IMPUGNAÇÃO E RESPOSTA

Referência: Processo Sei Nº 01300.005789/2023-78
Assunto: 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.

Descrevemos abaixo os pedidos de impugnações apresentado tempestivamente por empresas, na qualidade de licitante interessada em participar do Pregão Eletrônico nº 90009/2024, com suas respectivas respostas.

Impugnação 1:

1 TEMPESTIVIDADE

Inicialmente, esta peça é tempestiva. O prazo para impugnação ao Edital, conforme disposto no seu item 10.1, encerra-se no terceiro dia anterior à data de realização da licitação, no caso, em 13/11/2024 (quarta-feira), visto que a data da abertura da sessão pública está designada para o dia 19/11/2024 (terça-feira).

Assim, esta impugnação é tempestiva, impugnando-se desde já as alegações em contrário.

2 SÍNTESE E MÉRITO

Trata-se de Pregão Eletrônico n. 90009/2024, no qual o CNPq objetiva contratar "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."

Quando da publicação do primeiro edital, a Ponto Sec apresentou Impugnação ao instrumento convocatório, alegando, de modo extremamente pontual, o seguinte (vide Impugnação 3):

1. Restrição Injustificada, visto que o edital exige a aquisição de produtos da Trend Micro, com a justificativa de padronização e facilidade de gestão centralizada. Contudo, outras marcas poderiam oferecer soluções integradas e compatíveis, sem comprometer a segurança e eficiência dos sistemas, aumentando a concorrência e reduzindo custos;

2. Possibilidade de Divisão da Compra por Grupos: A empresa sugere a separação dos serviços licitados em grupos, como soluções de antispam e

segurança para endpoints, possibilitando a participação de diversos fabricantes e promovendo uma concorrência mais ampla e justa;

3. Ausência de Justificativa Técnica Adequada: Conforme o art. 41 da Lei 14.133/2021, indicações de marca devem ser justificadas formalmente por parecer técnico. A impugnação destacou que o edital carecia de justificativas técnicas robustas para a exclusividade da Trend Micro, citando, inclusive, jurisprudência do Tribunal de Contas da União (TCU) que reprova a restrição de marcas sem um estudo comparativo de alternativas.

4. Expansão Injustificada do Objeto: O escopo da contratação foi ampliado para incluir novos produtos da Trend Micro, sem justificativa técnica para a escolha desse fabricante específico. Na conclusão, a Impugnante solicitou a revisão do Edital para propor que o CNPq fizesse os ajustes para ampliar a concorrência, garantindo a possibilidade de oferta por outros fabricantes e a separação das soluções em grupos, além de adequar as justificativas técnicas conforme os requisitos legais. Ato seguinte, em Decisão publicada em 21/10/2024, às 11h29, a Comissão de Licitação julgou PROCEDENTE a Impugnação apresentada para REALIZAR as devidas RETIFICAÇÕES em relação ao que foi apontado.

(...)

Destaca-se, ainda, que além da Impugnação 3, da ora Impugnante, a Impugnação 2, apresentada por uma outra empresa, também foi PROVIDA, para que o edital fosse retificado a fim de “preservar os princípios da legalidade, isonomia e competitividade do certamente.

No entanto, para surpresa da Impugnante, ambos editais são extremamente similares e não houve qualquer alteração substancial e relacionada a(s)Impugnação(ões) apresentada(s). Veja-se a o percentual de similaridade dos arquivos (o relatório foi feito na plataforma Copyleaks):

(...)

Assim, não houve quaisquer alterações relevantes no instrumento convocatório, o que causa estranheza, haja vista que, a despeito de uma alteração ou outra de palavra, as exigências CONTINUAM DIRECIONANDO O CERTAME PARA UMA TREND MICRO.

(...)

A gestão centralizada de segurança é, de fato, um aspecto relevante em qualquer ambiente de TI, no entanto, isso não significa que apenas uma marca específica seja capaz de atender a esse requisito. Atualmente, existem diversas soluções no mercado, as quais citamos anteriormente, dentre outras, que oferecem funcionalidades semelhantes ou superiores e permitem integração via API com sistemas e produtos de diferentes fabricantes.

Portanto, a justificativa de padronização da gestão centralizada ou, ainda, de que a padronização gera mais segurança, não deveria ser usada para restringir a participação de outros fornecedores, já que não há exclusividade tecnológica que justifique essa limitação. Pelo contrário, abrir o processo a outros fabricantes poderia trazer mais inovação e variedade de opções, mantendo a gestão centralizada, além de elevar o nível de proteção cibernética do ambiente.

Portanto, restam afastados e impugnados os argumentos que justificariam a indicação da Trend Micro.

Para além, não se pode deixar de observar que o Edital está acompanhado do Estudo Técnico Preliminar da Contratação, no qual há as supostas justificativas – já trazidas anteriormente – para indicação da fabricante Trend Micro. Todavia, conforme trazido acima, nenhuma das justificativas se sustenta, vez que não há NENHUMA EXIGÊNCIA QUE SEJA DE EXCLUSIVIDADE TECNOLOGICA DA TREND MICRO.

Nesse ponto, passemos a análise do Item 9.6, no qual há uma "Análise das Soluções Viáveis" para atendimento dos requisitos do Edital.

(...)

Na análise da equipe técnica, somente a Trend Micro poderia atender todas as exigências e necessidades do CNPq, contudo, trata-se, com o devido acatamento, de análise no mínimo EQUIVOCADA.

Explica-se. A visibilidade unificada, assim como o gerenciamento e compartilhamento de eventos e políticas, é uma característica comum a todos os players mencionados na pesquisa (Symantec (Broadcom), Sophos, Trellix e, adicionalmente, Kaspersky), não se trata de características exclusivas da Trend Micro.

Com o devido acatamento, o que se percebe é que na nova publicação do Edital, houve apenas uma alteração das justificativas para a manutenção do pregão direcionado para Trend Micro, sem, contudo, considerar de fato que as exigências trazidas são sim atendidas por todos os principais players do seguimento.

(...)

Com apenas esses três fabricantes, já se demonstra que a argumentação de exclusividade da Trend Micro para atender às necessidades do CNPq é insuficiente, haja vista que, com a separação em dois grupos, seria muito mais factível o respeito à ampla concorrência e a obtenção de melhores preços.

O que se vê, portanto, é que a análise que fundamentou a escolha da Trend Micro parece baseada em informações que favorecem essa tecnologia de forma

injustificável, vez que somente gerará prejuízo aos cofres públicos em prejuízo à ampla concorrência.

Lado outro, o edital seria ainda MENOS RESTRITIVO e permitiria ainda mais a AMPLA CONCORRÊNCIA para OBTENÇÃO DA PROPOSTA MAIS VANTAJOSA, caso houvesse separação da solução de antispam em um grupo distinto, ou seja, a contratação seria divida em grupos.

Com isso – e com a correção da tabela para incluir referências de atendimento de diferentes fabricantes e tecnologias –, tem-se a possibilidade de participação de cinco (5) fabricantes/tecnologias distintas, o que enfraquece argumento de que outros players do mercado não poderiam atender às necessidades da contratante.

No cenário proposto (separação da licitação em grupos), a Impugnante analisou as soluções tecnológicas viáveis e consolidou as funcionalidades de cada uma, visando verificar o grau de atendimento às necessidades de segurança cibernética do CNPq.

Nesse ponto, com a separação da solução de antispam em um grupo específico, torna possível o atendimento por cinco fabricantes: Trend Micro, Symantec (Broadcom), Sophos, Trellix e Kaspersky, ampliando o leque de alternativas para além de um único fornecedor. A fim de justificar a possibilidade e ausência de prejuízo da separação por grupos, temos que o próprio Estudo Técnico Preliminar faz a referência ao quadrante do Gartner que versa EXCLUSIVAMENTE a Endpoint Protection Platform - EPP.

Da mesma forma, a referência utilizada da Forrester Wave também se relaciona à proteção de endpoints, evidenciando que ambas as avaliações são específicas para proteção de endpoints e não abrangem diretamente o segmento de antispam.

(...)

3 CONCLUSÃO

Diante do exposto, pugna-se por que sejam realizadas as modificações pertinentes no Edital de Licitação, atendendo-se às prescrições do art. 164, parágrafo único, da Lei n. 14.133/2021.

Resposta a Impugnação 1:

1. Em resposta ao pedido de impugnação apresentado pela empresa em relação ao Edital do Pregão Eletrônico 90009/2024, destinado à contratação de soluções integradas de tecnologia para segurança de endpoints, servidores de rede, antispam, ambiente de colaboração, dispositivos móveis, ambiente de containers e gerenciamento de superfície de ataque, com atualização contínua, garantia, suporte técnico e treinamento, temos as seguintes considerações.

2. Na publicação anterior deste Edital, o CNPq analisou e acolheu os pedidos de impugnação apresentados por duas licitantes, CentralTech e Cyberdefend, com o objetivo de preservar os princípios da legalidade, isonomia e competitividade. Em razão dessas impugnações, foi realizada a republicação do edital com as alterações pertinentes. O Estudo Técnico Preliminar foi revisado e ampliado, e o Termo de Referência atualizado, atendendo aos pontos levantados.

3. O pedido de impugnação atual alega que não houve alteração substancial no edital, mas constatamos que as imagens e os textos utilizados pela impugnante refletem documentos e informações da versão anterior do edital, baseando-se apenas em ferramenta comparativa de linhas de texto de PDF, o que é inadequado para um certame desta importância. Ademais, as alegações apresentadas, além de serem equivocadas, demonstram um desconhecimento dos documentos atuais, como evidenciado por: 1) a citação incorreta dos itens 2.26 e 2.36 do Termo de Referência, inexistentes na versão atual; 2) alegação de erro no item referente ao treinamento (item 9 do Termo de Referência), já corrigido e revisado; 3) afirmação da ausência de parecer técnico (inc. I, art. 43), contrariada ao longo do Estudo Técnico Preliminar que detalha as especificações técnicas, requisitos necessários e análises comparativas de soluções de segurança disponíveis no mercado; 4) suposta falta de despacho da autoridade superior (inc. II, art. 43), já presente e assinado no Estudo Técnico Preliminar; 5) referência desatualizada ao quadro de análise (antes item 9.6 e agora item 9.4.2), que foi revisado e atualizado, com mais funcionalidades e critérios de seleção.

4. A justificativa da pretensa contratação, conforme exaurido no Estudo Técnico Preliminar e no Termo de Referência, visa adotar soluções robustas de segurança para proteção dos ativos de TI, garantindo a integridade, confidencialidade e disponibilidade dos dados do CNPq, visto que em ataques cibernéticos recentes a órgãos do Governo Federal, grupos de hackers têm considerado sistemas de governo como alvos compensadores, no intuito de provocar diferentes impactos. Uma vez que o CNPq não possui soluções dedicadas para gerar visibilidade centralizada de eventos de segurança, a pretendida 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.

5. 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* e *phishing,*a exploração de vulnerabilidades específicas em *containers* e dispositivos móveis exigem uma abordagem mais ampla e integrada. Expandir a cobertura de segurança reduz consideravelmente a probabilidade e o impacto de incidentes cibernéticos. Brechas em ambientes não protegidos 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.

6. Conforme é demonstrado no estudo técnico, evidentemente não observado pela impugnante neste pedido, expandiu-se a análise das soluções de segurança para as principais disponíveis no mercado, englobando, também, as soluções da Symantec, Sophos, Trellix e Kaspersky mencionadas pela impugnante.

7. Além dos recursos técnicos especificados no Estudo Técnico Preliminar (5. Necessidades tecnológicas) e no Termo de Referência (Anexo VII – Requisitos técnicos das soluções), foram estabelecidos como critérios de seleção a presença de funcionalidades essenciais para o fortalecimento do ambiente de cibersegurança do CNPq, bem como o atendimento aos controles do Programa de Privacidade e Segurança da Informação – PPSI do Governo Federal. Citam-se: proteção de anti-malware, firewall integrado, EDR, XDR, *machine learning*, proteção contra *exploits* e *ransomware*, gerenciamento centralizado, DLP, integração com SIEM, controle de dispositivos, *whitelist* de aplicações, proteção pra dispositivos móveis, ambientes virtualizados, *containers*, multinuvem, e-mail e colaboração, automação de resposta a ameaças, análises forenses, *rollback*, *behavioral analysis, sandboxing* e *threat hunting.*

8. A análise comparativa das soluções está detalhada nos itens 9.4 (Cenário 4 - Contratação de nova solução para proteção dos de risco e superfície de ataque), 9.4.1 (Análise comparativa entre as soluções de segurança listadas no cenário 4), 9.4.2 (Análise comparativa das soluções dos fabricantes avaliados), 9.5 (Observância das alternativas às políticas, premissas e especificações técnicas vigentes) e 9.6 (Escolha da solução viável) do Estudo Técnico Preliminar ora publicado. Destaca-se que, além dos aspectos técnicos, a escolha da solução também utilizou-se de critérios quanto aos recursos funcionais disponíveis e alinhados às necessidades do CNPq, os aspectos sobre a estabilidade e confiança na solução, a facilidade de expansão, a redução do aprendizado, o tempo e a complexidade de migração.

9. As licitações públicas devem assegurar 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. 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.

10. 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, 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.

11. 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.

12. 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. Também deve-se ressaltar os aspectos técnicos que colaboram com esta decisão, tais como: 1) 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; 2) 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; 3) 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.

13. 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.

14. 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".*

15. 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 no certame.

16. 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.

17. 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.

18. Diante de todo o exposto no planejamento desta contratação, foi selecionada a solução ideal para o ambiente do CNPq quanto à proteção dos *endpoints*, servidores, *mobiles, containers*, e-mail, ambiente de colaboração e gerenciamento de risco e superfície de ataque, por meio de um amplo estudo comparativo de diversos cenários e 8 (oito) soluções de diferentes fabricantes conhecidos no mercado.

19. Resta claro que as alegações da impugnante utilizam-se de referências erradas e documentos defasados e também apontam evidente tendência a tumultuar o processo licitatório, prejudicando o interesse público.

20. O uso de informações incorretas e de documentos ultrapassados indica despreparo ou desinteresse genuíno em contribuir com a lisura do processo. A empresa, ao ignorar o Edital publicado, compromete a objetividade e a pertinência do pedido de impugnação, o que pode ser visto como um indício de má-fé ou, ao menos, de desleixo. Esse tipo de prática gera trabalho desnecessário para a comissão responsável pela licitação e não contribui para a melhoria do edital ou das condições do contrato, que é o objetivo legítimo de uma impugnação.

21. Ao apresentar impugnações infundadas e já sanadas anteriormente, a empresa parece buscar atrasar o andamento da licitação, interferindo de maneira negativa e sem justificativa sólida. Esse tipo de conduta compromete a eficiência e a agilidade do processo licitatório, que já é, por natureza, rigoroso e detalhado. A insistência em questões previamente resolvidas aponta para uma tentativa de tumultuar o processo, possivelmente para impedir a conclusão dentro dos prazos previstos.

22. Quando uma empresa apresenta impugnações meramente protelatórias, afeta diretamente o interesse público, que depende de soluções ágeis e eficazes para

questões de segurança. No caso de uma licitação para contratação de soluções de segurança, qualquer atraso pode ter consequências significativas, deixando a administração pública desprotegida ou desatualizada em relação a suas necessidades de segurança. Atrasos neste tipo de licitação comprometem a continuidade e eficácia dos serviços, impactando não apenas a administração, mas também a sociedade que depende dessas soluções para a segurança coletiva.

23. O tempo e os recursos gastos pela administração pública para responder a impugnações sem base válida representam desperdício de recursos, desviando esforços que poderiam ser direcionados para outras atividades essenciais. Este tipo de prática consome horas de trabalho de servidores, assessores jurídicos e demais envolvidos, gerando custo que, na prática, são pagos pela sociedade.

24. Desta feita, **não acatamos o pedido de impugnação proposto pela empresa.**

Impugnação 2:

• Exclusividade de Marca e Direcionamento do Edital

O Termo de Referência alega que a contratação da solução Trend Micro é a única capaz de atender às necessidades do CNPq, principalmente no que se refere à visibilidade unificada de ameaças e à detecção de ataques cibernéticos. Entretanto, diversas soluções de mercado oferecem recursos equivalentes e são amplamente reconhecidas por sua eficácia em proteção de endpoints e detecção de ameaças, com Gerenciamento Centralizado. Restringir o certame à Trend Micro sem justificativa técnica adequada viola o princípio da competitividade (art. 5º, II, da Lei 14.133/2021).

• Da Equivalência Técnica das Soluções de Segurança

Fabricantes como Broadcom (Symantec), Sophos, Kaspersky e Trellix, dentre outros, oferecem soluções que atendem plenamente às especificações técnicas do edital, incluindo proteção de endpoints, gerenciamento de superfície de ataque e integração com ambientes de colaboração. Essas soluções também incluem funcionalidades avançadas, como análise de ameaças baseada em inteligência artificial e integração com ferramentas de orquestração, assegurando a robustez e a eficiência das defesas cibernéticas, conforme necessário.

• Gestão Centralizada e Automação de Respostas a Incidentes

Soluções como o Sophos Central e o Symantec Endpoint Protection Manager oferecem visibilidade unificada e capacidade de gerenciamento centralizado, com respostas automatizadas a incidentes de segurança, características que o edital atribui exclusivamente à Trend Micro. Ambas as soluções são amplamente adotadas por grandes instituições e possuem integração com APIs, permitindo

comunicação com sistemas de outros fabricantes existentes no CNPq e facilitando a adaptação a ambientes híbridos.

• Da Falta de Justificação Técnica Adequada para Exclusividade

A escolha exclusiva pela Trend Micro carece de justificativas técnicas que atendam ao art. 41, I, da Lei 14.133/2021, que exige parecer técnico e despacho motivado da autoridade superior para a indicação de marca. A análise de mercado deveria ter incluído outras soluções igualmente qualificadas, conforme indicado pelo TCU no Acórdão 214/2020-Plenário. Ademais, o edital menciona a necessidade de padronização (art. 41, I, "a" da Lei 14.133/2021), mas essa padronização deve ser acompanhada de justificativa adequada, com parecer técnico e análise de contratações anteriores, o que não se verifica no caso.

• Pedido

Diante dos pontos apresentados, solicita-se a revisão das especificações técnicas do edital e a eliminação de exigências que direcionam para um único fabricante. A flexibilização das exigências e a abertura para outras soluções viabilizariam maior concorrência, possibilitando a obtenção de propostas mais vantajosas e em conformidade com os princípios da economicidade e da ampla competitividade.

Resposta a Impugnação 2:

1. Em resposta ao pedido de impugnação apresentado pela empresa em relação ao Edital do Pregão Eletrônico 90009/2024, destinado à contratação de soluções integradas de tecnologia para segurança de endpoints, servidores de rede, antispam, ambiente de colaboração, dispositivos móveis, ambiente de containers e gerenciamento de superfície de ataque, com atualização contínua, garantia, suporte técnico e treinamento, apresentamos as seguintes considerações.

2. No estudo técnico desta contratação, expandiu-se a análise das soluções de segurança para as principais disponíveis no mercado, incluindo as soluções da Symantec, Sophos, Kaspersky e Trellix mencionadas pela impugnante. Além das especificações técnicas detalhadas no Estudo Técnico Preliminar (item 5 - Necessidades tecnológicas) e no Termo de Referência (Anexo VII - Requisitos técnicos das soluções), foram estabelecidos como critérios de seleção a presença de funcionalidades essenciais para o fortalecimento do ambiente de cibersegurança do CNPq, bem como o atendimento aos controles do Programa de Privacidade e Segurança da Informação (PPSI) do Governo Federal, não se restringindo apenas às funcionalidades de gestão centralizada, automação de respostas a incidentes e inteligência artificial, conforme citado pela empresa. Utilizou-se, também, como critério a presença de funcionalidades essenciais para o CNPq, tais como: proteção contra malware, firewall integrado, EDR, XDR, machine learning, proteção contra exploits e ransomware, gerenciamento centralizado, DLP, integração com SIEM, controle de dispositivos, lista branca de aplicações, proteção para dispositivos móveis, ambientes virtualizados, containers,

multinuvem, e-mail e colaboração, automação de resposta a ameaças, análise forense, rollback, análise comportamental, sandboxing e threat hunting.

3. A análise comparativa das soluções está detalhada nos itens 9.4 (Cenário 4 - Contratação de nova solução para proteção dos ativos de risco e superfície de ataque), 9.4.1 (Análise comparativa entre as soluções de segurança listadas no cenário 4), 9.4.2 (Análise comparativa das soluções dos fabricantes avaliados), 9.5 (Observância das alternativas às políticas, premissas e especificações técnicas vigentes) e 9.6 (Escolha da solução viável) do Estudo Técnico Preliminar ora publicado. Na pesquisa, foram comparadas oito das principais soluções de segurança, destacando-se que, além dos aspectos técnicos, a escolha da solução considerou a disponibilidade de recursos funcionais alinhados às necessidades do CNPq (disponibilizados em quadro comparativo), a estabilidade e confiabilidade da solução, a facilidade de expansão, a redução no tempo de aprendizado, o tempo e a complexidade de migração e o investimento realizado na solução já implantada.

4. Salienta-se que a afirmação da impugnante sobre a ausência de parecer técnico (inciso I, art. 43) é contradita ao longo do Estudo Técnico Preliminar, assim como a alegada falta de despacho da autoridade superior (inciso II, art. 43), o qual está presente e assinado neste mesmo documento. Conforme preconizado pela Lei, o Estudo Técnico Preliminar está anexado ao Edital deste Pregão.

5. As licitações públicas devem assegurar igualdade de condições, consolidando o princípio constitucional da isonomia. Porém, para alcançar esse objetivo, é necessário observar que a finalidade da licitação é selecionar a proposta mais vantajosa para a Administração Pública. Assim, o objetivo da Administração não é acomodar, nas licitações públicas, qualquer solução excêntrica em torno do objeto pretendido, mas garantir ampla concorrência no atendimento das suas necessidades. Ressalta-se que diversas revendas do fabricante Trend Micro estão aptas e autorizadas a comercializar seus produtos e serviços, garantindo a competitividade no certame.

6. A definição da marca se baseia no princípio da padronização do ambiente, da continuidade da solução e da 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 problemas causados por incompatibilidades. Esse princípio está alinhado aos princípios da legalidade, finalidade, economicidade, interesse público e vantagem para a Administração Pública Federal (APF), sem prejuízo dos demais princípios que norteiam a contratação de bens e serviços para a APF. Por questões estratégicas e operacionais, é importante utilizar produtos que apresentem configuração, manutenção e operacionalidade iguais ou similares às atualmente instaladas, tornando o processo de implantação, operação e transmissão de conhecimento menos complexo, mais rápido 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 de operação da solução atual. Essa experiência assegura melhores condições para identificar e resolver problemas,

bem como para controlar e fiscalizar os serviços de segurança contratados, proporcionando efetividade e monitoramento eficiente dos serviços. A continuidade da solução mostra-se vantajosa, pois atendeu, ao longo dos anos, aos requisitos de segurança, sendo eficaz e eficiente nas ações preventivas de proteção de endpoints e servidores, além de proporcionar resposta rápida em incidentes.

7. O parcelamento da solução de TIC mostrou-se inviável, pois licenças, serviços de instalação, configuração, garantia, suporte do fabricante e repasse de conhecimento constituem uma solução unificada. É essencial que esses itens sejam fornecidos em conjunto, sem parcelamento, para garantir a implantação eficaz 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". Assim, a aquisição dos itens em lote único assegura compatibilidade entre todos os componentes, garantindo a harmonia e o desempenho adequado da solução, além de facilitar a manutenção, o suporte técnico e a garantia, já que todos os elementos estão integrados e fornecidos por um único provedor.

8. O propósito é alcançar uma solução única, gerenciada de forma centralizada, para atender quantitativa e 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. Conforme previsto na Lei nº 14.133/2021, em seu artigo 18, parágrafo único, o não parcelamento do objeto poderá ser adotado, desde que justificado, visando evitar a perda de economia de escala, a redução da segurança, a padronização necessária ou a eficiência.

9. 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 só fortalece a integração e a interoperabilidade entre os serviços, como também possibilita um melhor aproveitamento dos recursos compartilhados pela contratada. Essas características são fundamentais para garantir a sustentabilidade e eficácia do ciclo de vida dos serviços, alinhando-se aos objetivos do contrato e reforçando o princípio da economicidade que rege a administração pública. A Lei nº 14.133/2021 estabelece que o parcelamento deve ser considerado como regra para ampliar a competitividade, exceto quando uma justificativa técnica demonstra 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, conforme já justificado tecnicamente, o não parcelamento do objeto será adotado para garantir maior segurança, padronização e eficiência.

10. 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 novos custos para o CNPq. Cada lote exigiria uma nova etapa de implantação e configuração, gerando despesas adicionais consideráveis. A contratação parcelada também aumentaria os gastos com treinamento, pois cada solução 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, com diferentes prazos e condições de atendimento, prejudicando a eficiência e aumentando a complexidade da gestão.

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

12. Diante de todo o exposto no planejamento desta contratação, foi selecionada a solução ideal para o ambiente do CNPq quanto à proteção dos endpoints, servidores, dispositivos móveis, containers, e-mail, ambiente de colaboração e gerenciamento de risco e superfície de ataque, por meio de um amplo estudo comparativo de diversos cenários, alinhado às necessidades deste órgão e em conformidade com a Lei.

13. Diante disso, **não acatamos o pedido de impugnação proposto pela empresa.**

Impugnação 3:

1. Da Restrição Injustificada à Competitividade

O edital exige a utilização de produtos da Trend Micro para solução de segurança cibernética, limitando a possibilidade de outras empresas oferecerem suas soluções e violando os princípios da ampla concorrência e da isonomia, estabelecidos pelo art. 3º, §1º, da Lei 8.666/93 e pelo art. 5º, II, da Lei 14.133/2021. Essa exigência impede a Administração de avaliar alternativas igualmente robustas e, potencialmente, mais vantajosas economicamente, o que contraria o princípio da economicidade previsto no art. 2º, IV, da Lei 14.133/2021.

2. Da Inexistência de Exclusividade Tecnológica

O Termo de Referência justifica a exclusividade da Trend Micro alegando que apenas essa solução oferece gestão centralizada e visibilidade unificada de eventos de segurança. Contudo, soluções oferecidas por outros fabricantes, como a *Sophos Central*, *Kaspersky Security Center* e *Broadcom (Symantec) Endpoint Protection*, possuem capacidade de gestão centralizada e são amplamente reconhecidas como eficazes em relatórios de mercado, como o *Gartner Magic Quadrant* para plataformas de proteção (EPP) de endpoints referenciado no Edital versa.

Esses fabricantes disponibilizam plataformas que permitem o gerenciamento unificado de endpoints, servidores, dispositivos móveis, conteiners e ambientes de colaboração, além de oferecer integração via API para facilitar a comunicação entre diferentes soluções existentes no ambiente do CNPq. A argumentação de exclusividade tecnológica da Trend Micro, portanto, é falha e não justifica a restrição à participação de outros fabricantes.

3. Da Gestão Centralizada e Integração de Sistemas de Segurança

A gestão centralizada de segurança é essencial para a Administração, no entanto, a alegação de que apenas a Trend Micro possui essa capacidade não se sustenta. Soluções como a *Symantec Endpoint Protection* e o *Kaspersky Security Center* também oferecem consoles de gerenciamento integrados que permitem a monitorização, configuração e resposta a incidentes de forma unificada. Tais consoles são projetados para oferecer visibilidade abrangente sobre a segurança da rede, sendo capazes de se integrar com soluções de terceiros e oferecendo capacidades de automação e orquestração de segurança.

Além disso, todos esses fabricantes ofertam soluções que disponibilizam proteção para ambientes complexos, como redes multi-nuvem e sistemas híbridos, com suporte a dispositivos físicos, virtuais e baseados em contêineres, conforme as necessidades descritas no edital.

4. Da Justificativa Inadequada de Curva de Aprendizado

O edital justifica a escolha da Trend Micro com base na continuidade da ferramenta e na “curva de aprendizado” dos usuários. No entanto, a própria necessidade de treinamento e atualização exigida no contrato indica que todos os usuários precisarão passar por capacitação, independentemente da solução. Soluções de fabricantes como Sophos, Kaspersky e Broadcom oferecem interfaces amigáveis e bem documentadas, além de suporte técnico abrangente, facilitando a adaptação dos usuários e garantindo eficiência sem prejuízo à curva de aprendizado. Assim, o argumento de economia de tempo em adaptação não justifica a escolha de uma única marca.

5. Da Possibilidade de Maior Competitividade e Redução de Custos

A contratação em grupo único, com todos os serviços integrados, restringe a competitividade e eleva o custo da contratação. A Administração Pública poderia considerar a divisão do processo em grupos, separando a solução de antispam, por exemplo, de outras soluções de segurança. Isso permitiria a participação de fabricantes que oferecem soluções específicas para diferentes segmentos, ampliando a competição e permitindo maior variação de preços e descontos.

6. Pedido de Providências

Diante do exposto, requer-se a revisão do edital para excluir especificações que direcionam o certame para um único fornecedor, permitindo a ampla concorrência e possibilitando a obtenção da proposta mais vantajosa para a Administração. Recomenda-se a divisão em grupos distintos (EPP e Mensageria) possibilitando a participação de diversos fabricantes por GRUPO, garantindo maior competitividade, inovação tecnológica e mantendo-se a Gestão Centralizada.

Resposta a Impugnação 3:

1. Em resposta ao pedido de impugnação apresentado pela empresa em relação ao Edital do Pregão Eletrônico 90009/2024, destinado à contratação de soluções integradas de tecnologia para segurança de endpoints, servidores de rede, antispam, ambiente de colaboração, dispositivos móveis, ambiente de containers e gerenciamento de superfície de ataque, com atualização contínua, garantia, suporte técnico e treinamento, temos as seguintes considerações.

2. A justificativa da pretensa contratação, conforme exaurido no Estudo Técnico Preliminar e no Termo de Referência, visa adotar soluções robustas de segurança para proteção dos ativos de TI, garantindo a integridade, confidencialidade e disponibilidade dos dados do CNPq, visto que em ataques cibernéticos recentes a órgãos do Governo Federal, grupos de hackers têm considerado sistemas de governo como alvos compensadores, no intuito de provocar diferentes impactos. Uma vez que o CNPq não possui soluções dedicadas para gerar visibilidade centralizada de eventos de segurança, a pretendida 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. 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, a exploração de vulnerabilidades específicas em containers e dispositivos móveis exigem uma abordagem mais ampla e integrada. Expandir a cobertura de segurança reduz consideravelmente a probabilidade e o impacto de incidentes cibernéticos. Brechas em ambientes não protegidos 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.

4. Conforme é demonstrado no estudo técnico, expandiu-se a análise das soluções de segurança para as principais disponíveis no mercado, englobando, também, as soluções da Symantec, Sophos e Kaspersky mencionadas pela impugnante. Além dos recursos técnicos especificados no Estudo Técnico Preliminar (5. Necessidades tecnológicas) e no Termo de Referência (Anexo VII – Requisitos técnicos das soluções), foram estabelecidos como critérios de seleção a presença de funcionalidades essenciais para o fortalecimento do ambiente de cibersegurança do CNPq, bem como o atendimento aos controles do Programa de Privacidade e Segurança da Informação – PPSI do Governo Federal. Citam-se: proteção de anti-malware, firewall integrado, EDR, XDR, machine learning, proteção contra exploits e ransomware, gerenciamento centralizado, DLP, integração com SIEM, controle de dispositivos, whitelist de aplicações, proteção pra dispositivos móveis, ambientes virtualizados, containers, multinuvem, e-mail e colaboração, automação de resposta a ameaças, análises forenses, rollback, behavioral analysis, sandboxing e threat hunting.

5. A análise comparativa das soluções está detalhada nos itens 9.4 (Cenário 4 - Contratação de nova solução para proteção dos de risco e superfície de ataque), 9.4.1 (Análise comparativa entre as soluções de segurança listadas no cenário 4), 9.4.2 (Análise comparativa das soluções dos fabricantes avaliados), 9.5 (Observância das alternativas às políticas, premissas e especificações técnicas vigentes) e 9.6 (Escolha da solução viável) do Estudo Técnico Preliminar ora publicado. Destaca-se que, além dos aspectos técnicos, a escolha da solução também utilizou-se de critérios quanto aos recursos funcionais disponíveis e alinhados às necessidades do CNPq, os aspectos sobre a estabilidade e confiança na solução, a facilidade de expansão, a redução do aprendizado, o tempo e a complexidade de migração.

6. As licitações públicas devem assegurar 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. 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.

7. 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.

8. 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.

9. 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. Também deve-se ressaltar os aspectos técnicos que colaboram com esta decisão, tais como: 1) 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; 2) 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; 3) 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. 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.

11. 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".

12. 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 no certame.

13. 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.

14. 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.

15. Diante de todo o exposto no planejamento desta contratação, foi selecionada a solução ideal para o ambiente do CNPq quanto à proteção dos endpoints, servidores, mobiles, containers, e-mail, ambiente de colaboração e gerenciamento de risco e superfície de ataque, por meio de um amplo estudo comparativo de diversos cenários e 8 (oito) soluções de diferentes fabricantes conhecidos no mercado.

16. Desta feita, **não acatamos o pedido de impugnação proposto pela empresa.**

Serviço de Compras e Licitações - SELIC