de contêiner.
2.10	O sensor deve possuir compatibilidade com banco de dados externo, incluindo PostgreSQL 9.6, Oracle 11 e subsequentes.
2.11	Deve realizar escaneamento de maneira automática no momento do build da imagem e sob demanda.
2.12	Os resultados dos escaneamentos realizados pelos sensores devem ser enviados para console centralizada na nuvem para serem utilizados como objetos para as políticas e regras.
2.13	O sensor deve detectar *malware* e apresentar indicador de existência de *malware*, incluindo nome e localização do arquivo.
2.14	Detectar segredos e chaves incorporados nas imagens.
2.15	Permitir realizar consultas de verificação personalizadas para encontrar arquivos suspeitos ou indesejados.
2.16	Deve analisar o conteúdo da imagem *docker* baseado em uma lista de verificação de conformidade que inclua itens do PCI-DSS, HIPAA e NIST 800-190.
2.17	As vulnerabilidades encontradas em cada varredura devem fornecer no mínimo as gravidades: Baixa, Média e Alta.
2.18	solução deve ter a capacidade de criar regras manuais, além das regras internas fornecidas pela solução, incluindo o formato YARA.
2.19	Identificar vulnerabilidades na aplicação em execução nos serviços de Container em Kubernetes através dos seguintes Cloud Service Providers: Amazon Web Services (EKS), Microsoft Azure (AKS) e Google Cloud Platform (GKS).
2.20	Detalhamento do CVE e o risco de exposição da aplicação da imagem.

2.21	Identificar a imagem com a vulnerabilidade podendo tomar uma ação de bloqueio da mesma.

Solução de segurança para *mobile*	
ID	**DESCRIÇÃO**
1	**Dispositivos móveis iOS**
1.1	Deve ser compatível com os sistemas operacionais iOS 6.x e subsequentes.
2	**Dispositivos móveis Android**
2.1	Deve ser compatível com os sistemas operacionais Android 4 e subsequentes.
3	**Características gerais**
3.1	Deve ter gerenciamento centralizado.
3.2	Deve ter proteção avançada: • contra *malwares*; • contra aplicativos e sites maliciosos; • *phishing;* • vulnerabilidades de Wi-fi; • ataques conhecidos.
3.3	Deve notificar SO desatualizado.
3.4	Deve mapear vulnerabilidades do SO.
3.5	Deve possuir integração com soluções de gerenciamento de dispositivos móveis: • VMWare Workspace One; • Google Workspace Endpoint Management.
3.6	Deve possuir recursos de segurança avançada e capacidades de gerenciamento, tais como: • gerenciamento de risco de superfície de ataque; • Zero Trust Secure Access; • diretor de dispositivos móveis.

Gerenciamento de risco e superfície de ataque	
ID	**DESCRIÇÃO**
1	Deve exibir os 10 principais dispositivos com alto nível de risco na organização
2	Deve exibir os 10 principais usuários com alto nível de risco na organização.
3	Deve categorizar o índice de risco da organização, levando em consideração fatores de risco e indicadores específicos que afetam a rede.
4	Deve exibir as principais vulnerabilidades da organização, com base na pontuação de impacto ou no potencial global de exploração, e os ativos específicos que são afetados
5	Deve exibir o número total de alertas acionados nos últimos 7 dias e o nível de severidade dos modelos que acionaram os alertas.
6	Deve exibir os 20 principais *endpoints* que registraram mais detecções de filtro nos últimos 7 dias.

7	Deve proporcionar visibilidade completa de todos os ativos da organização, incluindo identidades, dispositivos, aplicações, APIs, dados e *shadow IT.*
8	Deve correlacionar a criticidade dos ativos, severidade de vulnerabilidades e atividade de ameaças para fornecer uma gestão de riscos baseada em contexto, dinâmicas e em tempo real.
9	Deve utilizar tecnologias de Inteligência Artificial e Machine Learning para automatizar respostas a ameaças.
10	Deve se integrar em ambientes de nuvem.
11	Deve permitir prever, visualizar e evitar explorações potenciais para prevenção de ataques.

Referência: Processo nº 01300.005789/2023-78 SEI nº 2193715

Documento assinado eletronicamente por **EMERSON DA MOTTA WILLER**, **Fiscal Requisitante do Contrato**, em 30/10/2024, às 18:49, conforme o art. 6º do Decreto nº 8.539, de 08 de outubro de 2015.

Documento assinado eletronicamente por **PAULO RODRIGUES DA COSTA**, **Integrante técnico da contratação**, em 31/10/2024, às 09:19, conforme o art. 6º do Decreto nº 8.539, de 08 de outubro de 2015.

Documento assinado eletronicamente por **CICERO MANOEL VERISSIMO GOMES**, **Integrante Administrativo**, em 31/10/2024, às 15:02, 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 **2193715** e o código CRC **06EBB309**.

CONSELHO NACIONAL DE DESENVOLVIMENTO CIENTÍFICO E TECNOLÓGICO

COORDENAÇÃO DE PROJETOS E DESENHO DE SERVIÇOS DE TECNOLOGIA DA INFORMAÇÃO - COPDS/CGETI/DASD

ANEXO VIII

MODELO DA PLANILHA DE CUSTOS E FORMAÇÃO DE PREÇOS

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.
1.2. 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.
1.3. Para cada item a ser licitado, deve-se entregar a planilha de custos e formação de preços modelada na tabela 1 deste anexo.
1.4. 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 (%)**
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**

2. COMPONENTES DE CUSTOS QUE INTEGRAM A PLANILHA

2.1. 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).
2.2. 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).
2.3. 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).
2.4. 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).
2.5. 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).
2.6. 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).
2.7. 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).
2.8. 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).
2.9. 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 01300.005789/2023-78 SEI nº 2151557

Documento assinado eletronicamente por **EMERSON DA MOTTA WILLER**, **Integrante requisitante da contratação**, em 13/09/2024, às 16:52, conforme o art. 6º do Decreto nº 8.539, de 08 de outubro de 2015.

Documento assinado eletronicamente por **PAULO RODRIGUES DA COSTA**, **Assistente em Ciência e Tecnologia**, em 13/09/2024, às 19:07, 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 **2151557** e o código CRC **F9DDD455**.

CONSELHO NACIONAL DE DESENVOLVIMENTO CIENTÍFICO E TECNOLÓGICO
Setor de Autarquias Sul (SAUS), Quadra 01, Lote 06, Bloco H - Bairro Asa Sul - CEP 70070-010 - Brasília - DF - www.gov.br/cnpq
Edifício Telemundi II

ESTUDOS PRELIMINARES DA CONTRATAÇÃO

INTRODUÇÃO
O Estudo Técnico Preliminar – ETP é o documento constitutivo da primeira etapa do planejamento de uma contratação, que caracteriza o interesse público envolvido e a sua melhor solução. Ele serve de base ao Termo de Referência a ser elaborado, caso se conclua pela viabilidade da contratação. O ETP tem por objetivo identificar e analisar os cenários para o atendimento de demanda registrada no Documento de Formalização da Demanda – DFD, bem como demonstrar a viabilidade técnica e econômica das soluções identificadas, fornecendo as informações necessárias para subsidiar a tomada de decisão e o prosseguimento do respectivo processo de contratação. **Referência: Inciso XI, do art. 2º e art. 11 da IN SGD/ME n.º 94/2022.**

1. INFORMAÇÕES BÁSICAS

Número do processo: 01300.005789/2023-78.

2. DESCRIÇÃO DA NECESSIDADE

Solução de segurança de *endpoints,* servidores de rede, ambiente de colaboração, *mobile,* ambiente de *containers, antispam* e gerenciamento de superfície de ataques.

2.1. MOTIVAÇÃO/JUSTIFICATIVA

O avanço acelerado da digitalização e da internet ampliou significativamente as vulnerabilidades e criou novas formas de ataques cibernéticos. Nesse cenário, é fundamental adotar soluções robustas de segurança para proteger ativos de TI e garantir a integridade, confidencialidade e disponibilidade dos dados.

Dados do Centro de Estudos, Resposta e Tratamento de Incidentes e Segurança no Brasil - CERT.br 2023 (*https://stats.cert.br/incidentes/*) apontam um aumento de 19% nos ataques a servidores web, destacando a necessidade de medidas de segurança proativas. Com o crescimento de ameaças como *ransomware*, SQL Injection e malwares, a proteção do ambiente de TI do CNPq, que presta serviços críticos à comunidade científica e à sociedade, deve ser aprimorada. Além disso, a Lei Geral de Proteção de Dados (LGPD) exige a adoção de soluções que garantam a segurança e privacidade dos dados, o que reforça a necessidade de atualizar a infraestrutura de cibersegurança da instituição.

O TCU, por meio do TC001.873/2020-2 (*https://portal.tcu.gov.br/imprensa/noticias/avaliacao-do-tcu-aponta-que-ataques-ciberneticos-merecem-atencao- governamental.htm - Rel. Min. Vital do Rêgo*) que culminou com o Acórdão 4.035 / 2020 – TCU - Plenário (*https://pesquisa.apps.tcu.gov.br/#/documento/acordao-completo/187320202.PROC/%2520/DTRELEVANCIA%2520desc%252C%2520NUMACORDAOINT%2520desc/0/%2520?uuid=e052e8c0-3e39-11eb-a2e2-479b45fdaccf*), também destaca a importância da implementação de controles críticos de segurança cibernética, conforme o framework do Center for Internet Security (CIS). O controle de defesa contra *malwares*, por exemplo, recomenda a utilização de ferramentas centralizadas que previnam, detectem e respondam rapidamente a ameaças em toda a infraestrutura de TI, incluindo *endpoints*, servidores, redes e ambientes de colaboração.

O controle 10 do CIS v8 - Defesas contra *malwares* - reforça a necessidade de se controlar ou impedir a instalação, disseminação e execução de aplicações, códigos ou scripts maliciosos em ativos corporativos prevenindo, detectando e corrigindo os pontos fracos de segurança antes que possam afetar, no caso, o CNPq. Por essa razão, a proteção eficaz contra *malware* inclui conjuntos tradicionais de prevenção e detecção de *malware* de *endpoint*. Essas ferramentas são mais bem gerenciadas de forma centralizada para fornecer consistência em toda a infraestrutura. Quando tratamos de uma solução de segurança avançada integrada de prevenção, detecção e resposta esse controle se relaciona como uma abordagem holística para a detecção e resposta a ameaças, que envolve a integração e correlação de dados de várias fontes em uma única plataforma. Essa abordagem permite que as equipes de segurança monitorem e analisem as atividades de segurança em toda a infraestrutura de TI, incluindo redes, *endpoints* e aplicativos.

Dessa maneira uma solução de segurança avançada integrada de prevenção, detecção e resposta deve ser capaz de analisar os dados coletados em tempo real, utilizando algoritmos avançados para identificar comportamentos suspeitos, devendo ser capaz de compartilhar inteligência de ameaças com outras ferramentas de segurança, como soluções de SIEM/SOAR. Além disso, ela deverá ser capaz de automatizar a detecção e a resposta a incidentes, incluindo a remediação de ameaças, a isolação de sistemas comprometidos e a coleta de evidências forenses. Isso tudo sem esquecer que ela deverá dispor de uma oferta de relatórios detalhados e trilhas de auditoria para fins de conformidade e gerenciamento de riscos.

O Gartner prevê que, até 2027, 50% das organizações usarão uma solução desse tipo para melhorar a detecção e resposta a ameaças. O Gartner também destaca a importância da integração das soluções de segurança avançada integrada de prevenção, detecção e resposta com outras ferramentas de segurança, como soluções de gerenciamento de informações e eventos de segurança (SIEM), soluções de prevenção de intrusões (IPS) e soluções de gerenciamento de vulnerabilidades (VMS), para fornecer uma visão mais abrangente das atividades de segurança.

Diante dos desafios criados pelos processos de transformação digital das organizações públicas e pelos desafios de dependência tecnológica impostos pela Covid-19, acabou por forçar as organizações a expandir seu ambiente de trabalho em regime remoto. Dessa forma, os ambientes das organizações tornaram-se mais visíveis e vulneráveis a ataques com roubo de informações além da possibilidade de comprometimento do ambiente do CNPq, a exemplo o expressivo aumento dos casos de *ransomware*.

Em ataques cibernéticos recentes, grupos de hackers têm considerado sistemas de governo como alvos compensadores, no intuito de provocar diferentes impactos, como: o potencial dano à imagem do Governo perante seu público interno e perante a comunidade internacional, o descrédito da população nos serviços públicos, a desconfiança de investidores internacionais na capacidade da administração pública em proteger seus próprios sistemas, a desconfiança nos processos eleitorais e o descontentamento da população com relação à Administração Pública.

Uma vez que o CNPq não possui soluções dedicadas para gerar visibilidade centralizada de eventos de segurança, a pretensa contratação vai diretamente a encontro destas necessidades, contribuindo de forma considerável para o aumento do nível de maturidade em segurança da informação do ambiente tecnológico da Instituição em diversas camadas além do cumprimento aos requisitos legais.

A paisagem de ameaças cibernéticas tem se tornado cada vez mais complexa e diversificada. O contrato anterior, firmado em 2018 e que utiliza a solução da fabricante Trend Micro, cobria *endpoints* e servidores. Entretanto, essa cobertura não contempla os novos vetores de ataque. Apesar da solução implementada pelo CNPq estar em operação há mais de 10 (dez) anos e atender satisfatoriamente, ameaças mais sofisticadas, como *ransomware, phishing* e exploração de vulnerabilidades específicas em *containers* e dispositivos móveis, exigem uma abordagem mais ampla e integrada.

O uso de *containers*, como *Docker* e *Kubernetes*, vem crescendo significativamente devido à sua eficiência e escalabilidade. No entanto, eles também trazem novos desafios de segurança, como a gestão de imagens inseguras, vulnerabilidades em ambientes orquestrados e a falta de visibilidade em tempo real. Uma solução de segurança dedicada a *containers* permitirá monitoramento contínuo, correção de vulnerabilidades e proteção contra ameaças específicas a esse ambiente.

Em relação aos dispositivos móveis, observa-se um aumento expressivo na adoção dessas tecnologias no ambiente corporativo, tanto para fins de comunicação quanto para acesso a dados e sistemas. Isso, por sua vez, amplia os riscos de ataques cibernéticos. A falta de uma solução específica para a proteção desses dispositivos pode expor a organização a ameaças como *malwares* móveis, aplicativos maliciosos e ataques de *phishing* voltados especificamente para dispositivos móveis.

Ferramentas de colaboração, como e-mails corporativos, aplicativos de comunicação (Microsoft Teams, Slack, etc.) e plataformas de compartilhamento de arquivos, tornaram-se essenciais para a operação das organizações. Entretanto, esses ambientes são frequentemente alvo de ataques, como *phishing*, *malware* distribuído por anexos e tentativas de roubo de credenciais. A respeito do serviço de *antispam*, com a crescente dependência da comunicação eletrônica, as empresas tornaram-se mais vulneráveis a uma inundação constante de mensagens não solicitadas, conhecidas como *spam*. Esta avalanche de e-mails indesejados pode comprometer a eficiência operacional, desperdiçar tempo valioso dos funcionários e aumentar os riscos de segurança cibernética. A contratação de um software de *antispam* torna-se uma necessidade crítica para mitigar estes desafios, visto que atualmente o CNPq não dispõe de um contrato ativo deste tipo de solução, sendo não apenas uma medida preventiva, mas também uma parte essencial da estratégia de segurança cibernética e gestão de comunicações. Ao investir em tecnologias robustas, as organizações podem proteger seus ativos digitais e garantir uma operação suave e eficiente, livre das perturbações causadas pelo dilúvio constante de *spam*.

A superfície de ataque das organizações tem se expandido significativamente com o aumento da digitalização e do trabalho remoto. Sem uma solução abrangente que possibilite mapear, monitorar e mitigar vulnerabilidades em todos os pontos de contato digital, a organização se torna vulnerável a explorações não monitoradas, como brechas de segurança em dispositivos conectados, redes e aplicações em nuvem.

Diversas regulamentações, como a LGPD (Lei Geral de Proteção de Dados) e outras normas de proteção de dados, exigem que as organizações mantenham uma infraestrutura de segurança robusta e abrangente para proteger dados sensíveis. Uma cobertura limitada apenas a *endpoints* e servidores não é suficiente para atender a essas exigências, especialmente em setores que lidam com grandes volumes de dados pessoais e sensíveis.

Por fim, expandir a cobertura de segurança reduz consideravelmente a probabilidade e o impacto de incidentes cibernéticos. Brechas em ambientes não protegidos, como *containers*, dispositivos móveis e plataformas de colaboração, podem gerar custos significativos para a organização, tanto em termos financeiros quanto reputacionais. Investir em uma segurança proativa ajuda a mitigar esses riscos de forma eficaz.

Destaca-se que uma gestão centralizada das tecnologias permite uma administração mais eficiente e coerente de todos os recursos de segurança, facilitando a implementação de políticas, monitoramento e manutenção de toda a infraestrutura de TI, alinhando-se ao Decreto n.º 10.222, de 5 de fevereiro de 2020, referente à Estratégia Nacional de Segurança Cibernética - E-Ciber. Essa abordagem unificada permite uma resposta mais rápida e eficaz a incidentes de segurança, garantindo uma postura defensiva mais proativa e resiliente.

3. ÁREA REQUISITANTE

Área requisitante	Responsável
COINT/CGETI	Ana Paula Mendes Teixeira

4. NECESSIDADES DE NEGÓCIO

De maneira inicial e não exaustiva podemos listar as seguintes necessidades de negócio:

- **Solução de segurança para *endpoints*:** é um software projetado para proteger dispositivos finais, como computadores, laptops e dispositivos móveis, contra uma variedade de ameaças digitais, incluindo *malware*, *ransomware*, *phishing* e outras formas de ataques cibernéticos. Essas soluções geralmente incluem recursos como antivírus, firewall, detecção de intrusão, controle de aplicativos e proteção de dados, visando garantir a integridade, confidencialidade e disponibilidade dos dados armazenados nos dispositivos e na rede corporativa.
- **Solução de segurança para servidores físicos, virtuais e em nuvem:** é um conjunto integrado de medidas e ferramentas destinadas a proteger os ativos de uma organização em ambientes de TI diversos. Essas soluções devem adaptar-se às peculiaridades de cada tipo de infraestrutura, garantindo a proteção de servidores físicos contra acessos não autorizados e ataques físicos, a segurança de servidores virtuais contra ameaças digitais e a integridade dos dados e aplicações em ambientes de nuvem, onde a responsabilidade pela segurança é compartilhada entre o provedor de serviços e o usuário.
- **Solução de segurança para e-mails (*antispam*):** é um conjunto de tecnologias e medidas projetadas para filtrar e-mails indesejados e potencialmente perigosos, como *spam*, *phishing* e *malware*, antes que cheguem à caixa de entrada dos usuários. Essas soluções utilizam uma variedade de métodos, como listas negras, análise de conteúdo, verificação de reputação de remetentes, assinaturas de malware e aprendizado de máquina, para identificar e bloquear mensagens maliciosas, protegendo assim os usuários e a infraestrutura de TI contra ameaças cibernéticas relacionadas a e-mails.
- **Solução de segurança para ambiente de colaboração:** é um software projetado para proteger plataformas de colaboração online, como intranets, sistemas de mensagens instantâneas, compartilhamento de arquivos e espaços de trabalho colaborativos, contra uma variedade de ameaças cibernéticas. Essas soluções incluem recursos como controle de acesso, criptografia de dados, monitoramento de atividades suspeitas, prevenção contra vazamento de dados e integração com outras soluções de segurança, visando garantir a confidencialidade, integridade e disponibilidade das informações compartilhadas entre os colaboradores, enquanto mantém a conformidade regulatória e protege a reputação e os ativos da organização.
- **Solução de segurança para *containers*:** é um software especializado destinado a proteger ambientes baseados em contêineres, como Docker e Kubernetes, contra ameaças cibernéticas. Essas soluções abordam os desafios únicos apresentados pela natureza dinâmica e escalável dos contêineres, incluindo a segmentação de redes, monitoramento contínuo, detecção de vulnerabilidades, gerenciamento de identidades e acessos, proteção de APIs, e integração com plataformas de DevOps para garantir que os contêineres sejam implantados, gerenciados e executados de forma segura em toda a cadeia de desenvolvimento e implantação de software.
- **Solução de segurança para dispositivos *mobile***: é um software projetado para proteger smartphones, tablets e outros dispositivos móveis contra uma variedade de ameaças cibernéticas, como *malware*, *phishing*, roubo de dados e acesso não autorizado. Essas soluções incluem recursos como antivírus, firewall, criptografia de dados, controle de acesso, detecção de ameaças em tempo real, gerenciamento de dispositivos móveis (MDM) e segurança de aplicativos, com o objetivo de garantir a integridade, confidencialidade e disponibilidade dos dados armazenados e transmitidos nos dispositivos móveis, além de proteger a privacidade e segurança dos usuários em ambientes corporativos e pessoais.

- **Gerenciamento de risco e superfície de ataque:** é uma ferramenta projetada para ajudar organizações a identificar, avaliar, monitorar e mitigar riscos associados à segurança cibernética. Um software dedicado a essas funções pode oferecer uma variedade de recursos, tais como mapeamento da superfície de ataque, análise de vulnerabilidades, monitoramento contínuo, relatórios e dashboards, gestão de incidentes e *compliance* e conformidade.

Os criminosos da internet (os atacantes/hackers) estão utilizando recursos de Inteligência Artificial (IA) para alavancar e acelerar, ainda mais, os ciclos de ataques. O uso de tecnologias de automação ofensiva resulta em menor latência para os atacantes ou em um tempo menor de violação (TTB), aumentando assim sua taxa de sucesso. As equipes de segurança precisam levar em consideração o fato de que os ataques estão ocorrendo em um ritmo muito mais rápido e ajustar suas estratégias defensivas. Isso requer tecnologia de automação avançada além de acompanhamento em tempo integral, com ferramentas de segurança avançadas e principalmente processos bem definidos.

O uso de uma ferramenta de segurança avançada integrada de prevenção, detecção e resposta possibilitará o aumento da estabilidade, disponibilidade e capacidade. O *core* desse tipo de ferramenta é dotado de módulos de IA (Inteligência Artificial) com enorme capacidade de detecção baseado em comportamento. Desta maneira, os riscos de alguma intercorrência são reduzidos visto que a modernização de ataques é acompanhada pela inteligência da ferramenta.

A reboque do já exposto temos uma das principais necessidades de negócio que se trata de buscar fazer mais com menos, ou seja, reduzir o custo total de propriedade (TCO) de sua infraestrutura de segurança, fornecendo uma abordagem integrada para a detecção e resposta a ameaças, que elimine ou reduza minimamente a necessidade de investir em múltiplas soluções de segurança.

Ademais, é primordial aprimorar a atuação preventiva, elevar o grau de detecção de comportamentos anômalos e agilizar a resposta a incidentes de segurança para que possamos melhorar a percepção de segurança perante os usuários do CNPq. Estes objetivos serão perseguidos nesta contratação para que estes estejam condizentes com a importância que a segurança da informação possui para a Instituição. Abaixo identificamos 5 fases no ciclo de segurança cibernética que fazem parte da estratégia de segurança da informação. São elas:

a. **Prevenção:** é o esforço para impedir que ameaças maliciosas se infiltrem na rede e para classificar os tipos de ataques direcionados ao CNPq em tempo real. Nesta fase do ciclo, o objetivo é poder interromper os ataques antes que qualquer processo possa ser executado na rede;

b. **Detecção:** é o esforço para reconhecer e identificar ameaças na infraestrutura de segurança de TI do CNPq que conseguiram se infiltrar apesar dos esforços de prevenção. Durante essa fase, a solução precisa ser capaz de identificar processos maliciosos que estão sendo executados em um *endpoint*, na rede e/ou na nuvem;

c. **Contenção:** é o esforço para impedir a disseminação de uma ameaça cibernética, uma vez que ela tenha sido detectada e identificada na rede;

d. **Recuperação:** ocorre após a contenção da ameaça. Nesta fase, as equipes de segurança do CNPq e da Contratada trabalham em conjunto para restaurar a infraestrutura de TI ao seu estado anterior e estável;

e. **Remediação:** é esforço feito para garantir que processos e tecnologias sejam atualizados para mitigar futuros eventos cibernéticos. Isso inclui o reforço de programas de treinamento e conscientização de funcionários, pois os indivíduos desempenham um papel crucial na viabilização de violações de segurança cibernética.

4.1. Soluções de segurança do mesmo fabricante e integradas entre si

Adotar uma única solução de segurança que cubra *endpoints*, servidores, e-mails, ambientes de colaboração, *containers*, dispositivos móveis, gerenciamento de risco e superfície de ataque oferece várias vantagens estratégicas e operacionais para o CNPq. Essa abordagem centralizada não apenas fortalece a postura de segurança, mas também simplifica a gestão e promove maior eficiência em toda a organização.

Uma pesquisa recente do Gartner (Gartner Survey Shows 75% of Organizations Are Pursuing Security Vendor Consolidation in 2022) mostrou que as organizações querem consolidar seus fornecedores de segurança para reduzir a complexidade e melhorar a postura a riscos. Longos processos de aquisição ou solicitações de propostas estão permitindo ofertas consolidadas, como XDR para *endpoints* e SASE para conectividade de ponta e segurança com integração no *backend*.

A consolidação de cibersergurança se apresenta como uma estratégia viável para enfrentar as crescentes ameaças do ambiente digital, especialmente em regiões emergentes como a América Latina. Em entrevista à Security Report (https://securityleaders.com.br/consolidacao-de-ciberseguranca-eficiencia-ou-risco/), o Diretor Global de Alianças em Segurança da Informação da Hitachi Vantara, BJ Deonarain, explica que a região segue vulnerável a ataques como *ransomware* e *phishing*. Na visão do executivo, a consolidação em uma solução pode ser uma solução para reduzir a complexidade das arquiteturas de segurança da informação, além de promover maior eficiência e controle de custos.

Uma plataforma unificada proporciona visibilidade centralizada de todos os ativos e áreas de TI, permitindo o monitoramento contínuo e a gestão de ameaças em tempo real. Isso capacita a equipe de segurança a detectar, investigar e responder rapidamente a incidentes, reduzindo o tempo de resposta e minimizando o impacto das ameaças.

A utilização de diversas soluções de segurança de fornecedores diferentes tende a aumentar a complexidade de integração, gerenciamento e suporte. Por outro lado, uma solução única simplifica esses processos, facilitando a implementação de políticas de segurança consistentes e uniformes em todos os sistemas e dispositivos. Essa simplificação também alivia a carga de trabalho da equipe de TI, melhorando a eficiência operacional e permitindo que o foco seja direcionado para iniciativas mais estratégicas.

Além disso, a adoção de uma solução unificada favorece a conformidade com regulamentações de segurança e privacidade, como a LGPD e o GDPR. Com todos os dados e logs de segurança geridos em uma plataforma única, auditorias e verificações de conformidade tornam-se mais fáceis, garantindo que as políticas de segurança sejam aplicadas de maneira consistente em toda a organização.

Soluções de segurança integradas também oferecem um suporte superior para a automação de respostas a incidentes (SOAR) e a orquestração de processos. Isso permite a execução de ações automáticas para mitigar ameaças, muitas vezes sem a necessidade de intervenção humana. Como resultado, a resposta a incidentes é mais rápida, o que reduz o potencial de danos causados por ataques e otimiza o uso dos recursos humanos da equipe de segurança, permitindo que se concentrem em ameaças mais complexas.

Outra vantagem altamente significativa é a cobertura robusta e amplificada de grande parte de vetores de ataque. Uma solução unificada adota uma abordagem de "defesa em profundidade", onde várias camadas de segurança se complementam, fechando lacunas de proteção que poderiam ser exploradas por ameaças avançadas. Isso fortalece a resiliência da organização contra ataques sofisticados.

Para os usuários finais, o uso de uma solução integrada resulta em uma experiência mais fluida e menos invasiva. A redução da necessidade de múltiplos logins, notificações redundantes ou softwares distintos melhora a produtividade, sem comprometer a segurança, proporcionando um ambiente mais estável e seguro.

No aspecto operacional, a gestão de *patches* e atualizações de segurança também é simplificada em uma solução unificada. Áreas críticas podem ser atualizadas de forma coordenada, minimizando os riscos de vulnerabilidades decorrentes de falhas ou atrasos em atualizações.

Além disso, uma plataforma integrada facilita a identificação e o controle de ativos e sistemas não autorizados, conhecidos como "*shadow IT*". Isso melhora a governança da TI, reduzindo os riscos associados ao uso de ferramentas não aprovadas pela organização, garantindo maior controle e segurança sobre os recursos de TI. Destaca-se também que, quando diferentes soluções que trabalham "integradas" não é incomum o surgimento de

algum problema e, em situações como estas, há uma disputa entre os fabricantes sobre quem é o responsável, interferindo na resolução do impedimento e impactando a instituição.

Por fim, a implementação e gestão de diversas soluções de segurança geralmente resultam em custos mais altos, tanto em licenciamento quanto em manutenção. Com uma única solução, esses custos são consolidados, permitindo que a organização aproveite economias de escala. Além disso, a redução da necessidade de integração personalizada entre ferramentas diferentes reduz o custo total de propriedade, já que os investimentos em treinamento, implantação e suporte também são centralizados e otimizados. Isso resulta em uma estratégia mais econômica e eficiente para o CNPq.

5. NECESSIDADES TECNOLÓGICAS

Solução de segurança de *endpoints* e Solução de segurança de servidores físicos, virtuais e em nuvem	
ID	**DESCRIÇÃO**
1	**Funcionalidades gerais**
1.1	Deve permitir a programação de atualizações automáticas das listas de definições de vírus, a partir de local predefinido da rede, ou de site seguro da internet, com frequência (no mínimo diária) e horários definidos pelo administrador da solução.
1.2	Deve permitir atualização incremental da lista de definições de vírus.
1.3	Deve permitir a atualização automática do *engine* do programa de proteção a partir de localização na rede local ou na internet, a partir de fonte autenticável.
1.4	Deve permitir o *rollback* das atualizações das listas de definições de vírus e *engines*.
1.5	Deve permitir a indicação de agentes para efetuar a função de replicador de atualizações e configurações, de forma que outros agentes possam utilizá-los como fonte de atualizações e configurações, não sendo necessária a comunicação direta com o servidor de *anti-malware* para essas tarefas.
1.6	Deve permitir que os agentes de atualização possam replicar os componentes de vacinas, motores de escaneamento, versão de programas, *hotfix* e configurações específicas de domínios da árvore de gerenciamento.
1.7	Deve permitir proteção das configurações da solução instalada na estação de trabalho através de senha ou controle de acesso, em ambos os casos, controlada por política gerenciada pelo console de administração da solução completa.
1.8	Deve possibilitar instalação "silenciosa".
1.9	Deve possuir firewall integrado.
1.10	Deve possuir EDR - Detecção e Resposta a Ameaças.
1.11	Deve possuir XDR - Extended Detection and Response.
1.12	Deve possuir *machine learning* e *behavioral analysis* para detecção de ameaças.
1.13	Deve possuir console de gerenciamento centralizado.
1.14	Deve possuir recursos de prevenção de perda de dados (DLP).
1.15	Deve possuir *whitelisting* de aplicações pré-aprovadas para execução.
1.16	Deve permitir integração com sistemas de gerenciamento de eventos de segurança (SIEM).
1.17	Deve permitir *rollback* de ações maliciosas.
1.18	Deve possuir capacidades de *threat hunting*.
1.19	Deve possui capacidade de executar arquivos suspeitos em ambiente isolado (sandbox).
2	**Proteção anti-malware para estações de trabalho Microsoft Windows**
2.1	A solução deve atender a estações de trabalho com solução de virtualização de desktops com o Sistema Operacional Windows.
2.2	Deve ser capaz de realizar a proteção a códigos maliciosos nos sistemas operacionais: • Microsoft Windows 8 e versões superiores.
2.3	Suportar as seguintes plataformas virtuais: • VMware Vsphere ESXi 7 e versões superiores.
2.4	Deve detectar, analisar e eliminar, automaticamente e em tempo real, programas maliciosos em: • Processos em execução em memória principal (RAM); • Arquivos executados, criados, copiados, renomeados, movidos ou modificados, inclusive em sessões de linha de comando (DOS ou Shell); • Arquivos compactados automaticamente, em pelo menos nos seguintes formatos: zip, exe, arj, mime/uu, Microsoft cab; • Arquivos recebidos por meio de programas de comunicação instantânea tais como Whatsapp, Telegram, Facebook Messenger, Microsoft Teams, Zoom, Google Meet; • Arquivos recebidos a partir de sites Web; • Arquivos acessados ou recebidos por e-mail.
2.5	Deve permitir diferentes configurações de detecção (varredura ou rastreamento): • Em tempo real de arquivos acessados pelo usuário; • Em tempo real dos processos em memória, para a captura de programas maliciosos executados em memória, sem a necessidade de escrita de arquivo; • Manual, imediato ou programável, com interface gráfica em janelas, personalizável, com opção de limpeza; • Por linha de comando parametrizável.
2.6	Deve possuir funcionalidade de "*Machine Learning*" utilizando como fonte de aprendizado a rede de inteligência do fabricante, identificando os aspectos maliciosos, características de boa pontuação e correlacionando, no mínimo, com as seguintes técnicas de proteção a vetores de ataque: • Reputação de URL para exploração de navegadores, websites infectados e Office Exploits; • Reputação de arquivos para downloads de arquivos e anexos de e-mail.
2.7	Execução do instalador de software com classificação comportamental do instalador.
2.8	Execução do malware de software com classificação comportamental do instalador.

3	**Proteção *anti-malware* para estações de trabalho Linux**
3.1	A solução deve atender a estações de trabalho Linux.
3.2	Deve ser capaz de realizar a proteção a códigos maliciosos nos seguintes sistemas operacionais, no mínimo: • Ubuntu Linux 20.04 e versões superiores; • Suse Linux Enterprise.
3.3	Deve possuir integração com a solução de Detecção e Resposta Avançada de Ataques (XDR).
3.4	A console de gerenciamento deve permitir o gerenciamento das políticas de segurança através da Internet.
4	**Solução de segurança para proteção para Data Center**
4.1	A solução de deve atender a um ambiente de aproximadamente 500 sockets e 30 hosts.
4.2	Deve ser compatível com pelo menos os seguintes sistemas operacionais nas versões indicadas e versões superiores: • CentOS 7 e superiores; • Debian GNU/Linux 10 e superiores; • Windows Server 2008 e superiores; • Oracle Linux 7 e superiores; • Red Hat Enterprise Linux 7 e superiores; • VMWare ESXi 7 e superiores.
4.3	Suportar as seguintes plataformas virtuais: • VMware Vsphere ESXi 7 e versões superiores.
4.4.	O console de gerenciamento deve ser on-premises, permitindo o gerenciamento das políticas de segurança através da Internet.
4.5.	Deve possuir integração com a solução de Detecção e Resposta Avançada de Ataques (XDR).
4.6	Deve ser gerenciada por console Web, compatível com pelo menos os browsers Microsoft Edge, Firefox e Google Chrome.
4.7	Deve suportar certificado digital para gerenciamento.
4.8	O console de administração deve permitir o envio de notificações via SMTP.
4.9	Todos os eventos e ações realizadas no console de gerenciamento precisam ser gravados, visando a auditoria.
4.10	Deve permitir a criação de widgets para facilitar a administração e visualização dos eventos.
4.11	A funcionalidade de anti-malware deve possuir as seguintes características: • Deve permitir a proteção contra códigos maliciosos através da instalação de agentes, permitindo rastrear ameaças em tempo real, varredura sob demanda e agendamento, com possibilidade de tomada de ações distintas para cada tipo de ameaça; • Deve possibilitar a criação de listas de exclusão, para que o processo do antivírus não execute a varredura em determinados diretórios ou arquivos do sistema operacional; • Deve possuir listas de exclusão separadas por módulo da proteção anti-malware como exclusão das detecções por comportamento, exclusão por machine learning e exclusão por assinatura; • Em plataforma Windows, deve permitir criar exclusões de escaneamento a partir do certificado digital das aplicações; • Deve possibilitar a verificação de ameaças dentro de arquivos compactados, efetuando a limpeza apenas de arquivos maliciosos em casos de detecção. A limpeza deve ocorrer sem a descompactação do arquivo; • O scan de arquivos comprimidos deve ser de no mínimo 6 camadas de compressão; • O scan de arquivos comprimidos do tipo OLE deve ser de no mínimo 20 camadas de compressão.
4.12	A funcionalidade de Proteção Contra URLs Maliciosas deve possuir as seguintes características: • Deve permitir a proteção contra acesso a websites ou URLs consideradas maliciosas ou de baixa reputação; • A lista de URLs deve ser fornecida e atualizada automaticamente pelo fabricante, permitindo a consulta em uma base local ou na nuvem da reputação das URLs acessadas;
4.13	O módulo de Firewall deve possuir as seguintes características: • Operar como firewall de host, através da instalação de agente nos servidores protegidos; • Deve possuir a capacidade de controlar o tráfego baseado nos tipos de protocolos, endereços IP e intervalo de portas.
5	**Detecção e Resposta Avançada de Ataques (XDR)**
5.1	Deve suportar a coleta de dados de diversas fontes, incluindo *endpoints*, rede, filtros da web e sensores de nuvem, para acelerar a detecção e resposta a incidentes e reduzir os tempos de resposta.
5.2	Deve permitir a integração com plataformas de segurança via API.
5.3	Deve ser capaz de ingerir diversas fontes de dados, entre elas *Network Intrusion Detection Systems* (NIDS), *Endpoint Protection Platforms* (EPP), E*ndpoint Detection and Response* (EDR), com objetivo de aprimorar o processo de detecção de ameaças e tornar ágil processo de correlação e investigação de alertas.
5.4	Deve permitir a integração com a ferramenta de gerenciamento de tickets CA Service Desk e GLPI possibilitando a gestão unificada de incidentes.
5.5	A quantidade de coletores necessários para a total ingestão de eventos do ambiente não deve onerar ou gerar custos adicionais de licenciamento;
5.6	Deve fornecer ambiente gráfico para criação de fluxos de interação.
5.7	Deve permitir a automação das atividades de resposta a incidentes com base nas necessidades e processos mapeados.
5.8	Deve fornecer visibilidade de possíveis vazamentos de contas de usuário.
5.9	Deve fornecer informações de elevação de privilégio das contas nos dispositivos.
5.10	Deve ser compatível com a solução NSX da VMware para permitir integração com os ambientes virtualizados do CNPq.
5.11	Deve realizar a coleta e análise dos dados de atividade de endpoints de desktop e servidor.
5.12	Deve realizar a coleta e análise dos dados de atividade de contas de e-mail.

5.13	Deve fornecer insights sobre a postura de segurança baseado em um índice geral de risco, exposição de dispositivos, ataques em andamento e outros fatores relacionados.
5.14	Deve realizar a descoberta dos ativos organizacionais expostos a ataques, incluindo dispositivos e ativos voltados para a Internet, contas, aplicativos em nuvem e ativos em nuvem.
5.15	Deve realizar a avaliação das comunicações com destino a internet relacionadas a atividades ou endereços maliciosos ou vulneráveis, identificando os usuários e dispositivos envolvidos, fornecendo informações de mitigação do risco detectado.
5.16	Possuir console Web para gerenciamento e administração da ferramenta.
5.17	Possuir modelos pré-definidos pelo fabricante de atividades suspeitas e maliciosas para identificação e categorização de ameaças no ambiente.
5.18	Deve fornecer um índice de risco com base nas configurações de produtos integrados do fornecedor para reduzir o risco induzido por erros humanos.
5.19	Permitir criação de listas de exceção de objetos para redução de falso-positivo.
5.20	Os modelos de detecção deverão possuir níveis de severidade (score) individuais para cada modelo em pelo menos os seguintes níveis: crítico; alto; médio; baixo.
5.21	Deve prover relatórios de inteligência de ameaças avançadas mais recentes e indicadores de comprometimento para ajudar sua organização a se defender proativamente contra ameaças.
5.22	Deve integrar relatórios de inteligência criados por especialistas em ameaças do fabricante e terceiros para ajudar na identificação de ameaças.
5.23	Os relatórios de ameaças do fabricante deverão gerar alertas de detecção caso sejam identificadas atividades presentes nos relatórios dentro do ambiente.
5.24	Deve ser possível identificar individualmente cada relatório de ameaça.
5.25	Deve permitir adicionar bases de inteligência terceiras de forma manual, por API, importando arquivos com base CSV ou STIX através de assinatura de feeds de inteligência de ameaças terceiros.
5.26	Deve ser possível realizar buscas através de *strings* parciais, exatas, valores nulos, *wildcards* e caracteres especiais.
5.27	O campo de busca deve permitir o uso de múltiplos operadores lógicos para no mínimo: E; Ou; Não.
5.30	Deve permitir indexar múltiplas buscas utilizando operadores lógicos.
5.31	Deve permitir salvar pesquisas com os critérios de busca e operadores lógicos utilizados para futuras consultas.
5.32	Deve permitir pesquisar por atividades de cada um dos contextos, mesmo que não tenham gerado qualquer tipo de detecção pelos modelos de detecção de ameaça.
5.33	Deve permitir investigar os alertas gerados pelos modelos de detecção por meio de uma análise impacto e análise de causa raiz.
5.34	Deve consolidar e correlacionar diferentes modelos de ameaça relacionados a um único evento.
5.35	Deve somar as pontuações (*score*) de cada modelo durante a correlação das atividades para melhor categorização do incidente.
5.36	Deve exibir todos os detalhes do incidente em uma única página, contendo no mínimo: • Status do incidente; • Score; • Quantidade de contas de e-mail impactadas; • Data e hora da detecção; • Técnica do MITRE utilizada; • Modelo(s) de detecção acionado(s); • Objetos detectados dentro de cada modelo; • Deve permitir alterar o status de cada evento, para no mínimo Novo, Em progresso/análise e Fechado ou escala equivalente.
5.37	Permitir adicionar comentários e notas a cada evento pelos analistas da ferramenta.
5.38	Durante o processo de análise da cadeia de processos deve ser possível verificar todos os objetos relacionados à esta análise, as atividades executadas pelos objetos e sua reputação conforme categorização do fabricante.
5.39	Deve ser possível interagir com cada um dos objetos relacionados ao evento para análise avançada e resposta.
5.40	Deve destacar e organizar as atividades relacionadas a cada modelo de detecção por ordem cronológica, permitindo identificar a relação de cada atividade com os modelos de detecção.
5.41	Permitir adicionar um comentário junto a cada ação tomada para registro e contextualização das ações.
5.42	Deve permitir remover arquivos SHA-1, URLs, IPs ou domínios a lista de bloqueio dos sensores.
5.43	Permitir coletar e fazer o download de um arquivo para investigação local detalhada.
5.44	Permitir adicionar o remetente (*sender*) de um e-mail na lista de bloqueio, impedindo o mesmo de enviar novos e-mails os usuários da sua empresa.
5.45	Mover o e-mail selecionado para a área de quarentena de um específico usuário ou todos os usuários que contenham este e-mail em suas caixas.
5.46	Deletar o e-mail selecionado das caixas selecionadas.
5.47	Deve permitir verificar todas as ações de respostas executadas no console ou por API.
5.48	Deve exibir os seguintes painéis de controle: • Índice de risco da empresa; • MITRE ATT&CK® Mapping for Enterprise; • Visão geral de alertas; • Top 10 vulnerabilidades em risco; • Top 10 usuários em risco; • Top 10 dispositivos em risco;
5.49	Deve permitir a geração e o download de relatórios únicos e/ou agendados.
5.50	Deve possuir a capacidade de sugerir termos de busca, de acordo com o conteúdo já buscado numa investigação, para agilizar a obtenção do resultado.
5.51	Deve permitir exportar sob demanda os logs em texto puro (CSV ou PDF).
5.52	Deve permitir investigação por palavras-chave customizadas para facilitar a busca de eventos.
5.53	Deve permitir recebimento e encaminhamento de logs via syslog.
5.54	Deve permitir receber logs de diferentes dispositivos.
6	**Proteção Host IPS e Host Firewall**

6.1	Deve ser capaz de realizar a proteção a códigos maliciosos nos seguintes sistemas operacionais e superiores: • Microsoft Windows 8; • CentOS 7; • Windows Server 2008; • Ubuntu 18; • Red Hat Enterprise Linux Server.
6.2	Deve possuir módulo para proteção de vulnerabilidades com as funcionalidades de host IPS e host firewall.
6.3	O módulo deve ser integrado como solução do *endpoint* e ser gerenciado pelo mesmo console, sem que haja custo de licença adicional.
6.4	Todas as regras das funcionalidades de *firewall* e IPS de host devem permitir apenas detecção (log) ou prevenção (bloqueio).
6.5	Deve permitir ativar e desativar o produto sem a necessidade de remoção.
6.6	Deve possuir capacidade de identificar e bloquear, no mínimo, os seguintes tipos de ataques: • *Denial of Service* (DOS); • *Port scanning;* • *Network Flooding*.
6.7	Deve permitir a emissão de alertas via SMTP e SNMP.
7	**Controle de aplicações de *endpoints***
7.1	Deve ser capaz de realizar a proteção a códigos maliciosos nos seguintes sistemas operacionais e superiores: • CentOS 7 e superiores; • Debian GNU/Linux 10 e superiores; • Windows Server 2008 e superiores; • Oracle Linux 7 e superiores; • Red Hat Enterprise Linux 7 e superiores.
7.2	O módulo deve ser integrado como solução do *endpoint* e ser gerenciado pelo mesmo console, sem que haja custo de licença adicional.
7.3	Deve permitir a criação de políticas de segurança personalizadas.
7.4	As políticas de segurança devem permitir a seleção dos alvos baseados nos seguintes critérios: • Nome parcial ou completo das estações de trabalho, permitindo a utilização de caractere coringa para identificação do nome parcial da máquina; • Range de endereços IPS; • Sistema operacional; • Grupos de máquinas espelhados do Active Directory e LDAP; • Usuários ou grupos do Active Directory e LDAP.
7.5	As políticas de segurança devem permitir a combinação lógica dos critérios para identificação do(s) alvo(s) de cada política.
7.6	As políticas de segurança devem permitir o controle do intervalo de envio dos logs.
7.7	As políticas de segurança devem permitir o controle do intervalo para envio de atualização de cada política.
7.8	As políticas de segurança devem permitir a definição de qual servidor de gerenciamento o agente de segurança deve comunicar-se.
7.9	As políticas de segurança devem permitir a ocultação do ícone do agente, que reside da barra de tarefas, e de notificações ao usuário.
7.10	As políticas de segurança devem permitir o controle através de regras de aplicação.
7.11	As regras de controle de aplicação devem permitir as seguintes ações: • Permissão de execução; • Bloqueio de execução; • Bloqueio de novas instalações.
7.12	As regras de controle de aplicação devem permitir o modo de apenas coleta de eventos (logs), sem a efetivação da ação regra.
8	**Proteção contra vazamento de informações (DLP) de *Endpoints***
8.1	Deve ser capaz de realizar a proteção contra vazamento de informações nos seguintes sistemas operacionais e versões superiores: • Microsoft Windows 8; • CentOS 7; • Windows Server 2008; • Ubuntu 18; • Red Hat Enterprise Linux Server.
8.2	O módulo deve ser integrado como solução do *endpoint* e ser gerenciado pelo mesmo console, sem que haja custo de licença adicional.
8.3	Deve possuir nativamente *templates* para atender as seguintes regulamentações: • LGPD (Lei nº 13.709/2018); • Lei do Sigilo Bancário (Lei Complementar nº 105/2001); • Lei do Prontuário Eletrônico (Lei nº 13.787/2018); • Marco Civil da Internet (Lei nº 12.965/2014); • Código de Defesa do Consumidor (Lei nº 8.078/1990).

8.4	Deve ser capaz de detectar informações, em documentos nos formatos: • Documentos: Microsoft office (doc, docx, xls, xlsx, ppt, pptx) openoffice, rtf, wordpad, text; xml, html; • Gráficos: visio, postscript, pdf, tiff; • Comprimidos: win zip, rar, tar, jar, arj, 7z, rpm, cpio, gzip, bzip2, unix/linux zip, lzh; • Códigos: c/c++, java, verilog, autocad.
8.5	Deve ser capaz de detectar informações, com base em: • Dados estruturados, como dados de cartão de crédito, dados pessoais, endereços de e-mail, CPF, entre outros, através de palavras ou frases exatas, padrão de documentos conhecidos e formato pré-definido de identificação de dados; • Dados não-estruturados, como documentos exportados, reformatados ou sem estrutura de dados definida, através de expressões regulares ou descoberta de dados por aprendizado de padrões e criação de *fingerprinting*.
8.6	Deve ser capaz de detectar em arquivos compactados.
8.7	Deve permitir a configuração de quantas camadas de compressão serão verificadas.
8.8	Deve permitir a criação de modelos personalizados para identificação de informações.
8.9	Deve permitir a criação de modelos com base em regras e operadores lógicos.
8.10	Deve possuir modelos padrões.
8.11	Deve permitir a importação e exportação de modelos.
8.12	Deve permitir a criação de políticas personalizadas.
8.13	Deve permitir a criação de políticas baseadas em múltiplos modelos.
8.14	Deve permitir mais de uma ação para cada política, como: • Apenas registrar o evento da violação; • Bloquear a transmissão; • Gerar alertar para o usuário; • Gerar alertar na central de gerenciamento; • Capturar informação para uma possível investigação da violação.
8.15	Deve permitir criar regras distintas com base se a estação está fora ou dentro da rede.
9	**MacOS**
9.1	Deve ser compatível com as seguintes versões do MacOS 10.13 e subsequentes.
9.2	Deve trabalhar de forma híbrida, fazendo uso de assinaturas, *machine learning* e detecção de comportamento para identificar *malwares* no *endpoint*.
9.3	Deve possuir uma regra pré-definida para análise de *malware* consultando extensões comumente utilizadas para otimizar o uso de recurso do *endpoint.*
9.4	A solução deve possuir uma regra pré-definida para análise de *malware* consultando somente arquivos Mach-O ou permitir ler todos os arquivos.
9.5	Deve permitir scanear compartilhamentos de rede, arquivos comprimidos e *Time Machine*.
9.6	Em caso de detecção a solução deve tomar uma das seguintes ações: • Liberar acesso; • Quarentenar; • Limpar; • Deletar.
9.7	Deve permitir colocar programa, extensões ou arquivos em exclusão para evitar falso positivos e otimizar o uso de recurso.
9.8	Deve possuir a função *Scan Cache*, otimizando o *scan* nas máquinas, armazenando informações dos arquivos que já são conhecidos como bons.
9.9	Deve possuir módulo de proteção contra alteração dos arquivos.
9.10	Deve ser capaz de liberar ou bloquear os seguintes dispositivos: • CD/DVD; • Compartilhamentos de rede; • SD card; • Dispositivos *thunderbolt* de armazenamento; • Dispositivos de armazenamento USB; • Deve ser possível adicionar dispositivos de armazenamento USB a lista de dispositivos permitidos utilizando nome do fabricante, ID do dispositivo e número de serial.
9.11	Deve ser possível configurar ao menos as seguintes ações: • Acesso total; • Somente leitura; • Bloqueio.

Solução de segurança para e-mails (*antispam*)	
ID	**DESCRIÇÃO**

1	A solução deverá atender, no mínimo, os serviços abaixo: • Disponibilidade do serviço; • Proteção contra vírus; • Efetividade no bloqueio de SPAM; • Ocorrência de falsos-positivos; • Latência máxima na entrega de mensagens.
2	Deve ser compatível com Zimbra e Microsoft 365.
2	**Características gerais da solução**
2.1	A solução deverá possuir *Single Sign-On* para acessar o console de administração.
2.2	A solução deverá permitir a criação de regras para entrada (*inbound*) e saída (*outbound*) de e-mails.
2.3	A solução deverá possuir console de gerenciamento web.
2.4	A solução deverá possuir console centralizada, incluindo: • Configurações de administração; • Objetos de política; • Objetos suspeitos; • Gerenciamento de usuário final; • Gerenciamento de diretório; • Informações sobre licenciamento; • Logs; • Relatórios; • Visualização de mensagens quarentenadas; • Gerenciamento de domínio; • *Dashboard* baseado em gráficos; • Rastreamento de e-mails, eventos e logs.
2.5	A solução deverá possuir *dashboards* possibilitando no mínimo a visualização de ameaças, *ransomwares*, detalhes de autenticação baseada em domínio, *sandbox*, BEC, SPAM, principais violações, eventos de DLP, consumo de banda, proteção *time-of-click*.
2.6	A solução deverá possuir configurações de *dashboard* sendo possível selecionar: • Direção do tráfego: entrada e saída de e-mails (*inbound/outbound*); • Período: data, semana e mês.
2.7	A solução deve suportar sistema ARC (*Authenticated Received Chain*), preservando os resultados da autenticação de e-mail.
2.8	A solução deve ser capaz de remover conteúdos ativos encontrados em documentos anexos como Microsoft Word, Excel e PowerPoint. Se caso o conteúdo ativo não puder ser removido, deve possuir a opção de excluir o anexo que contém o conteúdo ativo.
2.9	A solução deve possuir a funcionalidade de validação de DNS reverso do remetente, tendo a capacidade de criar listas de domínios PTR (Pointer Record) que serão bloqueados; (*New Feature Available on March* 28, 2022).
2.10	A solução deverá ser capaz de permitir a filtragem baseada em reputação IP para no mínimo: • Remetentes permitidos com base no endereço IP e país; • Remetentes bloqueados com base no endereço IP, país e região.
2.11	A solução deverá ser capaz de permitir a filtragem de remetente e destinatários para no mínimo: remetentes aprovados por endereço de e-mail ou domínio, remetentes bloqueados por endereço de e-mail ou domínio.
2.12	A solução deverá possibilitar incluir X-Header no cabeçalho da mensagem para mensagens de e-mail correspondentes a remetentes aprovados.
2.13	A lista de remetentes aprovados e remetentes bloqueados deverão exibir no mínimo as seguintes informações: • Remetente; • Domínio do destinatário; • Data.
2.14	Deverá possuir correspondência de IP do remetente, possibilitando especificar um IP ou um intervalo de endereços IP em um domínio do remetente identificado pelo endereço do cabeçalho da mensagem para permitir mensagens de e-mail apenas desses endereços.
2.15	Deverá detectar *malwares*, *worms*, e outras ameaças baseadas em assinatura e padrões.
2.16	Deverá ser capaz de detectar *spam* baseado em assinatura e padrões.
2.17	Deverá identificar e-mails marketing como redes sociais, fóruns e boletins de informações.
2.18	Deverá permitir criar exceções para e-mails marketing.
2.19	A configuração de spam deverá possuir no mínimo três níveis: baixo, meio e alto.
2.20	Deverá detectar ataques de comprometimento de e-mail.
2.21	Deverá possuir detectar *phishing* e conteúdos suspeitos.
2.22	Deverá detectar mensagens de *graymail.*
2.23	Deverá realizar varreduras em arquivos JSE e VBE para identificar ameaças de macro.
2.24	Deverá detectar ameaças desconhecidas utilizando *machine learning.*
2.25	Deverá permitir visualizar relatório detalhado para cada detecção *machine learning.*
2.26	Deverá possuir *engine* própria para detecção de explorações de documentos, ameaças de dia zero, vulnerabilidades conhecidas e outras ameaças usadas em ataques direcionados.
2.27	Deverá possuir proteção *anti-ransomware*.
2.28	Deverá possuir análise de URLs no corpo do e-mail.
2.29	Deverá possuir o recurso para analisar as URLs no momento do clique do usuário e as bloquear se forem maliciosas.

2.30	Deve possuir ações de bloqueio, liberação e alerta para as seguintes categorias ou equivalentes: perigoso, altamente suspeito, não testado e suspeito.
2.31	Deverá possuir proteção contra comprometimento de e-mail.
2.32	Deverá permitir adicionar usuários de alto perfil, possibilitando exportar a lista em CSV.
2.33	Deverá possibilitar importar usuários de alto perfil através de arquivo CSV.
2.34	Deverá fornecer informações detalhadas bem como razões para mensagens de e-mail detectadas como possíveis ataques analisados ou prováveis do *Business e-mail Compromise* (BEC).
2.35	Deverá possuir proteção contra-ataques de engenharia social.
2.36	Deverá fornecer informações detalhadas bem como razões para mensagens de e-mail detectadas como possíveis ataques de engenharia social.
2.37	Deverá ser capaz utilizar no mínimo os seguintes bancos de dados de reputação que: • Tenham uma lista de endereços IP de servidores de correio que são conhecidos por serem fontes de *spam*; • Tenham uma lista de endereços IP identificados como envolvidos em *ransomware* ativos, *malware* ou outras campanhas de ameaças por e-mail; • Tenham uma lista de IPs atribuídos dinamicamente.
2.38	Deverá possibilitar configurar diferentes tipos de exceções de varredura em um e-mail através de definições de condições e possibilitando executar as ações ou equivalentes de *bypass*, deleção do e-mail incluindo anexos.
2.39	As ações de verificação configuradas para cada exceção deverão ser aplicadas a todos os remetentes e destinatários.
2.40	Deverá possibilitar incluir *tag*.
2.41	Deverá possuir regras de varredura avançadas que permitam especificar as condições que a regra se aplica às mensagens verificadas pela solução.
2.42	Deverá possuir as seguintes condições: • Tamanho da mensagem; • Assunto; • Corpo do e-mail; • Cabeçalho; • Conteúdo do anexo; • Nome e/ou Extensão: ○ .386, .ACM,.ASP,.AVP, .BAT,.CGI, .CHM,.CLA,.CLASS,.CMD, .CNV, .COM, .CS, .DLL, .DRV, .EXE, .HLP, .HTA, .HTM, .JS*, .LNK, .OCX, .OPO, .PHP, .PL. .SH, .SYS, .VBS, VBE, VXD, .WBS, .WIZ. WSH, .DOC, .DOCM, DOCX, .DOT, .DOTM, .DOTX, .DVB, .EML, .MD*, .PPA, .PPAM, .PPS, .PPSM, .PPSX, .PPT, .PPTM, .PPTX, XL,XLA, XLAM, .XLC, .XLK, XLL,.XLM, .XLR, .XLS, .XLSB, .XLSM, XLSX, .XLT, .XLTM, XLTX; MIME. • Content-type: vídeo, áudio, imagens, documentos e outros; • Tamanho do anexo; • Anexo protegido por senha: .7z, .ace, .arj, .docx, .pptx, .rar, .xlsx, .zip; • Quantidade de anexos; • Número de destinatários.
2.43	Deverá possuir ações através das regras permitindo definir o que acontecerá com as mensagens que atendem às condições dos critérios da regra: • Criptografar mensagem de e-mail; • Monitorar, permitindo os administradores o monitoramento das mensagens. As ações de monitoramento incluem o envio de uma mensagem de notificação para outras pessoas ou o envio de um cópia oculta (Cco) da mensagem para outras pessoas; • Bloqueio, deverá interceptar a mensagem, impedindo que ela atinja o destinatário original. As ações de bloqueio incluem excluir a mensagem inteira, colocar em quarentena e enviar para um destinatário diferente; • Modificar, permitindo alterar a mensagem e/ou seus anexos. As ações de modificação incluem limpeza de vírus que podem ser limpos, exclusão de anexos de mensagens, inserção de um carimbo no corpo da mensagem ou TAG de assunto.
2.44	Deverá possibilitar selecionar de todas as correspondências ou equivalentes para acionar a regra somente quando todos os critérios configurados selecionados fizerem correspondência.
2.45	Deverá possibilitar selecionar de qualquer correspondências ou equivalentes para acionar a regra quando qualquer critério configurado fizerem correspondência.
2.46	Deve ser possível criar políticas de *malwares*, *spam* e filtragem de conteúdo com: • Definição do destinatário, possibilitando selecionar domínios cadastrados, domínios específicos e grupos de usuários; • Especificação de endereços de remetente; • Exceções.
2.47	A solução deverá possibilitar importar e exportar os destinatários, remetentes e listas de exceções.
2.48	Deve ser possível criar políticas que executem ações em mensagens que contêm *malware*, *worms* ou outros códigos maliciosos.
2.49	Deve ser possível realizar a limpeza de *malwares* ou códigos maliciosos, onde o *malware* pode ser removido com segurança do conteúdo do arquivo infectado, resultando em uma cópia não infectada da mensagem ou anexo original.
2.50	Deverá possuir o serviço de banner para customização do portal com a logo.
2.51	Deverá possuir integração com o Active Directory ou com LDAP.
2.52	Deverá permitir o gerenciamento de múltiplos domínios.
2.53	Deverá permitir a integração com Microsoft Office 365, Google G-Suite, Zimbra e outros servidores de e-mail.
2.54	O uso das REST APIs deve permitir executar operações para no mínimo: criação, leitura, atualização e exclusão.
3	**Criptografia de e-mail**
3.1	Deverá ser capaz de criptografar e-mails baseado em políticas.
3.2	Deverá assegurar a comunicação através da utilização do protocolo TLS.
3.3	Deverá permitir a configuração da checagem do TLS.
3.4	Deverá suportar: TLS 1.0 e subsequentes.
4	**Rastreamento de e-mail e auditoria**

4.1	Deve permitir o rastreamento de mensagens de forma centralizada e por meio da interface de gerenciamento, não sendo aceito pesquisa via linha de comando.
4.2	Deverá possuir permitir o rastreamento de mensagens enviadas e recebidas.
4.3	Deverá possibilitar pesquisas de log de rastreamento de e-mail por até 30 dias.
4.4	Deverá fornecer buscas para rastreamento de e-mail por: período, direção do tráfego, remetente, destinatário, tipo (bloqueado/liberado), ação, assunto, ID da mensagem e *hash* do anexo SHA256.
4.5	Deverá possibilitar exportar a busca no formato .CSV.
4.6	Deverá permitir a consulta de eventos com os logs das políticas aplicadas por até 30 dias.
4.7	Deverá fornecer consulta de eventos com os logs das políticas por: período, direção do tráfego, remetente, destinatário, nome da regra, tipo de ameaça, anexo, BEC, conteúdo, DLP, *Graymail, ransomware, phishing, spam*, *malware, web reputation*, ID da mensagem e ação.
4.8	Deverá permitir rastrear os cliques de URL por até 30 dias.
4.9	Deverá fornecer permitir rastrear os cliques de URL por: data, direção do tráfego, remetente, destinatário, ID da mensagem, URL, ação e a hora em que um URL foi clicada.
4.10	Deverá ser possível consultar os logs de auditoria da console da solução por até 30 dias.
4.11	Deverá ser possível encaminhar os logs para *syslog*.
5	**Relatórios**
5.1	Deverá fornecer relatórios com base em uma programação diária, semanal, mensal e trimestral.
5.2	Os relatórios deverão ser, pelo menos, no formato PDF.
5.3	Deverá ser possível criar relatórios agendados e manuais.
5.4	Deverá possibilitar obter relatório sobre com resumo do tráfego de e-mail de todos os domínios e por domínio, detecções de ameaças, detecções de arquivos da *sandbox*, detecções de URL da *sandbox* e os principais destinatários comprometidos por e-mail (BEC).
6	**Notificações**
6.1	Deverá suportar notificação via e-mail.
6.2	Deverá possuir modelos de notificação pré-definidas para violação de políticas.
6.3	Deverá notificar quando o e-mail possuir um anexo compactado.
6.4	Deverá notificar quando o tamanho da mensagem excedido.
6.5	Deverá notificar quando uma regra for desencadeada.
6.6	Deverá notificar quando houver uma configuração de violação de segurança.
6.7	Deverá notificar quando um vírus ou spam for identificado.
7	**Prevenção contra vazamento de dados**
7.1	Deverá permitir gerenciar as mensagens de e-mail com dados confidenciais e proteger contra perda de dados, monitorando as mensagens de e-mail de saída.
7.2	Deverá possibilitar criar regras por expressões regulares, palavras chaves e atributos do arquivo.
7.3	Deverá possuir *templates* pré-definidos.
7.4	Deverá possuir *templates* customizados.
7.5	Deverá possuir uma base com no mínimo 200 modelos para criação de regras.
7.6	Deverá permitir a customização de modelos aderência a LGPD.
8	**Da quarentena**
8.1	Deverá permitir visualizar as mensagens quarentenadas por data, direção do tráfego, remetente, destinatários e conteúdo.
8.2	Deverá permitir o gerenciamento da quarentena para múltiplos domínios.
8.3	Deverá permitir a customização da notificação de quarentena pelo menos semanalmente, uma vez ou mais vezes durante o dia.
8.4	A notificação de quarentena deverá permitir a customização.
8.5	A notificação de quarentena deverá ser, no mínimo, em inglês e português.
8.6	A solução deverá possibilitar a gestão de quarentena de forma que seja possível que o administrador possa visualizar: a razão de um determinado bloqueio, o remetente, o destinatário, a data, o assunto, o IP do host de destino, a mensagem original, o tamanho da mensagem original.
8.7	Com base nos requisitos acima, deve ainda permitir as ações liberar e/ou excluir a mensagem.
8.8	A solução deverá permitir realizar o download da mensagem quarentenada.
8.9	Caso uma mensagem seja bloqueada ou rejeitada, a solução deverá informar também a razão do bloqueio e quais as regras foram ativadas.
8.10	Deverá possuir *single sign-on* (SSO) para a quarentena de usuário.
8.11	Deverá possibilitar utilizar duplo fator de autenticação.
8.12	Deverá possibilitar que usuário tome as seguintes ações ou similar em sua própria quarentena: • Excluir e bloquear o remetente: possibilitando excluir permanentemente a mensagem e adicionar o endereço aos remetentes bloqueados; • Excluir, possibilitando excluir permanentemente a mensagem; • Entregar e aprovar o remetente, permitindo liberar a mensagem da quarentena e adicionar o endereço aos remetentes aprovados, para que mensagens futuras de remetentes aprovados não sejam mantidas em quarentena; • Entregar, permitindo assim liberar a mensagem da quarentena.
8.13	Deverá possibilitar que o usuário criar listas remetentes aprovados e remetentes bloqueados.

Solução de segurança para ambiente de colaboração	
ID	**DESCRIÇÃO**
1	A solução deve permitir a identificação e proteção contra ameaças no Microsoft Office 365 (Exchange Online, Sharepoint Online, Onedrive for Business e Microsoft Teams), Gsuite e Zimbra.

2	Identificar e bloquear arquivos maliciosos carregados para o Google Drive, Onedrive, Zimbra, Sharepoint e Microsoft Teams. Por exemplo, se um usuário tentar carregar um determinado arquivo malicioso ou proibido em uma das plataformas citadas, a solução deve fazer o bloqueio.
3	Bloquear upload de arquivos por tipo definido em política para as soluções supracitadas.
4	Identificar e bloquear URLs maliciosas em arquivos e URLs, incluindo URLs dentro de anexos.
5	Realizar escaneamentos de ameaças em tempo real nos serviços integrados, identificando componentes maliciosos.
6	Permitir realizar escaneamento retroativo de ameaças (sob demanda), isto é, em busca de ameaças já armazenadas nas caixas de e-mail dos usuários ou em diretórios do Google Drive, Onedrive e Sharepoint.
7	O nível de sensibilidade das URLs maliciosas deve ser configurável através de políticas.
8	Deve possuir capacidade de cadastro dos usuários importantes para focar a análise de ataques de Comprometimento de E-mail (BEC).
9	Deve permitir que os administradores configurem a periodicidade das notificações para, no mínimo, URLs maliciosas identificadas, SPAMs maliciosos, *phishing*, *ransomware*, arquivos analisados na *sandbox* e identificados como baixo, médio e alto risco.
10	Identificar tentativas de comprometimento de e-mail baseado em uma análise dos estilos de escrita de cada usuário cadastrado como importante.
11	Deve permitir a visualização das estatísticas no dashboard por serviço integrado (Gmail, Google Drive, Exchange Online, Zimbra, Teams, Onedrive, Sharepoint) e alterar o período dos logs para, no mínimo, 24 horas, 7 dias e 30 dias.
12	Deve permitir a exibição da tendência para cada um dos tipos de serviço integrado em relação ao mesmo período anterior. Por exemplo, exibir aumento ou redução das ameaças no Exchange Online ou Zimbra nos últimos 30 dias, comparando com os 30 dias anteriores.
13	Deve ter a capacidade de analisar arquivos e URLs em *sandbox* para identificação de ameaças desconhecidas (sem assinatura).
14	Deve utilizar mecanismos de proteção que contemplem, pelo menos, malwares conhecidos por assinatura, malwares desconhecidos por *Machine Learning*, bloqueio de conteúdo (por tipo de arquivo, por exemplo), reputação de URLs.
15	A solução deve permitir compartilhamento de informações através de SIEM via API ou através da gerência centralizada.
16	A solução deve prover relatórios que contemplem, pelo menos, riscos de segurança (ameaças), *ransomware*, arquivos analisados em *sandbox*, auditoria e sobre a API.
17	Os relatórios devem ser exportáveis para, pelo menos, PDF.
18	Os relatórios devem ser enviados por e-mail, mediante configuração do administrador.
19	A verificação *anti-malware* deverá permitir a customização das ações a serem tomadas, por exemplo: quarentenar, deletar e passar.
20	Realizar integração nuvem-a-nuvem, através de API da Microsoft e Google.
21	As ações configuráveis nas políticas do serviço de e-mail devem contemplar, no mínimo, etiquetar a mensagem (inserir *tag*), quarentenar, deletar, ignorar e mover para lixeira.
22	Os demais serviços devem possuir ações pré-definidas e configuráveis para eliminar, quarentenar e ignorar os arquivos identificados.
23	Deve empregar o uso de análise em ambiente virtual (sandbox) do próprio fabricante para detecção de malwares avançados, com objetivo de diminuir seu risco de violação.
24	As políticas deverão ser aplicáveis por usuário ou grupo sincronizado da estrutura de serviço online (Microsoft ou Google).
25	Possuir um dashboard com as principais ameaças detectadas, a exemplo dos tipos *ransomware*, *phishing*, comprometimento de e-mail.
26	Deverá ser capaz de implementar políticas com base no filtro de conteúdo das mensagens.
27	Deverá ter a capacidade de compartilhar objetos suspeitos identificados através da análise em *sandbox* com a gerência centralizada do fabricante.
28	Cada política de serviço deve ser configurável para apenas monitorar ou tomar ação de proteção.
29	As notificações enviadas para o administrador e para os usuários devem ser customizáveis, permitindo tradução, inclusão ou exclusão de campos.
30	Deverá permitir a configuração dos níveis de detecção para SPAM.
31	Deverá permitir o administrador criar exceções para permitir ou bloquear determinados endereços de e-mail e URLs manualmente.
32	A solução deve possuir capacidade de ignorar e-mails já enviados para a lixeira do serviço de e-mail.
33	Deve permitir ao administrador bloquear mensagens de *graymail* por tipo (mensagens de marketing, notificações de fóruns e redes sociais, etc).
34	Os logs devem ser interativos, permitindo ao administrador montar consultas baseadas nos parâmetros como serviço detectado, tipo/categoria da ameaça, usuários afetados, política acionada, nome da ameaça, dentre outros.
35	Os resultados das consultas de logs deverão ter opção de salvar como um relatório exportável.
36	Deve permitir que o administrador realize buscas pontuais nos logs, a partir de parâmetros previamente definidos.
37	Deve possuir áreas de quarentena distintas para cada um dos serviços integrados, permitindo a restauração, download ou exclusão de arquivos/e-mails quarentenados pela política.
38	Deve permitir a criação de exceções para detecções por *Machine Learning* e por *Sandbox*.
39	Deve ter a capacidade de integração com serviços de autenticação para logon único (*single sign-on*) com, pelo menos, Okta, ADFS, Keycloak e Azure AD.
40	Deve possuir capacidade de configuração de contas de administração com permissões granulares por administrador, permitindo visualização ou controle total dos itens de menu.
41	Deve suportar a integração com serviço de gerenciamento de incidentes do próprio fabricante através da plataforma de investigação.
42	O recurso de detecção e resposta para e-mails deverá ser integrado à solução da Microsoft Office 365 ou Zimbra sem a necessidade de alterar configurações dos serviços de e-mail, ou configurações dos usuários.
43	Possuir modelos pré-definidos pelo fabricante de atividades suspeitas e/ou maliciosas para identificação e categorização de ameaças no ambiente.
44	A solução deve ser capaz de associar diferentes modelos de ameaças e associá-los a um único incidente/evento.
45	Deve ter capacidade de apresentar informações relacionadas ao MITRE para cada um dos eventos detectados no ambiente, caso possuam.
46	Utilizar bases de inteligência de ameaças integrando relatórios de inteligência do fabricante e de terceiros para ajudar a identificar ameaças no ambiente.
47	Em caso de ameaça avançada por e-mail, a solução deve permitir tomar diferentes ações de resposta no ambiente, contemplando, no mínimo.
48	Deve permitir adicionar o remetente (*sender*) de um e-mail na lista de bloqueio, impedindo o mesmo de enviar novos e-mails os usuários internos.

49	Deve mover o e-mail selecionado para a área de quarentena de um específico usuário ou todos os usuários que contenham este e-mail em suas caixas.
50	Deve deletar o e-mail selecionado das caixas selecionadas.

Solução de segurança para containers	
ID	**DESCRIÇÃO**
1	**Módulo de proteção contínua e automatizada de imagens de containers no pipeline**
1.1	A solução deverá utilizar sensores para escanear imagens de container localizadas no datacenter *on-premises* e em nuvem.
1.2	A console de gerenciamento deve ter suporte a múltiplo fator de autenticação (MFA).
1.3	Deverá escanear imagens e containers durante a fase de desenvolvimento, no processo *deploy*, após o *deploy* e em tempo de execução.
1.4	Durante a fase de desenvolvimento a solução deve ter a capacidade de identificar vulnerabilidades, códigos maliciosos, chaves privadas e segredos, além de violação de conformidade, antes da imagem ir para a produção.
1.5	Na fase de *deployment* a solução deverá ter a capacidade de controle de admissão baseado em políticas, o qual deverá bloquear imagens que estejam fora do padrão definido pela organização.
1.6	Durante a execução em produção, a solução deverá ser capaz de fazer uma verificação contínua da conformidade e das regras aplicadas na fase de admissão.
1.7	A solução deve detectar tanto ameaças instaladas via gerenciador de pacote quanto aplicações instaladas diretamente.
1.8	Os escaneamentos realizados pelos sensores locais (*on-premises*) devem ser enviados para a plataforma centralizada para fins de reporte e correlação.
1.9	Quando em execução, os containers deverão ser monitorados por ações que violem as regras pré-definidas e mapeadas no framework MITRE ATT&CK, focado em técnicas para containers.
1.10	Em caso de violação da política durante a execução, a solução deverá permitir isolar ou encerrar o *pod* em questão;
1.11	A solução deve ser compatível com soluções de cluster *Kubernetes* em nuvem, incluindo: *Amazon Kubernetes Service* (EKS), *Google Kubernetes Engine* (GKE) e *Azure Kubernetes Service* (AKS);
1.12	Deverá ter compatibilidade com *Kubernetes* 1.14 ou superior (incluindo *OpenShift*).
1.13	As políticas devem ser segmentadas de acordo com a fase de desenvolvimento, contemplando ao menos: desenvolvimento, verificação contínua e tempo de execução.
1.14	Durante a fase de implantação, a solução deve permitir apenas monitorar as atividades dos containers e, caso o administrador deseje, a solução deve permitir realizar bloqueio da ação e isolamento do *pod*, de acordo com a fase;
1.15	A solução deve exibir os eventos que ocorreram nos containers, contemplando ao menos: ação, data/hora, cluster, política e regra que gerou o evento, severidade, nome da imagem do container, nome do *pod*;
1.16	Deve ter a capacidade de criar regras de proteção e *compliance* baseadas nas propriedades do *pod*, da imagem e do container, baseadas resultados do escaneamento da imagem e acesso ao *kubectl*;
1.17	A solução deve permitir criar exceções para as regras.
1.18	As regras de proteção devem incluir, no mínimo: • Containers que executam com permissão de root; • Containers com permissão para escalar privilégios; • Containers que podem escrever em sistemas de arquivos root; • Imagens de container com malware; • Imagens de container com vulnerabilidades.
1.19	A solução para proteção de containers em tempo de execução, deve ser compatível com os seguintes sistemas: • Amazon Linux 2 4.14.x, 5.4.x e 5.10.x; • RHCOS 4.18.x; • Ubuntu 4.15.x (generic), 5.4.x (generic, aws, azure e GKE), 5.11.x (generic, azure e aws); • Google Container-Optimized OS (COS) 5.4.x e 5.10.x; • Debian 5.10.x (generic).
2	**Sensor de escaneamento de imagens**
2.1	O sensor deve ser implantado como uma arquitetura de microsserviços.
2.2	Deve ser integrado na esteira de desenvolvimento da organização para analisar imagens de containers antes que elas possam ir para a produção.
2.3	Deve ser compatível com pelo menos as seguintes distribuições: RHEL, CentOS, Oracle Linux, Ubuntu, Debian, Alpine e Amazon Linux (2018 e 2).
2.4	Deve suportar a varredura de imagens do Docker em qualquer registro que suporte a API do Docker Registry V2.
2.5	A integração via registro deve ser compatível com: Docker Trusted Registry (DTR), Google Container Registry (GCR), Amazon Elastic Container Registry (ECR), Azure Container Registry (ACR), VMware Harbor, jFrog Artifactory, Sonatype Nexus e Quay Container Registry.
2.6	O console de gerenciamento do sensor deve oferecer suporte à implantação no Kubernetes 1.10.0 ou superior em uma plataforma certificada Kubernetes (ou equivalente como Red Hat Openshift).
2.7	A solução deve ter na API um recurso de webhook que permita que os componentes de CI / CD se registrem para receber notificações de eventos de verificação, incluindo 'verificação concluída', permitindo automatizar fluxos de trabalho.
2.8	Deve possuir APIs com o detalhamento das funções que podem ser utilizadas para a integração da solução com softwares de terceiros.
2.9	Deve possuir console de gerenciamento local no host, via linha de comando, que inclua a possibilidade de iniciar a varredura de contêiner.
2.10	O sensor deve possuir compatibilidade com banco de dados externo, incluindo PostgreSQL 9.6, Oracle 11 e subsequentes.
2.11	Deve realizar escaneamento de maneira automática no momento do build da imagem e sob demanda.
2.12	Os resultados dos escaneamentos realizados pelos sensores devem ser enviados para console centralizada na nuvem para serem utilizados como objetos para as políticas e regras.

2.13	O sensor deve detectar *malware* e apresentar indicador de existência de *malware*, incluindo nome e localização do arquivo.
2.14	Detectar segredos e chaves incorporados nas imagens.
2.15	Permitir realizar consultas de verificação personalizadas para encontrar arquivos suspeitos ou indesejados.
2.16	Deve analisar o conteúdo da imagem *docker* baseado em uma lista de verificação de conformidade que inclua itens do PCI-DSS, HIPAA e NIST 800-190.
2.17	As vulnerabilidades encontradas em cada varredura devem fornecer no mínimo as gravidades: Baixa, Média e Alta.
2.18	solução deve ter a capacidade de criar regras manuais, além das regras internas fornecidas pela solução, incluindo o formato YARA.
2.19	Identificar vulnerabilidades na aplicação em execução nos serviços de Container em Kubernetes através dos seguintes Cloud Service Providers: Amazon Web Services (EKS), Microsoft Azure (AKS) e Google Cloud Platform (GKS).
2.20	Detalhamento do CVE e o risco de exposição da aplicação da imagem.
2.21	Identificar a imagem com a vulnerabilidade podendo tomar uma ação de bloqueio da mesma.

Solução de segurança para *mobile*	
ID	**DESCRIÇÃO**
1	**Dispositivos móveis iOS**
1.1	Deve ser compatível com os sistemas operacionais iOS 6.x e subsequentes.
2	**Dispositivos móveis Android**
2.1	Deve ser compatível com os sistemas operacionais Android 4 e subsequentes.
3	**Características gerais**
3.1	Deve ter gerenciamento centralizado.
3.2	Deve ter proteção avançada: • contra *malwares*; • contra aplicativos e sites maliciosos; • *phishing;* • vulnerabilidades de Wi-fi; • ataques conhecidos.
3.3	Deve notificar SO desatualizado.
3.4	Deve mapear vulnerabilidades do SO.
3.5	Deve possuir integração com soluções de gerenciamento de dispositivos móveis: • VMWare Workspace One; • Google Workspace Endpoint Management.
3.6	Deve possuir recursos de segurança avançada e capacidades de gerenciamento, tais como: • gerenciamento de risco de superfície de ataque; • Zero Trust Secure Access; • diretor de dispositivos móveis.

Gerenciamento de risco e superfície de ataque	
ID	**DESCRIÇÃO**
1	Deve exibir os 10 principais dispositivos com alto nível de risco na organização
2	Deve exibir os 10 principais usuários com alto nível de risco na organização.
3	Deve categorizar o índice de risco da organização, levando em consideração fatores de risco e indicadores específicos que afetam a rede.
4	Deve exibir as principais vulnerabilidades da organização, com base na pontuação de impacto ou no potencial global de exploração, e os ativos específicos que são afetados
5	Deve exibir o número total de alertas acionados nos últimos 7 dias e o nível de severidade dos modelos que acionaram os alertas.
6	Deve exibir os 20 principais *endpoints* que registraram mais detecções de filtro nos últimos 7 dias.
7	Deve proporcionar visibilidade completa de todos os ativos da organização, incluindo identidades, dispositivos, aplicações, APIs, dados e *shadow IT.*
8	Deve correlacionar a criticidade dos ativos, severidade de vulnerabilidades e atividade de ameaças para fornecer uma gestão de riscos baseada em contexto, dinâmicas e em tempo real.
9	Deve utilizar tecnologias de Inteligência Artificial e Machine Learning para automatizar respostas a ameaças.
10	Deve se integrar em ambientes de nuvem.
11	Deve permitir prever, visualizar e evitar explorações potenciais para prevenção de ataques.

6. DEMAIS REQUISITOS NECESSÁRIOS E SUFICIENTES À ESCOLHA DA SOLUÇÃO DE TIC

6.1. Requisitos de projeto e de implementação

CONTRATADA elaborará um plano de implantação e operação da solução caso seja necessário a alteração do licenciamento devido à atualização ou melhorias a serem realizadas nas configurações da solução, contendo, pelo menos:

- Cronograma de atividades;
- Lista de verificação de atividades/fases da execução dos serviços;
- Detalhamento das atividades a serem realizadas, contendo comandos, manuais de operação, guias do fabricante ou quaisquer documentações necessárias para a correta execução; e
- Plano de *rollback*.

A CONTRATADA deverá realizar todas as atividades necessárias à instalação, configuração e testes de funcionamento da solução, respeitando o horário de funcionamento da CONTRATANTE.

A critério da CONTRATANTE, as atividades necessárias à instalação, configuração e testes da solução poderão ser agendadas para os finais de semana e/ou fora do horário comercial.

A equipe técnica da CONTRATADA será acompanhada pelo(s) responsável(eis) técnico(s) da CONTRATANTE nas atividades necessárias à instalação, configuração e testes de solução.

A CONTRATANTE poderá determinar alterações no projeto e/ou no cronograma de implantação, desde que não implique custos adicionais à CONTRATADA.

A CONTRATADA deverá respeitar os requisitos técnicos e as informações sobre o ambiente computacional fornecidas pela CONTRATANTE, sendo de sua responsabilidade a correção de eventuais inconformidades, mesmo que a título oneroso e sem qualquer custo à CONTRATANTE.

A CONTRATANTE poderá realizar, a seu critério, reuniões técnicas e gerenciais com a CONTRATADA para alinhamento de expectativas e para definição/revisão de configurações.

A CONTRATADA deverá, sempre que solicitado, providenciar o registro das reuniões, contemplando os acertos e as definições estabelecidas em comum acordo com a CONTRATANTE. Toda a documentação originada a partir das reuniões técnicas, caso solicitado pela CONTRATANTE, deverá ser fornecida ao CNPq, via Sistema Eletrônico de Informações (SEI) ou outro meio indicado pela CONTRATANTE.

Ao final das etapas de implantação e testes da solução, a CONTRATADA deverá entregar relatório de conclusão contendo todas as informações relativas à implantação e testes da solução, de forma a comprovar o atendimento aos requisitos técnicos definidos no Termo de Referência, que deverá ser aprovado pela CONTRATANTE.

6.2. Requisitos de implantação

A CONTRATADA deverá providenciar a instalação da solução, a qual deve ocorrer em, no máximo, 15 (quinze) dias corridos após a emissão da autorização para instalação/configuração.

A autorização para instalação poderá ser emitida para cada componente da solução individualmente, sendo que cada autorização terá seu prazo diferenciado.

A contratada deverá disponibilizar 1 (um) técnico, certificado na solução para instalação e configuração do produto no ambiente do CNPq.

A CONTRATADA deverá elaborar um projeto executivo, contendo as fases de execução dos serviços com a especificação de cada fase, incluindo o cronograma dos serviços a serem realizados com respectivos prazos e datas.

A instalação deverá ser realizada em máquinas disponibilizadas pela CONTRATANTE, com infraestrutura de armazenamento em Storage, e deve garantir a alta disponibilidade da solução. Os recursos de hardware e sistema operacional para a instalação serão fornecidos pelo CONTRATANTE.

A instalação deverá contemplar as seguintes fases:

- avaliação da estrutura operacional para definir questões de funcionamento e desempenho da solução;
- adequação do sistema operacional conforme requisitos da aplicação;
- instalação do software em sua última versão disponível no momento da instalação, contemplando todas as funcionalidades disponíveis no produto, configurado para alta disponibilidade;
- configuração de domínios, classes de serviços, gerenciamento hierárquico de armazenamento, *backup* e *restore* sem necessidade de parada do serviço, serviços de monitoramento via SNMP, listas de controle de acesso, e customização da interface web com o logotipo do CONTRATANTE, além de outras que o corpo técnico de informática da CONTRATANTE, de comum acordo com a CONTRATADA, possa vir a definir, respeitando as limitações técnicas do ambiente disponibilizado;
- migração de todos os dados e configurações dos usuários, hoje instalados na solução de e-mail para o novo ambiente, sem qualquer prejuízo para os usuários;
- fornecimento de documentação contendo informações detalhadas sobre todo o ambiente, procedimentos realizados no processo de instalação, descrição de todas as políticas adotadas (classe de serviço, HSM, backup etc.), procedimentos de backup e *disaster recovery*;
- todo o processo da instalação deve ser realizado na sede da CONTRATANTE, por técnicos certificados pelo fabricante da solução.

6.3. Requisitos de garantia

O prazo de garantia contratual da solução, complementar à garantia legal, é de, no mínimo, 24 (vinte e quatro) meses, contado a partir do primeiro dia útil subsequente à data do recebimento definitivo do objeto.

A garantia será prestada com vistas a manter o sistema de antivírus e o antispam em perfeitas condições de uso com todas as licenças, configuradas e operantes, sem qualquer ônus ou custo adicional para a CONTRATANTE.

A garantia abrange a realização de configuração, instalação, atualização entre outros da solução, a ser realizado pela CONTRATADA, ou, se for ocaso, de acordo com as normas técnicas específicas.

Uma vez notificada, a CONTRATADA realizará a reparação ou reconfiguração da solução no prazo especificado nos *Requisitos Temporais*, contados a partir da data de abertura de chamado pela CONTRATANTE.

O prazo indicado no subitem anterior, durante seu transcurso, poderá ser prorrogado uma única vez, por igual período, mediante solicitação escrita e justificada da CONTRATADA, aceita pela CONTRATANTE.

Caso o prazo da garantia oferecida pelo fabricante seja inferior ao estabelecido nesta cláusula, o fornecedor deverá complementar a garantia do bem ofertado pelo período restante.

A garantia do fabricante dos produtos fornecidos deve obrigatoriamente prover:

- atualização das versões dos softwares fornecidos, se novas versões forem disponibilizadas;

- atualização dos softwares fornecidos se houver lançamento de novos softwares em substituição aos fornecidos, ou mesmo não sendo uma substituição, se ficar caracterizada uma descontinuidade dos softwares fornecidos;
- acesso aos engenheiros do fabricante na modalidade de 24 (vinte e quatro) horas por dia e 7 (sete) dias por semana, durante o período contratado;
- garantia de prioridade de atendimento na fila de chamados na central de suporte do fabricante;
- gerente do fabricante dedicado para assuntos de incidentes.
    - este profissional deve ser apresentado pela CONTRATADA à CONTRATANTE no início da prestação dos serviços;
    - este profissional deverá realizar no mínimo 04 (quatro) visitas por ano de garantia para revisão do ambiente ou resolução de problemas técnicos.
- envio de alertas preventivos durante o período do contrato.
- A CONTRATADA deverá garantir o funcionamento das consoles de gerenciamento e atualização (inclusive na instalação ou atualização de versões/*releases*) ou problemas de incompatibilidade com outros softwares da CONTRATANTE.
    - os serviços de console de gerenciamento deverão estar disponíveis 90% no mês.
- A CONTRATADA deverá reinstalar ou substituir qualquer módulo da solução de antivírus por outro novo, no prazo de 5 (cinco) dias úteis, contados do recebimento de carta emitida pela CONTRATANTE, se:
    - ocorrerem 4 (quatro) ou mais defeitos que comprometam o seu uso normal, dentro de qualquer período de 30 (trinta) dias, ou;
    - a soma do tempo de paralisação do módulo ultrapassar 20 (vinte) horas, dentro de qualquer período de 30 (trinta) dias.

6.4. Requisitos de suporte e manutenção

A CONTRATADA deverá acompanhar e ajustar os seguintes itens na atividade de monitoramento:

- administração das configurações da solução oferecida;
- desempenho da solução.

A CONTRATADA deverá emitir, no mínimo, mensalmente, os seguintes relatórios:

- relatório de remoção de ameaças;
- recomendações de ajustes de configuração;
- vírus detectados;
- top 10 vírus detectados;
- vírus agrupado por dia;
- total de arquivos verificados;
- quantidade de arquivos bloqueados;
- quantidade de vírus identificados;
- quantidade de *phishing* identificados;
- quantidade de falsos positivos identificados;
- tentativas de ataques;
- detalhamento das ameaças encontradas;
- usuários que mais recebem e enviam códigos maliciosos;
- amostragem de ameaças identificadas;
- tipos de ações tomadas.

A CONTRATADA deverá prestar serviços de natureza continuada de suporte técnico *on-site* ou remotamente 24x7 em Brasília/DF relativos à prestação dos serviços de segurança das ferramentas implantadas, sem ônus para a CONTRATANTE, o qual será acionado por meio de abertura de chamados pela CONTRATANTE.

A CONTRATADA deverá disponibilizar para a CONTRATANTE uma Central de Atendimento (sítio na Internet, mensagem eletrônica e telefone) para consultas, aberturas de chamados técnicos e envio de arquivos para análise 24x7 durante a vigência do contrato.

A CONTRATADA deverá cumprir prazos máximos para resposta aos acionamentos, de acordo com o nível de severidade de cada chamado, conforme quadros a seguir:

Níveis de severidade dos chamados

Categoria	Nível	Descrição
Urgente	1	Serviços totalmente indisponíveis. Falha comprometendo um ou mais serviços em produção ou que deixe indisponíveis os recursos do mesmo. Impacto a múltiplos usuários e/ou falha em servidor de produção que afete as operações críticas do CNPq.
Crítico	2	Serviços parcialmente indisponíveis ou com degradação de tempo de resposta no acesso aos aplicativos. Intermitente em serviços suportados que torne o ambiente inoperante. Impacto individual ou a pequenos grupos. Operação normal afetada, mas sem interrupção.
Não Crítico	3	Serviços disponíveis com ocorrência de alarmes de avisos, consulta sobre problemas, dúvidas gerais sobre a ferramenta de segurança. Manutenção e monitoramento de eventos de falhas ou de avisos relatados pelo cliente. Pequeno impacto a um ou mais usuários. A correção pode ser feita de forma agendada, em um momento futuro.

O nível de severidade será informado pela CONTRATANTE no momento da abertura de cada chamado.

O nível severidade poderá ser reclassificado a critério da CONTRATANTE. Caso isso ocorra haverá o início de nova contagem de prazo, conforme o novo nível de severidade.

Todas as solicitações de suporte técnico devem ser registradas pela CONTRATADA para acompanhamento e controle da execução do serviço descrito no item *Requisitos temporais.*

Para a execução de atendimento é necessário a autorização da CONTRATANTE para instalação ou desinstalação de quaisquer softwares ou equipamentos que não façam parte da solução antivírus CONTRATADA.

Em caso de interrupção ou indisponibilidade do serviço, a CONTRATADA se compromete a realizar as correções necessárias a reativação do serviço e à prevenção de novas interrupções, respeitados os prazos de atendimento.

Entende-se por interrupção ou indisponibilidade dos serviços de antivírus quando os ativos de TI protegidos não puderem ser atualizados devido a problemas de responsabilidade da CONTRATADA ou quando os servidores de atualização estiverem indisponíveis.

6.5. Requisitos de capacitação

Os treinamentos deverão ser realizados e concluídos para até 2 (dois) servidores do CNPq, dentro de prazo máximo de 120 (cento e vinte) dias.

A CONTRATADA deverá fornecer treinamento específico sobre a instalação, operação, configuração e uso do console de gerenciamento, de caráter teórico e prático, da solução de segurança contratadas para 2 (dois) servidores da CONTRATANTE, em Brasília/DF.

O treinamento deverá ser sem custo adicional ao preço formulado em sua proposta, incluindo o material didático oficial.

O programa para o treinamento deverá ser previamente aprovado pela CONTRATANTE e eventuais mudanças de conteúdo solicitadas deverão constar no material didático.

No caso do treinamento fornecido não ser satisfatório, mediante avaliação tempestiva e fundamentada, tanto em relação à qualidade ou à carga horária efetiva, a CONTRATADA deverá realizar novo treinamento sem ônus adicional à CONTRATANTE.

Deverá ser emitido certificado de participação ao final do curso.

O escopo deste plano de treinamento para instalação, operação e configuração deve prever:

- informativo global dos componentes tecnológicos envolvidos na prestação dos serviços contratados;
- compreensão geral da filosofia de funcionamento e de operação da solução adotada;
- conhecimento e usabilidade dos recursos (hardwares e softwares) envolvidos;
- funcionalidades do sistema em seus respectivos módulos.

O plano de treinamento deve prever, para cada tema, a carga horária, recursos e condições imprescindíveis para o perfeito aproveitamento do treinamento incluindo a documentação didática a ser utilizada.

Os instrutores ou responsáveis pelos treinamentos, certificados pelo fabricante, são de responsabilidade da CONTRATADA e estes devem apresentar ao CNPq as respectivas agendas de treinamento.

Todo o material de apoio técnico necessário à realização dos treinamentos em ambiente da CONTRATADA, tais como os equipamentos, acessórios, ferramentas, etc. devem ser providos pela CONTRATADA em quantidade suficiente para permitir adequado aprendizado pelos treinados.

6.5. Requisitos legais

- Constituição Federal;
- Lei n.º 14.133, de 1º de abril de 2021;
- Portaria SGD/MGI n.º 5.950, de 26 de outubro de 2023;
- Instrução Normativa SGD/ME n.º 94, de 23 de dezembro de 2022;
- Instrução Normativa SEGES/ME n.º 65, de 7 de julho de 2021;
- Lei n.º 13.709, de 14 de agosto de 2018;
- Lei nº 8.248, de 23 de outubro de 1991;
- Decreto n.º 11.260, de 22 de novembro de 2022;
- Decreto n.º 9.637, de 26 de dezembro de 2018;
- Decreto nº 7.174, de 12 de maio de 2010;
- Decreto n.º 7.579/2011, de 11 outubro de 2011.

6.6. Requisitos temporais

Os serviços contratados deverão ser prestados pelo período de 24 (vinte e quatro) meses, prorrogáveis por até 10 anos, de acordo com os artigos 106 e 107 da Lei nº 14.133. A justificativa para este período em vez de 12 (doze) meses é que as licitantes podem oferecer descontos ou condições financeiras mais favoráveis, o CNPq poderá ter acesso contínuo à solução sem interrupções frequentes para renovação, fortalecimento do relacionamento com o fornecedor, continuidade do negócio diante da criticidade da solução, além do menor esforço administrativo para procedimento de renovação contratual.

O prazo para a entrega dos itens é de 30 (dias) dias corridos, prorrogável por igual período, mediante aprovação da CONTRATANTE, após emissão da Ordem de Serviço.

Os componentes das soluções serão recebidos provisoriamente no prazo de até 15 (quinze) dias corridos, pelo(a) responsável pelo acompanhamento e fiscalização do contrato, para efeito de posterior verificação de sua conformidade com as especificações constantes neste Termo de Referência e na proposta.

Os componentes das soluções poderão ser rejeitados, no todo ou em parte, quando em desacordo com as especificações constantes neste Termo de Referência e na proposta, devendo ser substituídos no prazo de 30 (trinta) dias corridos, a contar da notificação à CONTRATADA, às suas custas, sem prejuízo da aplicação das penalidades.

Os componentes das soluções serão recebidos definitivamente no prazo de até 15 (quinze) dias corridos, contados do recebimento provisório, após a verificação de sua conformidade com as especificações constantes neste Termo de Referência e na proposta.

Na hipótese da verificação a que se refere o subitem anterior não ser procedida dentro do prazo fixado, reputar-se-á como realizada, consumando-se o recebimento definitivo no dia do esgotamento do prazo, exceto no caso de não conformidade dos itens fornecidos com as especificações constantes no Termo de Referência e na proposta.

O recebimento provisório ou definitivo do objeto não exclui a responsabilidade da CONTRATADA pelos prejuízos resultantes da incorreta execução do contrato.

Os serviços de console de gerenciamento deverão estar disponíveis 90% no mês.

A CONTRATADA deverá reinstalar ou substituir qualquer módulo da solução de antivírus por outro novo, no prazo de 5 (cinco) dias úteis, contados do recebimento de carta emitida pela CONTRATANTE, se:

- ocorrerem 4 (quatro) ou mais defeitos que comprometam o seu uso normal, dentro de qualquer período de 30 (trinta) dias, ou;
- a soma do tempo de paralisação do módulo ultrapassar 20 (vinte) horas, dentro de qualquer período de 30 (trinta) dias.

A solução da CONTRATADA deverá garantir a detecção e remoção programas maliciosos como *spyware*, programas de propaganda, ferramentas como *password crackers*, etc., para os servidores e para os desktops, de forma automática, em pelo menos 90,00% (noventa por cento) dos casos. Para os casos em que a solução não remova a infecção automaticamente, a CONTRATADA continua responsável pela remoção das infecções remanescentes, devendo a CNPq indicar o prazo para a solução do problema.

A solução da CONTRATADA deverá garantir a atualização automática das assinaturas de antivírus em pelo menos 90% (noventa por cento) das estações e servidores ativos e disponíveis na rede em até no máximo 24 (vinte e quatro) horas após o recebimento desta pelo servidor de antivírus. Para os casos em que a solução não atualize automaticamente as assinaturas de antivírus, a CONTRATADA continua responsável pelas atualizações remanescentes, devendo ao CNPq indicar o prazo para a solução do problema.

A solução da CONTRATADA deverá evitar a proliferação programas maliciosos, programas de propaganda, ferramentas como *password crackers* etc., de forma a evitar epidemias (*outbreaks*).

Os atendimentos de suporte técnico prestados à CONTRATANTE deverão pautar-se pelas instruções abaixo:

- caso seja on-site, o atendimento deverá ser provido na sede do 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.
- A CONTRATADA deverá cumprir prazos máximos para resposta aos acionamentos, de acordo com o nível de severidade de cada chamado, conforme quadros abaixo:

Modalidade	Prazos de atendimento	Níveis de severidade		
		Urgente	Crítico	Não crítico
On-site, remoto, e-mail ou telefone	Início	1 hora	2 horas	24 horas
	Término	2 horas	4 horas	72 horas

6.7. Requisitos Sociais, Ambientais e Culturais

O atendimento aos chamados de assistência técnica, por qualquer meio de comunicação, deverão ser efetuados em língua portuguesa.

As pessoas envolvidas na execução das atividades deverão, durante sua permanência dentro das instalações do CNPq, se adequar às regras, costumes e normas internas que definem a conduta profissional e pessoal de servidores, colaboradores e visitantes da instituição.

Os profissionais deverão utilizar crachá de identificação ou documento de igual equivalência.

A CONTRATADA deverá observar o disposto na IN SLTI/MPOG nº 01/2010, de 19 de janeiro de 2010, referente à sustentabilidade ambiental.

O descumprimento de normas ambientais constatadas durante a execução do contrato será comunicado pelo CNPq ao órgão de fiscalização do Distrito Federal ou da União.

6.8. Requisitos de Segurança e Segurança da Informação e Privacidade

A CONTRATADA deverá manter sob sigilo as informações e comunicações de que tiver conhecimento, abstendo-se de divulgá-las, garantindo o sigilo e a inviolabilidade dos dados trafegados por meio dos enlaces eventualmente utilizados na execução das atividades, respeitando as hipóteses e condições constitucionais e legais de quebra de sigilo de telecomunicações.

A CONTRATADA deverá atender ao disposto na Política de Segurança da Informação do CNPq (POSIN), em suas normas integrantes e os profissionais que tiverem acesso ao ambiente computacional da instituição, deverão assinar o Termos de Responsabilidade e Sigilo.

Compete à CONTRATANTE dar ciência à CONTRATADA da POSIN e demais normas do CNPq.

A CONTRATADA não poderá armazenar consigo qualquer documento técnico que contemple configurações aplicadas nos equipamentos implantados na rede da CONTRATANTE.

A CONTRATADA deverá informar à CONTRATANTE todas as senhas utilizadas para a configuração dos equipamentos, as quais deverão ser alteradas pela CONTRATANTE com o apoio técnico da CONTRATADA, logo após o encerramento do contrato ou sempre que a CONTRATANTE julgar necessário.

A CONTRATADA deverá prover segurança de acesso físico e lógico aos recursos da CONTRATANTE que estiverem sob sua guarda.

Os recursos de TI não poderão ser utilizados pela CONTRATADA ou seus prepostos para realização de atividades alheias aos serviços previstos ou englobados nesta contratação.

A CONTRATADA deverá guardar sigilo sobre dados e informações obtidos em razão da execução dos serviços contratados ou da relação contratual mantida com o CNPq, abstendo-se de divulgá-los a terceiros sob qualquer pretexto, a menos que prévia e formalmente autorizada pela CONTRATANTE.

Todos os perfis de acesso e caixas postais eventualmente concedidos à CONTRATADA deverão ser imediatamente excluídos após o término do contrato.

A CONTRATANTE terá propriedade sobre todos os documentos e procedimentos operacionais produzidos no escopo da presente contratação.

A CONTRATADA deverá respeitar as normas de segurança estabelecidas pela CONTRATANTE durante a realização de atividades no ambiente desta. Essa sujeição não caracteriza qualquer vínculo empregatício com a CONTRATANTE.

Deverão ser adotadas as versões mais recentes dos softwares básicos do ambiente da CONTRATANTE.

6.9. Requisitos de reunião inicial

Deverá ser realizada uma reunião inicial com o objetivo de identificar as expectativas, nivelar os entendimentos acerca das condições estabelecidas no Contrato, Termo de Referência e seus Anexos e esclarecer possíveis dúvidas acerca da execução dos serviços.

Deverão participar dessa reunião, no mínimo, o Gestor e os Fiscais do contrato, membro(s) da equipe técnica da CONTRATANTE e o Preposto da CONTRATADA.

A reunião realizar-se-á na sede do CNPq em até 10 (dez) dias úteis após a assinatura do Contrato.

6.10. Requisitos de Arquitetura Tecnológica

Os serviços deverão ser executados observando-se as diretrizes de arquitetura tecnológica estabelecidas pela área técnica da CONTRATANTE.

A adoção de tecnologia ou arquitetura diversa deverá ser autorizada previamente pela CONTRATANTE. Caso não seja autorizada, é vedado à CONTRATADA adotar arquitetura, componentes ou tecnologias diferentes daquelas definidas pela CONTRATANTE.

6.11. Requisitos de Experiência Profissional

Os serviços de assistência técnica, suporte, garantia deverão ser prestados por técnicos devidamente capacitados nos produtos em questão, bem como com todos os recursos ferramentais necessários para a prestação dos serviços.

Para a prestação dos serviços de suporte técnico, garantia, atualização, implantação, configuração e treinamento das soluções de segurança, os profissionais da CONTRATADA deverão dispor de certificados expedidos pelo fabricante ou parceiros credenciados.

6.12. Requisitos de Formação da Equipe

A CONTRATADA deverá designar um responsável para contato direto com o CNPq, sem custo adicional para a CONTRATANTE. Além de ser o ponto focal da comunicação da CONTRATANTE, ele deverá assumir as responsabilidades da CONTRATADA perante o CNPq.

A CONTRATADA deverá indicar um substituto para o preposto que, na ausência deste, deverá assumir integralmente todas as responsabilidades perante à CONTRATANTE.

6.13. Requisitos de Metodologia de Trabalho

A execução dos serviços está condicionada ao recebimento pelo CONTRATADO de Ordem de Serviço (OS) emitida pela CONTRATANTE.

A OS indicará o serviço, a quantidade e a localidade na qual os deverão ser prestados.

O CONTRATADO deve fornecer meios para contato e registro de ocorrências.

A execução do serviço dever ser acompanhada pelo CONTRATADO, que dará ciência de eventuais acontecimentos à CONTRATANTE.

O fornecimento das licenças será feito por meio digital, conforme quantidade e tipos de licenças constantes em Ordem de Serviço.

A CONTRATADA deverá realizar a implantação da solução nos sites principal e secundário do CNPq.

Tanto o serviço de instalação quanto o de treinamento deverão ser agendados previamente com a equipe do CNPq.

7. ESTIMATIVA DA DEMANDA - QUANTIDADE DE BENS E SERVIÇOS

7.1. Estimativa dos produtos/serviços

Diante das características e requisitos necessários para atendimento ao CNPq, tratam-se de soluções de segurança de *endpoints*, servidores de rede, antispam, ambiente de colaboração, mobile, ambiente de *containers* e gerenciamento de superfície de ataque, observando a Portaria SGD/MGI n.º 5.950/2023.

Tais produtos necessitam de atualização contínua, garantia, além de serviços de implantação e treinamento para as equipes de monitoramento e operação de infraestrutura do CNPq. Assevera-se que o suporte técnico especializado também é essencial para extrair o máximo proveito dos recursos contratados.

7.2. Quantitativo dos produtos/serviços

O quantitativo das soluções baseou-se nos seguintes critérios:

- Solução de segurança para *endpoints*: atualmente o CNPq conta com 1.200 desktops e notebooks.
- Solução de segurança para servidores físicos, virtuais e em nuvem: atualmente o CNPq conta com 500 servidores físicos, virtuais e nuvem em sua infraestrutura de TI.
- Soluções de segurança para e-mails (*antispam)* e segurança para ambiente de colaboração: atualmente o CNPq conta com 1.000 usuários ativos com caixa de e-mail. Cada usuário receberá uma licença. A projeção de 1.200 é uma estimativa visando a possibilidade de crescimento da quantidade de servidores e colaboradores do órgão.
- Solução de segurança para *containers*: atualmente o ambiente de produção e desenvolvimento de TI do CNPq conta com 8 *containers.* Estima-se que este quantitativo pode chegar a 10 conforme novos sistemas forem sendo disponibilizados ou evoluídos.
- Gerenciamento de risco e superfície de ataque: a contabilização desta solução é baseada na soma entre *endpoints*, servidores físicos, virtuais e nuvem. Logo, serão necessárias 1.700 licenças.
- Instalação/configuração das soluções: é composto por um único serviço que será realizado para todas as soluções contratadas.
- Suporte mensal, garantia e atualização: trata-se de um serviço mensal. Logo, o contrato tem a vigência de 24 meses e durante todo o período deverá ser prestado o suporte às soluções.
- Treinamento das soluções: estima-se que o treinamento deve englobar 2 servidores, sendo um titular e outro reserva.

Item	Solução	Unidade de medida	Quantidade
1	Solução de segurança para *endpoints*	Unidade	1200
2	Solução de segurança para servidores físicos, virtuais e em nuvem	Unidade	500
3	Solução de segurança para e-mails (*antispam*)	Unidade	1200
4	Solução de segurança para ambiente de colaboração	Unidade	1200

5	Solução de segurança para *containers*	Unidade	10
6	Solução de segurança para dispositivos *mobile*	Unidade	50
7	Gerenciamento de risco e superfície de ataque	Unidade	1700
8	Instalação/configuração das soluções	Unidade	1
9	Suporte mensal, garantia e atualização	Mês	24
10	Treinamento das soluções	Pessoa	2

8. LEVANTAMENTO DE SOLUÇÕES

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.

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, de forma a proporcionar a escolha da melhor solução.

Foram identificadas 4 (quatro) possíveis soluções para a segurança da informação, conforme descrição da tabela a seguir:

Cenário	Descrição
1	Renovação do licenciamento da solução de proteção de estações de trabalho, servidores e dispositivos móveis já adquirida.
2	Solução existente no Portal de Software Público Brasileiro.
3	Manter a solução atual sem garantia e sem suporte.
4	Contratação de nova solução para proteção dos *endpoints*, servidores, *mobiles*, *containers,* ambiente de colaboração e gerenciamento de risco e superfície de ataque.

8.1. PMC-TIC

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

A proteção física e lógica da informação deve ser provida por ferramentas especializadas, seguras, consolidadas e, acima de tudo, que preservem a confidencialidade, a integridade e a disponibilidade da informação.

A análise comparativa de soluções, nos termos do inc. II do art. 11 da IN SGD/ME nº 94, de 23 de dezembro de 2022, visa a elencar as alternativas de atendimento à demanda considerando, além do aspecto econômico, os aspectos qualitativos em termos de benefícios para o alcance dos objetivos da contratação.

Conforme art. 14, II, c da IN SGD/ME n.º 94/2022, foram levantadas alternativas para a contratação de certificados digitais conforme apresenta-se a seguir:

9.1. Cenário 1 - Renovação do licenciamento da solução de proteção de estações de trabalho, servidores e dispositivos móveis já adquirida.

A primeira alternativa em avaliação envolve a renovação da solução de *endpoints* e servidores com a fabricante *Trend Micro,* visando preservar o investimento já realizado pelo CNPq por meio da renovação das licenças das ferramentas já adquiridas.

O CNPq vem utilizando, com sucesso, por mais de 10 anos, as soluções da fabricante *Trend Micro* para proteção de estações de trabalho, servidores e dispositivos móveis. O contrato 118/2018 adquiriu 1500 licenças para *endpoints*, além de 100 licenças para servidores, treinamento e suporte, permitindo que fosse alcançada experiência e uso das melhores práticas das ferramentas.

A solução adquirida à época não é mais comercializada, sendo atualizada para uma nova plataforma integrada de nome *Trend Vision One*, incluindo recursos como a capacidade de correlacionar eventos avançados e priorizar a resposta correspondente. Com esta solução, é possível visualizar o ciclo de vida de um ataque em toda a camada de rede, abrangendo dispositivos tanto gerenciados como não gerenciados, assim como sistemas contratados por terceiros, dispositivos IoT e IIoT, impressoras e sistemas BYOD.

Diante da necessidade de expansão do ambiente seguro do CNPq, contextualizada em seções anteriores, apenas a renovação das licenças existentes não é desejável, **tornando este cenário inviável**, visto que haverá necessidade de proteção, também, para outros vetores de ataque surgem a todo momento.

9.2. Cenário 2 - Solução existente no portal de software público brasileiro.

Neste cenário foi analisada a possibilidade de usar as ferramentas disponíveis no Portal de Software Público Brasileiro para atender as necessidades específicas em questão.

Após uma pesquisa no Portal de Software Público (https://www.gov.br/governodigital/pt-br/plataformas-e-servicos-digitais/software-publico/catalogo/catalogo), verificou-se que não há programas que apresentem as características essenciais para a solução desejada. Portanto, a utilização de software público para fornecimento de licenças, suporte técnico, garantia e atualizações **não é viável**. Nesse contexto, é necessário contratar uma empresa especializada que possa atender às demandas com precisão. Por conta desta lacuna identificada, recomendamos que este cenário seja descartado, visto que não atende aos requisitos críticos estabelecidos pelo CNPq.

9.3. Cenário 3 - Manter a solução atual sem garantia e sem suporte.

Esta solução compreende a não realização da renovação das licenças já utilizadas ou não realizar a aquisição de uma nova ferramenta de proteção de *endpoints* e servidores, mantendo somente as licenças que o CNPq já possui, sem garantia e suporte do fabricante.

Assim, vale ressaltar que softwares desatualizados são uma relevante porta de entrada para cibercriminosos, uma vez que a falta de atualizações de segurança - criadas justamente como resposta a brechas de segurança - torna os sistemas altamente vulneráveis. A recente onda de ataques por *criptoransomware* denominada "WannaCry", por exemplo, é uma ameaça que aproveita a falta de atualizações em sistemas operacionais Windows para invadir computadores. Este cenário **não é viável** para o CNPq.

9.4. Cenário 4 - Contratação de nova solução para proteção dos *endpoints*, servidores, *mobiles*, *containers,* ambiente de colaboração e gerenciamento de risco e superfície de ataque.

O cenário 2 envolve a aquisição de uma nova solução de segurança no mercado para atender às necessidades do CNPq. Nesse contexto, é crucial realizar uma análise detalhada das necessidades e requisitos de segurança da organização, garantindo que a nova solução seja capaz de satisfazer plenamente essas demandas. É fundamental que essa solução integre todas as "portas de entrada" de segurança, incluindo e-mail, *endpoints*, servidores e redes, bem como ofereça recursos avançados de Detecção e Resposta Estendida (XRD) por meio de uma única centralizadora de logs e detecções.

Para proporcionar uma avaliação mais precisa, considerando que o mercado de soluções corporativas de segurança de *endpoints* é diversificado e inclui várias opções, fizemos uma análise das principais soluções conhecidas no mercado, com base no *r*eview de *Endpoint Protection Platform do Gartner* (https://www.gartner.com/reviews/market/endpoint-protection-platforms - acessado em outubro/2024).

A partir desta consulta, foram selecionadas as seguintes soluções: **Trellix Endpoint Security (ENS); Sophos Intercept X Endpoint; Symantec Endpoint Security Complete; Microsoft Defender for Endpoint; SentinelOne Singularity Platform; CrowdStrike Falcon; Trend Apex One; Kaspersky Endpoint Security:**

A análise de cada uma destas visa verificar se atendem plenamente as necessidades definidas nos requisitos deste estudo. A seguir, apresentam-se as principais características técnicas e recursos de cada solução:

1. **Trellix Endpoint Security (ENS):** EDR avançado com análise de comportamento; proteção baseada em machine learning; integração com soluções de segurança como SIEM e SOAR; controle de dispositivos USB e whitelisting de aplicações; suporte a sandboxing e firewall integrado; gestão centralizada via console; foco em resposta rápida e automação de remediações.
2. **Sophos Intercept X Endpoint:** Combina EDR com inteligência artificial para bloqueio de ameaças avançadas; exploit prevention e proteção contra ransomware com rollback de ações; sandboxing para análise de arquivos suspeitos; integração com a plataforma de gerenciamento central Sophos Central; controle de aplicativos, firewall integrado e DLP; oferece proteção para dispositivos móveis.
3. **Symantec Endpoint Security Complete:** Proteção abrangente com EDR e XDR, além de DLP; cobertura para ambientes multinuvem e dispositivos móveis; proteção para e-mails e colaboração; integração com SIEM e suporte a sandboxing; gestão de vulnerabilidades e firewall integrado; foco em análise forense e automação de respostas.
4. **Microsoft Defender for Endpoint:** EDR e XDR integrados com o ecossistema Microsoft; proteção contra exploits e ransomware; gestão centralizada através do Microsoft 365 Defender; Machine learning e análise de comportamento para detecção proativa; proteção multinuvem e integração com SIEM e SOAR; suporte para ambientes híbridos (on-premises e nuvem).
5. **SentinelOne Singularity Platform:** EDR e XDR com foco em automação total de respostas a ameaças; proteção baseada em IA e análise comportamental; suporte para rollback de ransomware e análise forense; integração com SIEM e ferramentas de segurança para respostas coordenadas; proteção para workloads em nuvem, contêineres e ambientes virtualizados.
6. **CrowdStrike Falcon:** EDR em tempo real com análise baseada em inteligência artificial; detecção baseada em comportamento e hunting de ameaças; proteção multinuvem e integração com outras ferramentas de segurança; gestão centralizada via Falcon Platform; análises forenses e automação de resposta a incidentes; suporte para proteção de endpoints, servidores e dispositivos móveis.
7. **Trend Apex One:** EDR com foco em análise de comportamento e machine learning; proteção contra ransomware e vulnerabilidades; gestão de vulnerabilidades e proteção para workloads em nuvem; firewall integrado, sandboxing e suporte para ambientes multinuvem; proteção de e-mails e colaboração, além de controle de dispositivos; suporte a ambientes virtualizados e contêineres.
8. **Kaspersky Endpoint Security:** EDR com proteção antivírus e anti-malware de alta performance; controle de dispositivos e proteção contra exploits; DLP e firewall integrado; proteção contra ransomware com backup e rollback; proteção para dispositivos móveis e ambientes virtualizados; gestão centralizada e proteção de e-mails.

9.4.1. Análise comparativa entre as soluções de segurança listadas no cenário 4.

Foi realizada uma análise consolidada das soluções e das funcionalidades que cada uma atende com o objetivo de verificar o grau de atendimento às necessidades de segurança cibernética do CNPq.

Neste cenário foram avaliados como critérios de seleção a presença das funcionalidades abaixo listadas, que são essenciais para o fortalecimento do ambiente de cibersegurança, bem como o atendimento aos controles do Programa de Privacidade e Segurança da Informação - PPSI do Governo Federal:

- **Proteção antivírus/anti-malware**: detecta, bloqueia e remove vírus, *malwares* e outras formas de software malicioso que possam infectar o sistema. Atua com assinatura de ameaças conhecidas e, em alguns casos, com análise heurística para detectar comportamentos maliciosos.
- **Firewall integrado**: controla o tráfego de rede que entra e sai dos *endpoints*, bloqueando acessos não autorizados e prevenindo ataques baseados em rede, como tentativas de intrusão ou exploração de vulnerabilidades.
- **EDR (Detecção e Resposta a Ameaças)**: fornece monitoramento contínuo e resposta automatizada a ameaças avançadas nos *endpoints,* identificando comportamentos suspeitos e permitindo investigações detalhadas e remediação rápida.
- **XDR (Extended Detection and Response)**: expande as capacidades do EDR para coletar e correlacionar dados de múltiplas fontes (como rede, nuvem, e-mail) e fornecer uma visão unificada das ameaças em várias superfícies de ataque.
- **Machine Learning para detecção de ameaças**: utiliza algoritmos de aprendizado de máquina para identificar padrões e comportamentos anômalos, permitindo a detecção de novas ameaças que ainda não foram catalogadas (*zero-day threats*).
- **Proteção contra exploits**: previne o uso de vulnerabilidades conhecidas em software e sistemas para comprometer *endpoints*, bloqueando ataques que exploram falhas de segurança, como buffer overflows ou execução de código remoto.
- **Proteção ransomware**: detecta e bloqueia ataques de *ransomware* antes que eles possam criptografar arquivos, utilizando técnicas de monitoramento de comportamento e bloqueio de atividades suspeitas que indicam um ataque.
- **Gerenciamento centralizado (Console)**: fornece uma plataforma unificada para gerenciar a segurança de todos os dispositivos protegidos. Permite que administradores apliquem políticas, monitorem ameaças e tomem ações corretivas de forma centralizada.
- **Prevenção de Perda de Dados (DLP)**: monitora e controla o fluxo de dados sensíveis para prevenir que informações confidenciais sejam transmitidas ou acessadas indevidamente, tanto dentro como fora da organização.
- **Integração com SIEM**: conecta-se a sistemas de gerenciamento de eventos de segurança (SIEM) para centralizar logs e eventos, facilitando a correlação de dados e a detecção de ameaças em diferentes áreas da infraestrutura.
- **Controle de dispositivos**: monitora e gerencia o uso de dispositivos periféricos, como USBs e discos externos, para evitar que dispositivos não autorizados sejam usados para introduzir malwares ou extrair dados.

- **Whitelisting de aplicações**: permitir que apenas aplicativos pré-aprovados (em uma lista branca) sejam executados no endpoint, prevenindo a execução de software malicioso ou não autorizado.
- **Proteção para dispositivos móveis**: fornece segurança para smartphones e tablets, incluindo proteção contra malwares, controle de aplicativos, e gestão de dispositivos móveis (MDM), para proteger dados e acessos corporativos.
- **Proteção em ambientes multinuvem**: oferece segurança para workloads e dados que estão em execução em várias plataformas de nuvem (como AWS, Azure e Google Cloud), monitorando e protegendo contra ameaças específicas da nuvem.
- **Segurança para e-mails e colaboração**: protege sistemas de e-mail e plataformas de colaboração (como Microsoft 365, Zimbra e Google Workspace) contra phishing, malwares e roubo de credenciais, prevenindo ataques por anexos maliciosos ou links de phishing.
- **Automação de respostas a ameaças**: utiliza plataformas de orquestração de segurança (SOAR) para automatizar respostas a incidentes de segurança, agilizando a remediação e reduzindo o tempo de resposta às ameaças.
- **Análises forenses**: fornece ferramentas para investigar a origem e a natureza de uma ameaça ou ataque, permitindo que os analistas de segurança identifiquem a causa raiz e ajustem as defesas.
- **Rollback de ações maliciosas**: reverte as mudanças feitas por ataques, como a remoção de malwares e a recuperação de arquivos criptografados por ransomware, restaurando o sistema ao seu estado anterior à infecção.
- **Proteção para ambientes virtualizados**: protege máquinas virtuais e infraestruturas virtualizadas (como VMware, Hyper-V), detectando e bloqueando ameaças específicas para esses ambientes, incluindo a proteção de hypervisors e VMs.
- **Suporte a contêineres e workloads em nuvem**: protege contêineres (como Docker e Kubernetes) e workloads em execução na nuvem, monitorando vulnerabilidades e comportamentos anômalos nesses ambientes.
- **Detecção baseada em comportamento (Behavioral Analysis)**: monitora o comportamento de processos e aplicativos em tempo real para identificar atividades suspeitas que indicam possíveis ameaças, mesmo que essas ameaças sejam desconhecidas.
- **Sandboxing (análise de arquivos suspeitos)**: executa arquivos suspeitos em um ambiente isolado (sandbox) para verificar seu comportamento e determinar se são maliciosos, sem risco de infectar o sistema real.
- **Capacidades de Threat Hunting**: fornece ferramentas para analistas de segurança buscarem ativamente por ameaças que podem estar ocultas ou que ainda não foram detectadas automaticamente, permitindo investigações mais detalhadas e proativas.

9.4.2. Análise comparativa das soluções dos fabricantes avaliados

Funcionalidade	Trellix Endpoint Security	Sophos Intercept X Endpoint	Symantec Endpoint Security Complete	Microsoft Defender for Endpoint	SentinelOne Singularity Platform	CrowdStrike Falcon	Trend Micro Apex One	Kaspersky Endpoint Security
Proteção antivírus/anti-malware	Sim	Sim	Sim	Sim	Sim	Sim	Sim	Sim
Firewall integrado	Sim	Sim	Sim	Sim	Sim	Sim	Sim	Sim
EDR (Detecção e Resposta a Ameaças)	Sim	Sim	Sim	Sim	Sim	Sim	Sim	Sim
XDR (Extended Detection and Response)	Não	Não	Sim	Sim	Sim	Sim	Sim	Não
Machine Learning para detecção de ameaças	Sim	Sim	Sim	Sim	Sim	Sim	Sim	Sim
Proteção contra *exploits*	Sim	Sim	Sim	Sim	Sim	Sim	Sim	Sim
Proteção *ransomware*	Sim	Sim (com rollback)	Sim	Sim	Sim (rollback e recuperação)	Sim (prevenção proativa)	Sim	Sim (rollback parcial)
Gerenciamento centralizado (Console)	Sim (ePO)	Sim (Sophos Central)	Sim (Symantec Integrated Cyber Defense Manager)	Sim (Microsoft 365 Defender)	Sim (Singularity)	Sim (CrowdStrike Falcon Console)	Sim (Apex Central)	Sim (Kaspersky Security Center)
Prevenção de Perda de Dados (DLP)	Não	Sim	Sim	Não	Não	Não	Sim	Sim
Integração com SIEM	Sim	Sim	Sim	Sim	Sim	Sim	Sim	Sim
Controle de dispositivos	Sim	Sim	Sim	Sim	Sim	Sim	Sim	Sim
Whitelisting de Aplicações	Sim	Sim	Sim	Não nativamente	Sim	Sim	Sim	Sim
Proteção para dispositivos móveis	Sim	Sim	Sim	Sim	Sim	Sim	Sim	Sim
Proteção em ambientes multinuvem	Não	Sim	Sim	Sim	Sim	Sim	Sim	Não
Segurança para e-mails e colaboração	Não	Sim	Sim	Sim	Não	Não	Sim	Sim (via complementos)

Funcionalidade	Trellix Endpoint Security	Sophos Intercept X Endpoint	Symantec Endpoint Security Complete	Microsoft Defender for Endpoint	SentinelOne Singularity Platform	CrowdStrike Falcon	Trend Micro Apex One	Kaspersky Endpoint Security
Automação de respostas a ameaças	Limitado	Sim	Sim	Sim	Sim	Sim	Sim	Sim
Análises forenses	Sim	Sim	Sim	Sim	Sim	Sim	Sim	Sim
Rollback de ações maliciosas	Não	Sim	Sim	Sim	Sim (com reparo automático)	Sim	Sim	Sim
Proteção para ambientes virtualizados	Sim	Sim	Sim	Sim	Sim	Sim	Sim	Sim
Suporte a *contêineres* e *workloads* em nuvem	Não	Sim	Sim	Sim	Sim	Sim	Sim	Não
Detecção baseada em comportamento (*Behavioral Analysis*)	Sim	Sim	Sim	Sim	Sim	Sim	Sim	Sim
Sandboxing (análise de arquivos suspeitos)	Não nativo	Sim	Sim	Sim	Sim	Sim	Sim	Sim
Capacidades de *Threat Hunting*	Sim	Sim	Sim	Sim	Sim	Sim	Sim	Sim
Resultado da comparação	Não atende	Não atende	Atende	Não atende	Não atende	Não atende	Atende	Não atende

Conforme apresentado no quadro acima, apenas as soluções *Symantec Endpoint Security Complete* e *Trend Micro Apex One* atenderam todos os requisitos dos critérios apresentados.

A solução *Symantec Endpoint Security Complete* se destaca por sua integração robusta com XDR, capacidades avançadas de EDR, proteção abrangente para dispositivos móveis e uma forte cobertura multinuvem. É uma solução sólida para organizações que precisam de uma abordagem unificada para proteção em várias superfícies de ataque e têm um ecossistema de segurança altamente integrado.

Por sua vez, a solução *Trend Micro Apex One* oferece uma excelente proteção contra ameaças avançadas, com foco em *zero-day threats*, além de uma cobertura forte para ambientes virtualizados e contêineres, e boa integração com sua plataforma *Vision One* (XDR). Se destaca especialmente para organizações que utilizam nuvem e contêineres como parte essencial de suas operações.

Após uma análise detalhada e comparativa entre as soluções *Trend Micro Apex One* e *Symantec Endpoint Security Complete,* o CNPq optou pela continuidade e expansão da solução Trend Micro. A escolha foi embasada em uma série de fatores que se alinham às necessidades operacionais e estratégicas do órgão, considerando aspectos como estabilidade do ambiente, curva de aprendizado, tempo de migração e confiança no fornecedor atual.

A seguir, apresentamos a justificativa, detalhando as razões técnicas e operacionais que tornam o Trend Micro Apex One a solução mais adequada para o CNPq.

Estabilidade e confiança no ambiente atual: o CNPq já utiliza a solução Trend Micro em parte de seu ambiente tecnológico. A estabilidade comprovada da plataforma ao longo dos mais de 10 anos em utilização, sem interrupções críticas ou falhas de segurança relevantes, reforça a confiança na manutenção desse ambiente. Ao optar pela continuidade da solução Trend Micro, o órgão minimiza os riscos de interrupções causadas por problemas de integração ou migração, preservando o histórico de estabilidade conquistado. A introdução de uma nova solução de segurança, como a *Symantec Endpoint Security Complete*, exigiria uma fase de adaptação e um período de instabilidade potencial durante a transição, o que não pode acontecer, visto que este serviço é essencial e contínuo. Isso não só poderia comprometer o ambiente de segurança em um curto prazo, mas também aumentar a carga de trabalho para equipes de TI e segurança durante o processo de familiarização com uma nova plataforma. Além disso, é crucial considerar que a manutenção e expansão da solução de segurança Trend Micro no CNPq oferece vantagens técnicas, operacionais e de segurança indispensáveis para a proteção da instituição. A Trend Micro dispõe de soluções avançadas de cibersegurança que defendem contra ameaças conhecidas e emergentes. Nos últimos anos, os órgãos da APF foram alvos de um número crescente de ataques cibernéticos, como invasões, *ransomwares* e vazamento de dados. Exemplos recentes incluem ataques ao Ministério da Gestão e Inovação (https://www.gov.br/pf/pt-br/assuntos/noticias/2024/07/policia-federal-apura-ataque-cibernetico-contra-sistemas-do-governo-federal); a Casa da Moeda Brasileira, o Conselho de Controle de Atividades Financeiras, Ministério do Desenvolvimento, Ministério da Fazenda, Ministério da Igualdade Racial, Ministério da Microempresa e da Empresa de Pequeno Porte, Ministério das Mulheres, Ministério do Planejamento e Orçamento, Ministério da Previdência Social, Ministério dos Povos Indígenas (https://www.nexojornal.com.br/extra/2024/07/24/governo-apura-ataque-hacker-que-afetou-11-orgaos-e-ministerios); Agência Nacional das Águas (https://www.gov.br/ana/pt-br/assuntos/noticias-e-eventos/noticias/ana-retoma-sistemas-gradualmente-apos-ataque-cibernetico#:~:text=Ap%C3%B3s%20o%20ataque%20cibern%C3%A9tico%20verificado,ANA%20para%20acesso%20e%20utiliza%C3%A7%C3%A3o); Superior Tribunal de Justiça (https://agenciabrasil.ebc.com.br/geral/noticia/2024-09/stj-sofre-ataque-hacker-mas-nega-prejuizo-ao-sistema). Esses incidentes reforçam a necessidade de uma solução de segurança robusta e confiável para proteger o ambiente institucional do CNPq.

Facilidade de expansão e aprendizado reduzido: a continuidade com a Trend Micro garante uma curva de aprendizado reduzida, pois a equipe técnica já está familiarizada com a interface, funcionalidades e melhores práticas da solução. Ao manter essa familiaridade, o CNPq economiza tempo e recursos que, apesar de estar previsto em um treinamento, a familiaridade com a solução da fabricante torna o aprendizado mais assertivo e rápido.

Em contraste, a adoção da Symantec exigiria um tempo significativo para treinamento das equipes de TI e segurança, além de um esforço adicional para configurar e integrar a nova solução com os sistemas atuais. O tempo de adaptação e ajuste de políticas de segurança em uma nova plataforma poderia retardar a resposta a incidentes de segurança e comprometer o cumprimento das rotinas operacionais durante a transição.

Tempo e complexidade de migração: o processo de migração para uma nova plataforma de segurança envolve complexidades significativas, especialmente quando a infraestrutura tecnológica já está adaptada a um fornecedor específico. A migração de todos dos ativos instalados para a solução Symantec exigiria um planejamento extenso e uma execução cuidadosa para evitar falhas de segurança ou perda de dados. Por outro lado, a manutenção da solução Trend Micro elimina a necessidade de um processo de migração complexa, permitindo que o CNPq continue utilizando as funcionalidades já configuradas, enquanto expande para novas áreas e serviços de forma integrada. Isso garante uma continuidade operacional suave, sem interrupções ou riscos adicionais.

Recursos funcionais e alinhamento às necessidades do CNPq: a solução *Trend Micro Apex One* foi escolhida não apenas pela confiança existente, mas também pela sua capacidade de atender a todas as áreas críticas de segurança do CNPq, incluindo:

- Segurança de *endpoints* e servidores de rede: a *Apex One* oferece proteção robusta contra ameaças conhecidas e emergentes, com capacidade de detecção de ataques avançados em *endpoints* e servidores.
- Ambiente de colaboração e *containers*: suporte avançado para segurança de containers e ambientes de colaboração, que são cruciais em infraestruturas modernas, garantem que o CNPq possa operar de forma segura mesmo em cenários de alta colaboração digital.
- Segurança móvel e *antispam*: a integração de proteção para dispositivos móveis e a funcionalidade antispam do Apex One fortalecem a defesa contra ataques baseados em e-mails e comunicações móveis.
- Gerenciamento de superfície de ataque: o Trend Micro oferece uma visão abrangente da superfície de ataque, permitindo que o CNPq identifique e mitigue riscos antes que eles se transformem em ameaças ativas.

Embora a *Symantec Endpoint Security Complete* também ofereça funcionalidades abrangentes, a *Trend Micro* se destaca por fornecer uma solução já consolidada, com recursos avançados de inteligência de ameaças e integração contínua em diversos ambientes tecnológicos. A adaptabilidade da Trend Micro à infraestrutura existente do CNPq e sua capacidade de expandir para novas áreas de segurança tornam essa solução a mais alinhada às necessidades do órgão.

Confiança no fornecedor e relacionamento com a Trend Micro: o relacionamento já estabelecido entre o CNPq e a *Trend Micro* é um fator importante na decisão. A confiança no suporte técnico, no atendimento ao cliente e na capacidade de resposta rápida a problemas emergentes é crucial para garantir que as operações de segurança permaneçam sólidas e resilientes. Além disso, a *Trend Micro* tem demonstrado capacidade contínua de inovação, mantendo sua solução atualizada e alinhada às novas ameaças do cenário cibernético global. Por outro lado, a troca para um novo fabricante, como a *Symantec Endpoint Security Complete*, traria riscos consideráveis, incluindo a necessidade de desenvolver uma nova relação com um fornecedor diferente. Esse processo de adaptação implicaria em um período de incerteza, com potenciais desafios relacionados ao tempo de resposta, ao suporte técnico e à familiaridade com o ambiente do CNPq. Manter o relacionamento com a *Trend Micro* evita esse risco e preserva a continuidade das operações, sem interrupções que poderiam comprometer a segurança da instituição em um momento crítico.

Custo Total de Propriedade (TCO) e economia de recursos: outro fator decisivo é o custo total de propriedade. A manutenção da solução da Trend Micro representa uma otimização dos investimentos já realizados, garantindo que o CNPq continue usufruindo de economia em escala e suporte eficiente, sem a necessidade de reestruturar os processos de segurança. Manter e expandir a solução atual pode proporcionar economias de escala, pois o aumento de licenciamento reduz o custo *per capita* de proteção por disposição. Além disso, a padronização da solução antivírus facilita a gestão centralizada, simplificando a operação e reduzindo os custos associados a instalação, treinamento, manutenção e suporte técnico. É possível afirmar que a economicidade é evidente, visto que, ao permitir a contratação de diferentes soluções para atender aos diversos itens licitados, conforme solicitado, a instituição seria obrigada a contratar, para cada solução vencedora, os serviços de instalação da solução; treinamento da equipe; suporte técnico; e integração entre cada solução. Isso geraria uma multiplicidade de contratos a serem fiscalizados, sobrecarregando a equipe com demandas adicionais de tempo, administração e gestão de conflitos. Empresas que não conhecem a realidade das instituições podem sugerir mudanças, mas não consideram os desafios de compatibilidade, possíveis falhas de comprometimento e o risco de novas licitações para manter a segurança do ambiente.

9.5. Observância das alternativas às políticas, premissas e especificações técnicas vigentes

Requisito	Cenário	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	
	4		X	
A Solução está disponível no Portal do Software Público Brasileiro?	1		X	
	2		X	
	3		X	
	4		X	
A Solução é um software livre ou software público?	1		X	
	2		X	
	3		X	
	4		X	
A Solução é aderente às políticas, premissas e especificações técnicas definidas pelos Padrões e-PING, e-MAG?	1	X		
	2	X		
	3		X	
	4	X		
A Solução é aderente às regulamentações da ICPBrasil? (quando houver necessidade de certificação digital)	1			X
	2			X
	3			X
	4			X
A Solução é aderente às orientações, premissas e especificações técnicas e funcionais do e-ARQ Brasil? (quando o objetivo da solução abranger documentos arquivísticos)	1			X
	2			X
	3			X
	4			X

9.6. Escolha da solução viável

Consideramos que um dos objetivos das licitações públicas é assegurar a todos os licitantes igualdade de condições, consolidando, assim, o princípio constitucional da isonomia. Porém, para consecução desse objetivo, deve-se observar que a finalidade da licitação é selecionar proposta mais vantajosa para o interesse da Administração Pública. Neste sentido, o entendimento do Superior Tribunal de Justiça:

> "*ADMINISTRATIVO. PROCEDIMENTO LICITATÓRIO. AUTORIA. EMPRESA. LEGALIDADE.*
>
> *Quando, em procedimento licitatório, exige-se comprovação, em nome da empresa, não está sendo violado o art. 30 §1º, II, caput, da Lei 8.666/1993. É de vital importância, no trato da coisa pública, a permanente perseguição ao binômio qualidade e eficiência, objetivando não só garantir a segurança jurídica do contrato, mas também a consideração de certos fatores que integram a finalidade das licitações, máxime em se ao administrador a elaboração de dispositivos, sempre em atenção à pedra de toque do ato administrativo – a lei – mas com dispositivos que busquem resguardar a Administração de aventureiros ou de licitantes de competência estrutural, administrativa e organizacional duvidosa.*" Recurso provido. (Resp. nº 44.750-SP, rel. Ministro Francisco Falcão, 1ª T., unânime, DJ de 25.9.00)

Assim sendo, o objetivo da Administração não é acomodar, nas licitações públicas, toda e qualquer solução excêntrica em torno do objeto pretendido, mas garantir uma ampla concorrência em torno do atendimento de suas necessidades.

Diante de todo o exposto, **o único cenário viável para o CNPq é a contratação de uma solução integrada para proteção dos *endpoints*, servidores, *mobiles, containers*, ambiente de colaboração e gerenciamento de risco e superfície de ataque,** onde foram comparadas 9 soluções de segurança de diferentes fabricantes. Com base na análise dos fatores críticos, incluindo estabilidade, tempo de migração, confiança no fornecedor atual, e a capacidade de atender às necessidades de segurança do CNPq, as soluções da **Trend Micro** se destacam como a escolha mais adequada. Sua manutenção e expansão garantem uma abordagem de segurança robusta, confiável e eficiente, permitindo que o CNPq continue protegendo seu ambiente tecnológico em constante evolução. Neste contexto, é importante reiterar que a escolha da solução de segurança deve ser pautada pelas necessidades particulares do CNPq, pelo ambiente de TI, pela economicidade e pelas prioridades de segurança da organização. Embora as soluções alternativas apresentadas neste estudo sejam consistentes em termos de segurança, a Trend Micro se destaca ao oferecer recursos que são essenciais para atender às necessidades do Conselho.

A definição da marca se baseia no princípio da padronização do ambiente, da continuidade da solução e unificação da ferramenta de gerenciamento. Desta forma, a equipe de TI responsável pela segurança da informação pode aplicar políticas de segurança integradas e homogêneas, eliminando possíveis prejuízos causados por eventuais incompatibilidades. O princípio da padronização, da continuidade da solução, está alinhado com os princípios da legalidade, finalidade, economicidade, interesse público e vantagem para a Administração Pública Federal (APF), sem prejuízo dos demais princípios que estão presentes na contratação de bens, produtos e serviços para a APF. Por questões estratégicas e de operação, é importante utilizar produtos que apresentem configuração, manutenção e operacionalidade iguais ou similares ao atualmente instalado, tornando o processo de implantação, operação e transmissão de conhecimento menos complexo, mais célere e com menos riscos e impactos negativos ao negócio. A equipe técnica do CNPq desenvolveu experiência prática em lidar com incidentes e problemas durante o período em que a atual solução se encontra em operação. Dispor desta experiência assegura melhores condições na identificação e resolução dos problemas, controle e fiscalização dos serviços de segurança contratados, podendo resolvê-los com efetividade e acompanhamento e fiscalização dos serviços. A continuidade da solução mostra-se vantajosa por ter demonstrado, por todos esses anos, que a solução atende aos requisitos de segurança, pois tem sido eficaz e efetiva nas ações de proteção dos *endpoints* e servidores de forma preventiva e nas correções, soluções e tempo de respostas nos eventuais incidentes.

Ao se admitir uma quantidade demasiada de fornecedores, além da perda de uniformidade e padronização da solução, haveria evidente risco de descompasso no fornecimento dos itens da solução. Destarte, a admissão da adjudicação por item, desconfigura a caracterização da Solução de Tecnologia da Informação, vez que resultaria na perda irreparável da capacidade de integração dos serviços e do potencial de compartilhamento de recursos – condições que não podem ser asseguradas meramente mediante especificações técnicas. Portanto, a estruturação proposta agrupa de forma lícita, segura, técnica e economicamente viável, serviços de uma mesma natureza, que guardam correlação entre si, seja por similaridade técnica ou de tecnologia, bem como de aplicabilidade e de configuração do modelo de contratação propriamente dito, sem causar qualquer prejuízo à ampla competitividade.

O CNPq também levou em consideração o investimento realizado anteriormente e o interesse da curva de aprendizagem (*onboarding*), a fim de diminuir o tempo de aprendizagem e ganhar no período de adaptação da atualização das ferramentas. Os benefícios desta estratégia, também deve-se ressaltar os aspectos técnicos que colaboram com esta decisão, tais como:

- Gestão centralizada das tecnologias: a centralização na gestão das tecnologias permite uma administração mais eficiente e coerente de todos os recursos de segurança, facilitando a implementação de políticas, monitoramento e manutenção em toda a infraestrutura de TI.
- Integração ativa entre as soluções de segurança: a integração entre as soluções de segurança promove uma abordagem holística na proteção do ambiente de TI, garantindo que cada componente funcione em harmonia para fortalecer a segurança global e fornecer uma defesa robusta contra ameaças cibernéticas.
- Visão unificada por meio de console única: a disponibilidade de uma console única proporciona uma visão unificada e centralizada de todas as operações de segurança, simplificando a administração, o monitoramento e a análise de eventos em tempo real. Essa abordagem unificada permite uma resposta mais rápida e eficaz a incidentes de segurança, garantindo uma postura defensiva mais proativa e resiliente.

10. REGISTRO DE SOLUÇÕES CONSIDERADAS INVIÁVEIS

Conforme estipulado no § 1º do art. 11 da Instrução Normativa SGD/ME n.º 94/2022, todas as soluções identificadas como inviáveis devem ser devidamente registradas no Estudo Técnico Preliminar da Contratação, acompanhadas de uma breve descrição e justificativa. Esse registro dispensa a necessidade de elaborar os cálculos de custo total de propriedade.

Com base nas análises detalhadas apresentadas neste documento, as seguintes soluções foram consideradas inviáveis:

1. **Renovação do licenciamento da solução de proteção de estações de trabalho, servidores e dispositivos móveis já adquirida:** diante da necessidade de expansão do ambiente seguro do CNPq para cobertura de outros vetores de ataque, apenas a renovação das licenças existentes não é desejável para o CNPq, tornando este cenário inviável.
2. **Solução disponível no Portal de Software Público Brasileiro:** a pesquisa realizada no Portal de Software Público brasileiro não revelou nenhuma solução que atenda às necessidades específicas, tornando essa opção inviável.
3. **Manter a solução atual sem garantia e sem suporte:** torna-se um alto risco manter a solução atual sem garantia, atualizações e suporte, visto que os ataques cibernéticos estão cada vez mais sofisticados e impactantes.

11. ANÁLISE COMPARATIVA DE CUSTOS (TCO)

Conforme verificado na análise detalhada anteriormente, a fabricante Trend Micro, do cenário 4, é a escolha mais assertiva e benéfica para garantir a segurança do ambiente tecnológico do órgão. Dentro das necessidades do CNPq, os produtos fornecidos pela fabricante Trend estão descritos no quadro a seguir e correlacionados com as necessidades do CNPq:

Item	Solução	Nome da solução Trend Micro
1	Solução de segurança para *endpoints*	Trend Vision One - Endpoint Security Essentials
2	Solução de segurança para servidores físicos, virtuais e em nuvem	Trend Vision One - Endpoint Security Pro
3	Solução de segurança para e-mails (*antispam*)	Trend Micro One Email and Collaboration Security - Pro
4	Solução de segurança para ambiente de colaboração	
5	Solução de segurança para *containers*	Trend Cloud One Container Security
6	Solução de segurança para dispositivos *mobile*	Trend Micro Mobile Security
7	Gerenciamento de risco e superfície de ataque	Attack Surface Risk Management

Foi realizado um levantamento dos custos inerentes a estas soluções, bem como os serviços de suporte, treinamento e implantação.

Essa pesquisa buscou valores de serviços com as características iguais ou similares aos requisitados pela área demandante e amparada pelo previsto no Art. 5º da IN SEGES/ME 65/2021 combinado com o Art. 23 da Lei 14.133/2021, onde é determinado que os parâmetros podem ser empregados de forma combinada ou não. Como resultado foi elaborada a pesquisa de preço detalhada na Nota Técnica 2015071.

Para estudo de cálculo da pesquisa de preços que compõem esta Nota Técnica, foi utilizada a média aritmética simples composta pelos valores das contratações similares apresentadas no parâmetro II, aquisições similares de outros entes públicos, e no parâmetro IV, propostas comerciais:

MÉDIA DOS PARÂMETROS								
Item	**Descrição da solução pretendida**	**Quantidade (A)**	**Parâmetro I (B)**	**Parâmetro II (C)**	**Parâmetro III (D)**	**Parâmetro IV (E)**	**Parâmetro V (F)**	**Média dos Parâmetros (G)**
1	Trend Vision One - Endpoint Security Essentials	1200	-	R$ 311,55	-	R$ 392,08	-	**R$ 351,82**
2	Trend Vision One - Endpoint Security Pro	500	-	R$ 2.680,80	-	R$ 3.320,12	-	**R$ 3.000,46**
3	Trend Micro One Email and Collaboration Security - Pro	1200	-	R$ 145,50*	-	R$ 939,43	-	**R$ 939,43**
4	Trend Cloud One Container	10	-	-	-	R$ 11.553,99	-	**R$ 11.553,99**
5	Trend Micro Mobile Security	50	-	-	-	R$ 116,51	-	**R$ 116,51**
6	Attack Surface Risk Management (ASRM)	1700	-	-	-	R$ 238,02	-	**R$ 238,02**
7	Instalação/configuração das soluções	1	-	-	-	R$ 79.166,66	-	**R$ 79.166,66**
8	Suporte técnico, garantia e atualização 24x7	24	-	R$ 6.500,00	-	R$ 12.400,00	-	**R$ 9.450,00**
9	Treinamento das soluções de segurança	2	-	R$ 17.791,87	-	R$ 23.916,66	-	**R$ 20.854,27**

12. DESCRIÇÃO DA SOLUÇÃO DE TIC A SER CONTRATADA

Após a realização da análise comparativa de soluções e do custo total de propriedade, **a solução escolhida é a ferramenta de segurança avançada integrada de prevenção, detecção e resposta da fabricante Trend Micro no modelo de subscrição de licenças, dando continuidade à segurança de *endpoints* e servidores, expandindo para *mobile*, *container,* ambiente de colaboração, e-mail e superfície de ataque.** Uma solução de segurança avançada integrada de prevenção, detecção e resposta é uma plataforma de segurança cibernética integrada que combina a prevenção, detecção e resposta de ameaças de vários produtos de segurança cibernética. Esse tipo de solução oferece uma abordagem mais abrangente para detecção e resposta de ameaças do que as soluções de segurança cibernética tradicionais, permitindo que as organizações detectem e respondam rapidamente a ameaças em toda a sua infraestrutura de TI.

Algumas das características de uma solução deste tipo incluem, dentre outras:

- detecção de ameaças baseada em inteligência artificial e aprendizado de máquina;
- correlação de eventos de segurança de diferentes fontes em uma única plataforma;
- análise comportamental de usuários, dispositivos e aplicativos para identificar atividades suspeitas;
- integração com outros produtos de segurança cibernética;
- gerenciamento de incidentes de segurança cibernética; e
- visualização de dados em tempo real para uma melhor compreensão da postura de segurança cibernética da organização.

13. ESTIMATIVA DE CUSTO TOTAL DA CONTRATAÇÃO

R$ 3.923.404,59 (três milhões, novecentos e vinte e três mil quatrocentos e quatro reais e cinquenta e nove centavos) para o período de 24 (vinte e quatro) meses, prorrogável até o limite legal, art. 107 da lei n.º 14.133/2021 de 10 (dez) anos.

ITEM	ESPECIFICAÇÃO	CATSER	UNIDADE	QUANTIDADE	VALOR UNITÁRIO	VALOR TOTAL
1	Solução de segurança para *endpoints Trend Vision One - Endpoint Security Essentials*	27502	Unidade	1.200	R$ 351,82	R$ 422.184,00
2	Solução de segurança para servidores físicos, virtuais e em nuvem *Trend Vision One - Endpoint Security Pro*	27502	Unidade	500	R$ 3.000,46	R$ 1.500.230,00
3	Solução de segurança para e-mails (*antispam*) e ambiente de colaboração *Trend Micro One Email and Collaboration Security - Pro*	27502	Unidade	1.200	R$ 939,43	R$ 1.127.316,00

4	Solução de segurança para *containers* Trend Cloud One Container	27502	Unidade	10	R$ 11.553,99	R$ 115.539,90
5	Solução de segurança para dispositivos *mobile Trend Micro Mobile Security*	27502	Unidade	50	R$ 116,51	R$ 5.825,50
6	Gerenciamento de risco e superfície de ataque *Attack Surface Risk Management (ASRM)*	27502	Unidade	1.700	R$ 238,02	R$ 404.634,00
7	Instalação/configuração das soluções	26972	Unidade	1	R$ 79.166,66	R$ 79.166,66
8	Suporte técnico, garantia e atualização 24x7	27332	Mês	24	R$ 9.450,00	R$ 226.800,00
9	Treinamento das soluções de segurança	3840	Pessoa	2	R$ 20.854,27	R$ 41.708,53

14. JUSTIFICATIVA TÉCNICA DA ESCOLHA DA SOLUÇÃO

Conforme detalhado nas seções anteriores deste estudo, a escolha da solução integrada de segurança avançada de prevenção, detecção e resposta foi fundamentada nos incidentes recorrentes de segurança da informação no âmbito do Governo Federal, na crescente sofisticação das técnicas dos atacantes e no aumento dos vazamentos de dados relatados pela mídia. Diante desse cenário, optou-se por uma solução moderna, capaz de fornecer proteção abrangente ao ambiente computacional, com alta visibilidade e confiabilidade nas detecções, evitando que atividades anômalas ou maliciosas sejam executadas em tempo real, antes de impactar os dispositivos e usuários do CNPq.

Para a proteção eficaz contra ameaças modernas, é essencial que a solução utilize mecanismos de aprendizado de máquina e inteligência artificial, que permitam identificar e bloquear ataques em tempo real. Além disso, para garantir visibilidade total do ambiente, a solução contratada será capaz de analisar metadados de todas as máquinas e dispositivos de segurança do parque computacional, de forma a identificar e bloquear qualquer anomalia que comprometa os pilares da segurança da informação.

A continuidade dos serviços é um fator crucial para os gestores, pois a interrupção dos serviços públicos causaria transtornos significativos aos cidadãos. Dessa forma, a solução de segurança avançada integrada de prevenção, detecção e resposta da Trend Micro é a mais adequada para garantir a disponibilidade do ambiente sem impactar a infraestrutura ou os serviços fornecidos pelo CNPq.

14.1. Do parcelamento da contratação decorrente de aspectos técnicos

O parcelamento da solução de TIC se mostrou inviável, pois as licenças, serviços de instalação, configuração, garantia, suporte do fabricante e repasse de conhecimento formam uma solução unificada. É essencial que esses itens sejam fornecidos em conjunto, sem parcelamento, para garantir a implantação efetiva da solução. Essa abordagem está em conformidade com a alínea "a", inciso V do artigo 40 da Lei nº 14.133, de 1º de abril de 2021, que estabelece o princípio "*da padronização, considerando a compatibilidade de especificações estéticas, técnicas ou de desempenho*".

Dessa forma, a aquisição dos itens em um lote único assegura que todos os componentes sejam compatíveis entre si, garantindo a harmonia e o desempenho adequado da solução. Além de promover maior facilidade na manutenção, suporte técnico e garantia, uma vez que todos os elementos estão integrados e fornecidos por um único provedor.

O propósito é alcançar uma solução única, gerenciada de forma centralizada, para atender tanto quantitativa como qualitativamente às necessidades atuais da Pasta, proporcionando garantias adicionais à Administração de que não haverá ambiguidades em relação às responsabilidades por possíveis falhas na execução do contrato.

Novamente, conforme previsto na Lei n.º 14.133/2021, em seu artigo 18, parágrafo único, o não parcelamento do objeto poderá ser adotado, desde que justificado, conforme segue:

> *"Parágrafo único. O não parcelamento do objeto deverá ser justificado, visando evitar a perda de economia de escala, a redução da segurança, a padronização necessária ou a eficiência."*

A Lei n.º 14.133/2021 estabelece que o parcelamento deve ser considerado como regra para ampliar a competitividade, exceto quando houver justificativa técnica que demonstre que a fragmentação seria prejudicial ao contrato. Isso é especialmente relevante em contratações de alta complexidade, como soluções de segurança integrada, onde o parcelamento pode comprometer a eficiência e a compatibilidade do objeto contratado. Assim sendo, conforme já justificado tecnicamente, em alinhamento com o referido artigo, o não parcelamento do objeto será adotado, com vista a garantir melhor segurança, padronização e eficiência. Ressalta-se que, mesmo com o não parcelamento do objeto, existem diversas revendas do fabricante *Trend Micro* aptas e autorizadas a comercializar seus produtos e serviços, garantindo assim a competividade nos certames.

15. JUSTIFICATIVA ECONÔMICA DA ESCOLHA DA SOLUÇÃO

No quesito economicidade, a solução escolhida é a que melhor lida com os aspectos econômicos, visto que o modelo de subscrição permite ao CNPq pagar exatamente pelo uso, sem investir em uma solução de maneira perpétua, mobilizando recursos de capital e, na maioria dos casos, pagando além do uso.

15.1. Do parcelamento da contratação decorrente de aspectos econômicos

A divisão da contratação em múltiplos lotes afetaria negativamente o custo e a viabilidade econômica da solução, além de comprometer a uniformidade e padronização do sistema. Esse modelo, ao implicar na adoção de soluções de diferentes fabricantes, resultaria em uma série de novos custos para o CNPq. Primeiramente, cada lote exigiria uma nova etapa de implantação e configuração, o que geraria despesas adicionais consideráveis. A contratação parcelada também aumentaria os gastos com treinamento, pois cada solução adotada requer conhecimentos técnicos específicos e distintos, exigindo treinamentos especializados e multiplicando os esforços de capacitação. Da mesma forma, os custos de suporte seriam incrementados, uma vez que cada solução demandaria contratos separados de assistência técnica e manutenção, além de diferentes prazos e condições de atendimento, prejudicando a eficiência e aumentando a complexidade da gestão.

Dessa forma, a adoção de uma solução única representa um ganho significativo em termos de eficiência administrativa, ao unificar a gestão contratual e simplificar o processo de monitoramento e controle. Esse modelo atende ao preceito constitucional de busca pela eficiência no setor público, otimizando recursos e assegurando uma execução mais coesa e integrada dos serviços contratados.

A unicidade da solução contratada não apenas fortalece a capacidade de integração e interoperabilidade entre os serviços, como também possibilita um melhor aproveitamento dos recursos compartilhados pela contratada. Essas características são fundamentais para garantir a sustentabilidade e a eficácia do ciclo de vida dos serviços, alinhando-se com os objetivos intrínsecos do contrato e reforçando o princípio da economicidade que rege a administração pública.

16. BENEFÍCIOS A SEREM ALCANÇADOS COM A CONTRATAÇÃO

Repisando que o modelo ora escolhido como a opção viável é a que promove a contratação da solução no modelo de subscrição onde somente será demandado e pago aquelas licenças devidamente instaladas e em uso impedindo o uso incorreto. Em igual sentido, cria-se uma possibilidade de avaliação anual acerca da manutenção/renovação do contrato visto a velocidade com que a tecnologia da informação evolui. Não seria surpresa se ao longo dos anos as constantes evoluções tecnológicas caminhem para uma nova solução, que desempenhe o atendimento aos requisitos do CNPq de maneira distinta, mais otimizada, mais inteligente, menos custosa e mais efetiva. Neste momento essa é a solução que melhor se encaixa nesse cenário.

De maneira complementar listamos, de maneira não exaustiva, alguns dos benefícios a serem experimentados pelo CNPq com a contratação da solução de segurança avançada integrada de prevenção, detecção e resposta objeto deste estudo técnico. Segue:

- destinação otimizada dos investimentos em TI;
- melhorar a assertividade nos investimentos em soluções de segurança da informação efetivamente necessárias;
- aumentar a maturidade de gestão de serviços de TIC;
- maior controle de segurança da informação e proteção de dados no âmbito do CNPq: por meio da redução de malwares, sistemas desatualizados, dentre outros problemas;
- apoio nas auditorias de Segurança da Informação e Comunicações: a obtenção de relatórios detalhados permitirá a devida diligência durante as auditorias;
- detecção mais rápida das ameaças;
- resposta mais eficiente aos incidentes de segurança;
- redução de alertas de falsos positivos;
- melhor visibilidade para às áreas de TI do CNPq e da prestadora de serviços;
- redução de custos reduzindo a contratação de outras ferramentas;
- integração com outras soluções de TI; e
- redução de riscos com violações de dados.

17. PROVIDENCIAS A SEREM ADOTADAS

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

Conforme descrito neste Estudo Técnico e no Documento de Oficialização de Demanda (SEI 1738403), o CNPq necessita e possui condições de adquirir e operar a contratação ora apresentada.

19. RESPONSÁVEIS

Conforme o § 2º do Art. 11 da IN SGD/ME n.º 94/2022, o Estudo Técnico Preliminar deverá ser aprovado e assinado pelos Integrantes Técnicos e Requisitantes e pela autoridade máxima da área de TIC:

Integrante Requisitante	Integrante Técnico
(Assinado eletronicamente) **Emerson da Motta Willer** Analista em C&T 15380671	*(Assinado eletronicamente)* **Paulo Rodrigues da Costa** Assistente em C&T 06718345

Conforme o Inc. II do Art. 43 da Lei n.º 14.133/2021, que estabelece os princípios de igualdade de condições e da proposta mais vantajosa nas licitações públicas, acolhe-se o entendimento exposto sobre a importância da isonomia e da eficiência na contratação para assegurar a escolha da proposta que melhor atenda ao interesse público.

Considerando a análise técnica realizada, justifica-se a padronização da solução de segurança integrada para o CNPq, com indicação da marca *Trend Micro*, como a escolha mais eficiente e vantajosa. Essa solução abrange *endpoints*, servidores, dispositivos móveis e demais aspectos de segurança da informação, assegurando continuidade operacional e redução de custos. A uniformidade e centralização da tecnologia em uma única plataforma permite uma gestão integrada e facilita a aplicação de políticas de segurança, monitoramento, fiscalização e manutenção, gerando menos complexidade e maior celeridade ao processo.

Conforme a Lei nº 14.133/2021, artigo 41, que permite a indicação de marca em licitações quando fundamentada tecnicamente, o presente estudo técnico confirma que a padronização atende aos princípios de legalidade, economicidade, eficiência e interesse público. Diante do exposto, defiro a continuidade do processo licitatório com a indicação de fornecedor, observando-se que a escolha é técnica e juridicamente fundamentada e que contribui para o alcance da proposta mais vantajosa e segura para a Administração.

Autoridade máxima da área de Tecnologia da Informação e Comunicação - TIC
(Assinado eletronicamente) **Geraldo Sorte** Coordenador-geral de Tecnologia da Informação Portaria DASD/CNPq n.º 1219, de 26 de janeiro de 2023

Documento assinado eletronicamente por **EMERSON DA MOTTA WILLER**, **Fiscal Requisitante do Contrato**, em 30/10/2024, às 18:49, conforme o art. 6º do Decreto nº 8.539, de 08 de outubro de 2015.

Documento assinado eletronicamente por **PAULO RODRIGUES DA COSTA**, **Integrante técnico da contratação**, em 31/10/2024, às 09:17, conforme o art. 6º do Decreto nº 8.539, de 08 de outubro de 2015.

Documento assinado eletronicamente por **GERALDO SORTE**, **Coordenador-Geral de Tecnologia da Informação PORTARIA Nº 217, DE 3 DE MARÇO DE 2022**, em 31/10/2024, às 11:52, conforme o art. 6º do Decreto nº 8.539, de 08 de outubro de 2015.

Documento assinado eletronicamente por **CICERO MANOEL VERISSIMO GOMES**, **Integrante Administrativo**, em 31/10/2024, às 15:02, 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 **2188063** e o código CRC **5B6C7A85**.

CONTRATO ADMINISTRATIVO Nº ...../...., QUE FAZEM ENTRE SI A UNIÃO, POR INTERMÉDIO DO (A) ..... E .....

O **CONSELHO NACIONAL DE DESENVOLVIMENTO CIENTÍFICO E TECNOLÓGICO (CNPq),** com sede no Setor de Autarquias Sul (SAUS), Quadra 01 Lote 06 Bloco H, Edifício Telemundi II, Bairro Asa Sul, CEP: 70.070-010, na cidade de Brasília/DF, inscrito no CNPJ sob o nº 33.654.831/0001-36, neste ato representado(a) pelo(a) ..... (*cargo e nome*), nomeado(a) pela Portaria nº ....., de ..... de ..... de 20..., publicada no *DOU* de ..... de ..... de ....., portador da Matrícula Funcional nº ....., doravante denominado CONTRATANTE, e o(a) ....., *inscrito(a) no CNPJ/MF sob o nº ....., sediado(a) na ....., em .....* 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 SEI nº 01300.005789/2023-78 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 Pregão Eletrônico n° 90009/2024, mediante as cláusulas e condições a seguir enunciadas.

CLÁUSULA PRIMEIRA – OBJETO (art. 92, I e II)

1.1. O objeto do presente instrumento é a contratação de solução de tecnologia da informação e comunicação de solução de segurança de endpoints, servidores de rede, antispam, ambiente de colaboração, mobile, ambiente de containers e gerenciamento de superfície de ataque com atualização contínua, garantia, implantação, suporte técnico e treinamento, nas condições estabelecidas no Termo de Referência.

1.2 Objeto da contratação:

GRUPO 1						
ITEM	**ESPECIFICAÇÃO**	**CATSER**	**UNIDADE**	**QUANT**	**VALOR UNITÁRIO**	**VALOR TOTAL**
1	Solução de segurança para *endpoints Trend Vision One - Endpoint Security Essentials*	27502	Unidade	1.200		
2	Solução de segurança para servidores físicos, virtuais e em nuvem *Trend Vision One - Endpoint Security Pro*	27502	Unidade	500		
3	Solução de segurança para e-mails (*antispam*) e ambiente de colaboração *Trend Micro One Email and*	27502	Unidade	1.200		

	Collaboration Security - Pro					
4	Solução de segurança para *conteiners Trend Cloud One Container*	27502	Unidade	10		
5	Solução de segurança para dispositivos *mobile Trend Micro Mobile Security*	27502	Unidade	50		
6	Gerenciamento de risco e superfície de ataque *Attack Surface Risk Management (ASRM)*	27502	Unidade	1.700		
7	Instalação/configuração das soluções	26972	Unidade	1		
8	Suporte técnico, garantia e atualização 24x7	27332	Mês	24		
9	Treinamento das soluções de segurança para 3 servidores	3840	Pessoa	2		
VALOR TOTAL R$						

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 24 (vinte e quatro) meses contados da assinatura do contrato, prorrogável para até 10 anos, na forma dos artigos 106 e 107 da Lei n° 14.133, de 2021.

2.2.1. A prorrogação de que trata esse item é condicionada à avaliação, por parte do Gestor do Contrato, da vantajosidade da prorrogação, a qual deverá ser realizada motivadamente, com base no Histórico de Gestão do Contrato, nos princípios da manutenção da necessidade, economicidade e oportunidade da contratação, e nos demais aspectos que forem julgados relevantes.

2.2.2. O contratado não tem direito subjetivo à prorrogação contratual.

2.2.3. A prorrogação de contrato deverá ser promovida mediante celebração de termo aditivo.

2.2.4. Nas eventuais prorrogações contratuais, os custos não renováveis já pagos ou amortizados ao longo do primeiro período de vigência da contratação deverão ser reduzidos ou eliminados como condição para a renovação.

CLÁUSULA TERCEIRA – MODELOS DE EXECUÇÃO E GESTÃO CONTRATUAIS (art. 92, IV, VII e XVIII)

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. Não será admitida a subcontratação do objeto contratual.

CLÁUSULA QUINTA - PREÇO

5.1. O valor total da contratação é de R$..... (.....).

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 (art. 92, V e VI)

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 (art. 92, V)

7.1. Os preços inicialmente contratados são fixos e irreajustáveis no prazo de um ano contado da data do orçamento estimado, em __/__/__ *(DD/MM/AAAA)*.

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.

7.3. Nos reajustes subsequentes ao primeiro, o interregno mínimo de um ano será contado a partir dos efeitos financeiros do último reajuste.

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).

7.5. Nas aferições finais, o(s) índice(s) utilizado(s) para reajuste será(ão), obrigatoriamente, o(s) definitivo(s).

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.

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.

7.8. O reajuste será realizado por apostilamento.

CLÁUSULA OITAVA - OBRIGAÇÕES DO CONTRATANTE (art. 92, X, XI e XIV)

8.1. São obrigações do Contratante, além das previstas no termo de referência:

8.2. Exigir o cumprimento de todas as obrigações assumidas pelo Contratado, de acordo com o contrato e seus anexos;

8.3. Receber o objeto no prazo e condições estabelecidas no Termo de Referência;

8.4. Notificar o Contratado, por escrito, sobre vícios, defeitos ou incorreções verificadas no objeto fornecido, para que seja por ele substituído, reparado ou corrigido, no total ou em parte, às suas expensas;

8.5. Acompanhar e fiscalizar a execução do contrato e o cumprimento das obrigações pelo Contratado;

8.6. Comunicar a empresa para emissão de Nota Fiscal no que pertine à parcela incontroversa da execução do objeto, para efeito de liquidação e pagamento, quando houver controvérsia sobre a execução do objeto, quanto à dimensão, qualidade e quantidade, conforme o art. 143 da Lei nº 14.133, de 2021;

8.7. Efetuar o pagamento ao Contratado do valor correspondente à execução do objeto, no prazo, forma e condições estabelecidos no presente Contrato e no Termo de Referência;

8.8. Aplicar ao Contratado as sanções previstas na lei e neste Contrato;

8.9. Cientificar o órgão de representação judicial da Advocacia-Geral da União para adoção das medidas cabíveis quando do descumprimento de obrigações pelo Contratado;

8.10. 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.

8.11. 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.

8.12. Responder eventuais pedidos de reestabelecimento do equilíbrio econômico-financeiro feitos pelo contratado no prazo máximo de 30 (trinta) dias.

8.13. Notificar os emitentes das garantias quanto ao início de processo administrativo para apuração de descumprimento de cláusulas contratuais.

8.14. Comunicar o Contratado na hipótese de posterior alteração do projeto pelo Contratante, no caso do art. 93, §2º, da Lei nº 14.133, de 2021.

8.15. 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 (art. 92, XIV, XVI e XVII)

9.1. O Contratado deve cumprir todas as obrigações constantes deste Contrato e de 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:

9.2. Manter preposto aceito pela Administração no local ou do serviço para representá-lo na execução do contrato.

9.3. A indicação ou a manutenção do preposto da empresa poderá ser recusada pelo órgão ou entidade, desde que devidamente justificada, devendo a empresa designar outro para o exercício da atividade.

9.4. Atender às determinações regulares emitidas pelo fiscal do contrato ou autoridade superior (art. 137, II) e prestar todo esclarecimento ou informação por eles solicitados;

9.5. Alocar os empregados necessários ao perfeito cumprimento das cláusulas deste contrato, com habilitação e conhecimento adequados, fornecendo os materiais, equipamentos, ferramentas e utensílios demandados, cuja quantidade, qualidade e tecnologia deverão atender às recomendações de boa técnica e a legislação de regência;

9.6. Reparar, corrigir, remover, reconstruir ou substituir, às suas expensas, no total ou em parte, no prazo fixado pelo fiscal do contrato, os serviços nos quais se verificarem vícios, defeitos ou incorreções resultantes da execução ou dos materiais empregados;

9.7. Responsabilizar-se pelos vícios e danos decorrentes da execução do objeto, de acordo com o Código de Defesa do Consumidor (Lei nº 8.078, de 1990), 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 no edital, o valor correspondente aos danos sofridos;

9.8. Não contratar, durante a vigência do contrato, cônjuge, companheiro ou parente em linha reta, colateral ou por afinidade, até o terceiro grau, de dirigente do contratante ou do fiscal ou gestor do contrato, nos termos do artigo 48, parágrafo único, da Lei nº 14.133, de 2021;

9.9. 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, até o dia trinta do mês seguinte ao da prestação dos serviços, os seguintes documentos:

1) prova de regularidade relativa à Seguridade Social;

2) certidão conjunta relativa aos tributos federais e à Dívida Ativa da União;

3) certidões que comprovem a regularidade perante a Fazenda Municipal ou Distrital do domicílio ou sede do contratado;

4) Certidão de Regularidade do FGTS – CRF; e

5) Certidão Negativa de Débitos Trabalhistas – CNDT.

9.10. Responsabilizar-se pelo cumprimento das obrigações previstas em Acordo, Convenção, Dissídio Coletivo de Trabalho ou equivalentes das categorias abrangidas pelo contrato, por todas as obrigações trabalhistas, sociais, previdenciárias, tributárias e as demais previstas em legislação específica, cuja inadimplência não transfere a responsabilidade ao Contratante;

9.11. Comunicar ao Fiscal do contrato, no prazo de 24 (vinte e quatro) horas, qualquer ocorrência anormal ou acidente que se verifique no local dos serviços.

9.12. Prestar todo esclarecimento ou informação solicitada pelo Contratante ou por seus prepostos, garantindo-lhes o acesso, a qualquer tempo, ao local dos trabalhos, bem como aos documentos relativos à execução do empreendimento.

9.13. 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.

9.14. Promover a guarda, manutenção e vigilância de materiais, ferramentas, e tudo o que for necessário à execução do objeto, durante a vigência do contrato.

9.15. Conduzir os trabalhos com estrita observância às normas da legislação pertinente, cumprindo as determinações dos Poderes Públicos, mantendo sempre limpo o local dos serviços e nas melhores condições de segurança, higiene e disciplina.

9.16. 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.

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

9.18. Manter durante toda a vigência do contrato, em compatibilidade com as obrigações assumidas, todas as condições exigidas para habilitação na licitação;

9.19. 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 (art. 116);

9.20. 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 (art. 116, parágrafo único);

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

9.22. 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;

9.23. Cumprir, além dos postulados legais vigentes de âmbito federal, estadual ou municipal, as normas de segurança do Contratante;

CLÁUSULA DÉCIMA - OBRIGAÇÕES PERTINENTES À LGPD

10.1. As partes deverão cumprir a Lei nº 13.709, de 14 de agosto de 2018 (LGPD), quanto a todos os dados pessoais a que tenham acesso em razão do certame ou do contrato administrativo que eventualmente venha a ser firmado, a partir da apresentação da proposta no procedimento de contratação, independentemente de declaração ou de aceitação expressa.

10.2. Os dados obtidos somente poderão ser utilizados para as finalidades que justificaram seu acesso e de acordo com a boa-fé e com os princípios do art. 6º da LGPD.

10.3. É vedado o compartilhamento com terceiros dos dados obtidos fora das hipóteses permitidas em Lei.

10.4. A Administração deverá ser informada no prazo de 5 (cinco) dias úteis sobre todos os contratos de suboperação firmados ou que venham a ser celebrados pelo Contratado.

10.5. Terminado o tratamento dos dados nos termos do art. 15 da LGPD, é dever do contratado eliminá-los, com exceção das hipóteses do art. 16 da LGPD, incluindo aquelas em que houver necessidade de guarda de documentação para fins de comprovação do cumprimento de obrigações legais ou contratuais e somente enquanto não prescritas essas obrigações.

10.6. É dever do contratado orientar e treinar seus empregados sobre os deveres, requisitos e responsabilidades decorrentes da LGPD.

10.7. O Contratado deverá exigir de suboperadores e subcontratados o cumprimento dos deveres da presente cláusula, permanecendo integralmente responsável por garantir sua observância.

10.8. O Contratante poderá realizar diligência para aferir o cumprimento dessa cláusula, devendo o Contratado atender prontamente eventuais pedidos de comprovação formulados.

10.9. O Contratado deverá prestar, no prazo fixado pelo Contratante, prorrogável justificadamente, quaisquer informações acerca dos dados pessoais para cumprimento da LGPD, inclusive quanto a eventual descarte realizado.

10.10. Bancos de dados formados a partir de contratos administrativos, notadamente aqueles que se proponham a armazenar dados pessoais, devem ser mantidos em ambiente virtual controlado, com registro

individual rastreável de tratamentos realizados (LGPD, art. 37), com cada acesso, data, horário e registro da finalidade, para efeito de responsabilização, em caso de eventuais omissões, desvios ou abusos.

10.11. Os referidos bancos de dados devem ser desenvolvidos em formato interoperável, a fim de garantir a reutilização desses dados pela Administração nas hipóteses previstas na LGPD.

10.12. O contrato está sujeito a ser alterado nos procedimentos pertinentes ao tratamento de dados pessoais, quando indicado pela autoridade competente, em especial a ANPD por meio de opiniões técnicas ou recomendações, editadas na forma da LGPD.

10.13. Os contratos e convênios de que trata o § 1º do art. 26 da LGPD deverão ser comunicados à autoridade nacional.

CLÁUSULA DÉCIMA PRIMEIRA – GARANTIA DE EXECUÇÃO (art. 92, XII)

11.1. A contratação conta com garantia de execução, nos moldes do art. 96 da Lei nº 14.133, de 2021, na modalidade XXXXXX, em valor correspondente a 5% (cinco por cento) do valor inicial/total/anual do contrato.

OU

11.2. O contratado apresentará, 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, podendo optar por caução em dinheiro ou títulos da dívida pública ou, ainda, pela fiança bancária, em valor correspondente a 5% (cinco por cento) do valor inicial/total/anual do contrato.

11.3. Caso utilizada a modalidade de seguro-garantia, a apólice permanecerá em vigor mesmo que o contratado não pague o prêmio nas datas convencionadas.

11.4. Caso utilizada a modalidade de seguro-garantia, a apólice deverá ter validade durante a vigência do contrato e por 90 (noventa) dias após o término da vigência contratual, permanecendo em vigor mesmo que o contratado não pague o prêmio nas datas convencionadas.

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

11.6. 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, ressalvado o disposto no item 11.7 deste contrato.

11.7. 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.

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

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

11.8.2. multas moratórias e punitivas aplicadas pela Administração à contratada; e

11.8.3. obrigações trabalhistas e previdenciárias de qualquer natureza e para com o FGTS, não adimplidas pelo contratado, quando couber.

11.9. A modalidade seguro-garantia somente será aceita se contemplar todos os eventos indicados no item 11.8, observada a legislação que rege a matéria.

11.10. A garantia em dinheiro deverá ser efetuada em favor do contratante, em conta específica na Caixa Econômica Federal, com correção monetária.

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

11.12. 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.

11.13. No caso de alteração do valor do contrato, ou prorrogação de sua vigência, a garantia deverá ser ajustada ou renovada, seguindo os mesmos parâmetros utilizados quando da contratação.

11.14. 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, contados da data em que for notificada.

11.15. O Contratante executará a garantia na forma prevista na legislação que rege a matéria.

11.15.1. 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 (art. 137, § 4º, da Lei n.º 14.133, de 2021).

11.15.2. 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.

11.16. Extinguir-se-á a garantia com a restituição da apólice, carta fiança ou autorização para a liberação de importâncias depositadas em dinheiro a título de garantia, acompanhada de declaração do contratante, mediante termo circunstanciado, de que o contratado cumpriu todas as cláusulas do contrato;

11.17. 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.

11.18. 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.

11.19. O contratado autoriza o contratante a reter, a qualquer tempo, a garantia, na forma prevista no Edital e neste Contrato.

11.20. A garantia de execução é independente de eventual garantia do produto ou serviço prevista especificamente no Termo de Referência.

CLÁUSULA DÉCIMA SEGUNDA – INFRAÇÕES E SANÇÕES ADMINISTRATIVAS (art. 92, XIV)

12.1. 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.

12.2. Serão aplicadas ao contratado que incorrer nas infrações acima descritas as seguintes sanções:

i) **Advertência**, quando o contratado der causa à inexecução parcial do contrato, sempre que não se justificar a imposição de penalidade mais grave (art. 156, §2º, da Lei nº 14.133, de 2021);

ii) **Impedimento de licitar e contratar**, quando praticadas as condutas descritas nas alíneas "b", "c" e "d" do subitem acima deste Contrato, sempre que não se justificar a imposição de penalidade mais grave (art. 156, § 4º, da Lei nº 14.133, de 2021);

iii) **Declaração de inidoneidade para licitar e contratar**, quando praticadas as condutas descritas nas alíneas "e", "f", "g" e "h" do subitem acima deste Contrato, bem como nas alíneas "b", "c" e "d", que justifiquem a imposição de penalidade mais grave (art. 156, §5º, da Lei nº 14.133, de 2021).

iv) **Multa:**

(1) Moratória 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;

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

a. O atraso superior a 15 (quinze) dias 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.

(3) Compensatória, para as infrações descritas nas alíneas "e" a "h" do subitem 12.1, de 0,5% a 1% do valor do Contrato.

(4) Compensatória, para a inexecução total do contrato prevista na alínea "c" do subitem 12.1, de 5% a 10%do valor do Contrato.

(5) Para infração descrita na alínea "b" do subitem 12.1, a multa será de 1% a 3% do valor do Contrato.

(6) Para infrações descritas na alínea "d" do subitem 12.1, a multa será de 5% a 10% do valor do Contrato.

(7) Para a infração descrita na alínea "a" do subitem 12.1, a multa será de 1% a 5% do valor do Contrato, ressalvadas as seguintes infrações:

ID	Ocorrência	Glosa/Sanção
1	Não comparecer injustificadamente à reunião inicial.	Advertência. Em caso de reincidência, multa 1% sobre o valor total do Contrato.
2	Quando convocado dentro do prazo de validade da sua proposta, não celebrar o Contrato, deixar de entregar ou apresentar documentação falsa exigida para o certame, ensejar o retardamento da execução de seu objeto, não manter a proposta, falhar ou fraudar na execução do Contrato, comportar-se de modo inidôneo ou cometer fraude fiscal.	A Contratada ficará impedida de licitar e contratar com a União, Estados, Distrito Federal e Municípios e, será descredenciada no SICAF, ou nos sistemas de cadastramento de fornecedores pelo prazo de até 5 (cinco) anos, sem prejuízo das demais cominações legais, e multa de 5% do valor da contratação.
3	Ter praticado atos ilícitos visando frustrar os objetivos da licitação.	A Contratada será declarada inidônea para licitar e contratar com a Administração Pública.
4	Demonstrar não possuir idoneidade para contratar com a Administração em virtude de atos ilícitos praticados.	Suspensão temporária de 6 (seis) meses para licitar e contratar com a Administração Pública, sem prejuízo da Rescisão Contratual.

5	Não executar total ou parcialmente os serviços previstos no objeto da contratação.	Multa de até 10% sobre o valor total do Contrato.
6	Suspender ou interromper, salvo motivo de força maior ou caso fortuito, os serviços solicitados, por até de 30 dias, sem comunicação formal ao gestor do Contrato.	Multa de até 5% sobre o valor total do Contrato.
7	Não prestar os esclarecimentos imediatamente, referente à execução dos serviços, salvo quando implicarem em indagações de caráter técnico, hipótese em que serão respondidos no prazo máximo de 5 dias úteis.	Advertência. Em caso de reincidência, multa de 1% sobre o valor total do Contrato por dia útil de atraso em prestar as informações por escrito, ou por outro meio quando autorizado pela Contratante, até o limite de 10 dias úteis.
		Após o limite de 10 dias úteis, aplicar-se-á multa de 5% do valor total do Contrato.
8	Provocar intencionalmente a indisponibilidade da prestação dos serviços quanto aos componentes de software (sistemas, portais, funcionalidades, banco de dados, programas, relatórios, consultas etc.).	A Contratada será impedida de licitar e contratar com órgãos e entidades da União, com o consequente descredenciamento no SICAF pelo prazo de até cinco anos, sem prejuízo às penalidades de correntes da inexecução total ou parcial do contrato, o que poderá acarretar a rescisão do Contrato, sem prejuízo das demais penalidades previstas na Lei n.º 14.133/2021.
9	Permitir intencionalmente o funcionamento dos sistemas de modo adverso ao especificado na fase de levantamento de requisitos e às cláusulas contratuais, provocando prejuízo aos usuários dos serviços.	A Contratada será impedida de licitar e contratar com órgãos e entidades da União, com o consequente descredenciamento no SICAF pelo prazo de até cinco anos, sem prejuízo às penalidades decorrentes da inexecução total ou parcial do contrato, o que poderá acarretar a rescisão do Contrato, sem prejuízo das demais penalidades previstas na Lei n.º 14.133/2021.
10	Comprometer intencionalmente a integridade, disponibilidade ou confiabilidade e autenticidade das bases de dados dos sistemas.	A Contratada será impedida de licitar e contratar com órgãos e entidades da União, com o consequente descredenciamento no SICAF pelo prazo de até cinco anos, sem prejuízo às penalidades decorrentes da inexecução total ou parcial do contrato, o que poderá acarretar a rescisão do Contrato, sem prejuízo das demais penalidades previstas na Lei n.º 14.133/2021.
11	Comprometer intencionalmente o sigilo das informações armazenadas nos sistemas da contratante.	A Contratada será impedida de licitar e contratar com órgãos e entidades da União, com o consequente descredenciamento no SICAF pelo prazo de até cinco anos, sem prejuízo às penalidades decorrentes da inexecução total ou parcial do contrato, o que poderá acarretar a rescisão do Contrato, sem prejuízo das demais penalidades previstas na Lei n.º 14.133/2021.

12	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 5% (dois por cento) do valor total do Contrato.

12.3. A aplicação das sanções previstas neste Contrato não exclui, em hipótese alguma, a obrigação de reparação integral do dano causado ao Contratante (art. 156, §9º, da Lei nº 14.133, de 2021)

12.4. Todas as sanções previstas neste Contrato poderão ser aplicadas cumulativamente com a multa (art. 156, §7º, da Lei nº 14.133, de 2021).

12.5. Antes da aplicação da multa será facultada a defesa do interessado no prazo de 15 (quinze) dias úteis, contado da data de sua intimação (art. 157, da Lei nº 14.133, de 2021)

12.6. 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 (art. 156, §8º, da Lei nº 14.133, de 2021).

12.7. Previamente ao encaminhamento à cobrança judicial, a multa poderá ser recolhida administrativamente no prazo máximo de 30 (trinta) dias, a contar da data do recebimento da comunicação enviada pela autoridade competente.

12.8. 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.

12.9. Na aplicação das sanções serão considerados (art. 156, §1º, da Lei nº 14.133, de 2021):

a) a natureza e a gravidade da infração cometida;
b) as peculiaridades do caso concreto;
c) as circunstâncias agravantes ou atenuantes;
d) os danos que dela provierem para o Contratante;
e) a implantação ou o aperfeiçoamento de programa de integridade, conforme normas e orientações dos órgãos de controle.

12.10. 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 (art. 159).

12.11. A personalidade jurídica do Contratado poderá ser desconsiderada sempre que utilizada com abuso do direito para facilitar, encobrir ou dissimular a prática dos atos ilícitos previstos neste Contrato ou para provocar confusão patrimonial, e, nesse caso, todos os efeitos das sanções aplicadas à pessoa jurídica serão estendidos aos seus administradores e sócios com poderes de administração, à pessoa jurídica sucessora ou à empresa do mesmo ramo com relação de coligação ou controle, de fato ou de direito, com o Contratado, observados, em todos os casos, o contraditório, a ampla defesa e a obrigatoriedade de análise jurídica prévia (art. 160, da Lei nº 14.133, de 2021)

12.12. 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. (Art. 161, da Lei nº 14.133, de 2021)

12.13. 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 14.133/21.

12.14. 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.

CLÁUSULA DÉCIMA TERCEIRA – DA EXTINÇÃO CONTRATUAL (art. 92, XIX)

13.1. O contrato será extinto quando vencido o prazo nele estipulado, independentemente de terem sido cumpridas ou não as obrigações de ambas as partes contraentes.

13.2. 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.

13.3. 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.

13.4. 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.

13.5. O contrato poderá ser extinto antes de cumpridas as obrigações nele estipuladas, ou antes do prazo nele fixado, por algum dos motivos previstos no artigo 137 da Lei nº 14.133/21, bem como amigavelmente, assegurados o contraditório e a ampla defesa.

13.5.1. Nesta hipótese, aplicam-se também os artigos 138 e 139 da mesma Lei.

13.5.2. 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.

13.5.3. Se a operação implicar mudança da pessoa jurídica contratada, deverá ser formalizado termo aditivo para alteração subjetiva.

13.6. O termo de extinção, sempre que possível, será precedido:

13.6.1. Balanço dos eventos contratuais já cumpridos ou parcialmente cumpridos;

13.6.2. Relação dos pagamentos já efetuados e ainda devidos;

13.6.3. Indenizações e multas.

13.7. 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 (art. 131, *caput,* da Lei n.º 14.133, de 2021).

13.8. 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 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 (art. 14, inciso IV, da Lei n.º 14.133, de 2021).

CLÁUSULA DÉCIMA QUARTA – DOTAÇÃO ORÇAMENTÁRIA (art. 92, VIII)

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 (art. 92, III)

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 – ALTERAÇÕES

16.1. Eventuais alterações contratuais reger-se-ão pela disciplina dos arts. 124 e seguintes da Lei nº 14.133, de 2021.

16.2. 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.

16.3. 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).

16.4. 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.

CLÁUSULA DÉCIMA SÉTIMA – PUBLICAÇÃO

17.1. 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 OITAVA– FORO (art. 92, §1º)

18.1. Fica eleito o Foro da Justiça Federal em Brasília/DF, 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 14.133/21.

[Local], [dia] de [mês] de [ano].

_____

Representante legal do CONTRATANTE

_____

Representante legal do CONTRATADO

TESTEMUNHAS:

1-

2-