GOVERNO DO ESTADO DE RONDÔNIA
Superintendência Estadual de Compras e Licitações - SUPEL
Comissão de Tecnologia - SUPEL-COTEC

RESPOSTA

RESPOSTA AO PEDIDO DE ESCLARECIMENTO

PREGÃO ELETRÔNICO: Nº. 90236/2025/SUPEL/RO

PROCESSO ADMINISTRATIVO: Nº. 0036.028242/2024-36

OBJETO: Registro de Preços para contratação de empresa para fornecimento, sob demanda, de solução de segurança para proteção de e-mail, Endpoint e proteção contra ataques avançados, incluindo instalação, configuração, repasse de conhecimento, suporte técnico e garantia, para atender às necessidades da Secretaria de Estado da Saúde - SESAU/RO, por um período de 01 (um) ano, podendo ser prorrogado, conforme a Lei Federal nº 14.133 de 1° de abril de 2021.

A Superintendência Estadual de Licitações - SUPEL, através de seu Pregoeiro Substituto e Equipe de Apoio, nomeados por força das disposições contidas na Portaria nº 158/2026/GAB/SUPEL/RO, publicada no DOE de 07 de julho de 2026, informa que elaborou resposta ao Pedido de Esclarecimento apresentado por empresa interessada, interposto em face do PE 90236/2025/SUPEL/RO, conforme abaixo.

1. DAS PRELIMINARES

Em sede de admissibilidade, verificou-se que foram preenchidos os pressupostos de legitimidade, interesse processual, fundamentação e tempestividade (nos termos da Lei Federal N.° 14.133/2021, art. 164, e do item 6 do Instrumento Convocatório), no que se refere à empresa A, B, C, D, E e F, conforme documentos de Id. (74286070, 74288553, 74290105 e 74291183), regularmente colacionado aos autos do processo administrativo SEI.

Não obstante, considerando a pertinência das matérias suscitadas, os pedidos apresentados foram analisados em sua integralidade, razão pela qual passa-se à formulação da Resposta ao Pedido de Esclarecimento.

2. DO PEDIDO DE ESCLARECIMENTO E DA RESPOSTA DA SESAU-NSC

2.1 SÍNTESE DO PEDIDO DE ESCLARECIMENTO EMPRESA A, ID. (73115722 e 73366589):

(...)

1. Item 8.10.2.1.1 a 8.10.2.1.13 e 8.10.2.1.173 a 8.10.2.1.188 – Compatibilidade com Sistemas Operacionais Legados.

Considerando a diversidade de sistemas operacionais especificados no edital, incluindo plataformas legadas ou descontinuadas por seus fabricantes, tais como Windows 2000, Windows Server 2003, AIX 6.1, Solaris 10 e distribuições Linux em versões antigas, solicitamos esclarecer se o atendimento ao requisito poderá considerar as limitações técnicas inerentes a estes sistemas operacionais, especialmente em funcionalidades avançadas de detecção, investigação e resposta disponibilizadas pelas soluções de segurança mais recentes.

2.Item 8.10.2.1.15 – Compatibilidade de Navegadores

Considerando a descontinuação oficial do Internet Explorer pela Microsoft e a adoção dos navegadores modernos atualmente suportados pelo mercado, solicitamos esclarecer se serão aceitas soluções compatíveis com navegadores modernos equivalentes, tais como Microsoft Edge, Google Chrome e Mozilla Firefox.

3.Itens 8.10.3.1.2 a 8.10.3.1.4 – Mitigação de Ameaças em Rede

Solicitamos esclarecer se as funcionalidades de inspeção, detecção, correlação e mitigação de ameaças poderão ser atendidas por uma arquitetura composta por componentes integrados da mesma solução, desde que o conjunto da plataforma atenda integralmente aos requisitos previstos no edital.

4.Item 8.10.4.60 – Integração com Equipamentos de Rede

Solicitamos esclarecer se o requisito poderá ser considerado atendido por mecanismos de integração, APIs ou orquestração disponibilizados pela solução ofertada, desde que permitam executar ações automatizadas de contenção compatíveis com o ambiente da CONTRATANTE.

5.Item 3.2 – Descrição Detalhada do Objeto

CATMAT 27499 – Solução de segurança avançada para mitigação de ameaças na rede, observamos que na coluna "Throughput de dados" consta o valor "2".

Para o correto entendimento do requisito e dimensionamento da solução a ser ofertada, solicitamos esclarecer se o valor informado corresponde a 2 Gbps (gigabits por segundo) de throughput de rede ou se refere a outra unidade de medida

6.Entendemos que a exigência prevista no item 17.1, alínea "c", relativa à apresentação de "ato constitutivo, estatuto ou contrato social em vigor", abrange as sociedades anônimas (S/A), mediante apresentação do Estatuto Social e dos documentos comprobatórios de seus administradores. Está correto o entendimento?

(...)

2.2 DA MANIFESTAÇÃO DO SESAU-NSC, ID. (74286070):

(...)

1. Manifestação Técnica

Está correto o entendimento. Os requisitos do Termo de Referência estabelecem a compatibilidade da solução com os sistemas operacionais atualmente existentes no ambiente da SESAU. Considerando que determinados sistemas operacionais legados encontram-se fora do ciclo de suporte de seus fabricantes, serão aceitas as limitações técnicas inerentes à própria plataforma, desde que a solução ofertada possua suporte oficialmente declarado pelo fabricante para os respectivos sistemas operacionais e disponibilize o máximo de funcionalidades suportadas para cada plataforma. Eventuais restrições a recursos avançados de EDR, XDR, análise comportamental, investigação ou resposta automatizada, decorrentes exclusivamente das limitações dos sistemas operacionais legados, serão aceitas desde que devidamente documentadas pelo fabricante da solução.

2. **Manifestação Técnica**

Sim. Considerando que o Internet Explorer encontra-se oficialmente descontinuado pela Microsoft, serão aceitas soluções compatíveis com navegadores modernos amplamente utilizados e suportados pelo mercado, tais como Microsoft Edge, Google Chrome e Mozilla Firefox, ou outros navegadores equivalentes oficialmente suportados pelo fabricante da solução. O objetivo do requisito é garantir o pleno acesso e a operação das funcionalidades previstas no Termo de Referência, não havendo obrigatoriedade de compatibilidade exclusiva com o Internet Explorer.

3. Está correto o entendimento. As funcionalidades de inspeção, detecção, correlação e mitigação de ameaças serão consideradas atendidas quando disponibilizadas por componentes integrados pertencentes à mesma solução e ao mesmo fabricante, desde que o conjunto da plataforma atenda integralmente aos requisitos técnicos estabelecidos no edital. A Administração busca o atendimento funcional de forma integrada, com gerenciamento centralizado, interoperabilidade nativa e pleno atendimento aos requisitos do Termo de Referência, não sendo exigido que todos os recursos estejam concentrados em um único componente.

4. **Manifestação Técnica**

Sim. O requisito será considerado atendido desde que a solução possua mecanismos de integração com dispositivos de rede, tais como switches e roteadores, capazes de executar ações automatizadas de contenção e resposta a incidentes de segurança, incluindo alteração dinâmica de VLAN, isolamento de dispositivos, bloqueio de comunicação ou desativação de portas de rede. Tais funcionalidades poderão ser implementadas por meio de APIs, conectores, mecanismos de integração ou plataformas de orquestração disponibilizadas pelo fabricante da solução, desde que atendam integralmente aos requisitos técnicos do Termo de Referência e observem o disposto no

item 6.6 quanto à integração dos componentes da solução.

5. **Manifestação Técnica**

Esclarece-se que o valor “2” constante da linha do Item 3 (CATMAT 27499 — Solução de segurança avançada para mitigação de ameaças na rede) corresponde à QUANTIDADE do item, expressa na respectiva UNIDADE DE MEDIDA “Por Throughput de dados”, conforme a estrutura da tabela do item 3.2 do Termo de Referência (colunas “UNIDADE DE MEDIDA” e “QUANTIDADE”). Trata-se, portanto, de quantitativo de licenciamento da solução, e não de parâmetro técnico de desempenho. O valor “2” não representa, nem nunca representou, capacidade de inspeção de 2 (dois) Gbps. A capacidade técnica de throughput da solução é estabelecida, de forma vinculante, no item 8.10.3.1.2 do Termo de Referência, que exige solução dimensionada para inspecionar, no mínimo, 04 (quatro) Gbps de throughput. É esta a especificação que deve orientar o dimensionamento e a elaboração das propostas.

Registra-se que não há antinomia entre a tabela sintética do item 3.2 e a especificação técnica do item 8.10.3. O próprio instrumento convocatório estabelece, de forma expressa, a prevalência e a complementaridade da descrição técnica detalhada: (i) o item 3.2.1 do Termo de Referência dispõe que “a descrição completa dos objetos está presente no item 8 deste Termo de Referência”; e (ii) as cláusulas 4.2 e 4.3 do Edital fixam as especificações técnicas/quantidades nos itens 8.10 e 3.2 do Anexo I, prevalecendo as especificações do Anexo I em caso de divergência. Assim, a tabela do item 3.2 possui caráter sintético e deve ser lida em conjunto com o item 8, que a complementa e prevalece. Por conseguinte, será aceita a oferta de uma única solução/appliance NDR, ou arquitetura equivalente do mesmo fabricante, desde que devidamente dimensionada para inspecionar, no mínimo, 04 (quatro) Gbps de tráfego e atenda integralmente aos demais requisitos técnicos estabelecidos no Termo de Referência.

Natureza do esclarecimento. A presente manifestação possui caráter meramente interpretativo e consolida o que já decorre, de forma vinculante, do item 8.10.3.1.2 e das cláusulas de prevalência acima citadas, não inovando, restringindo ou ampliando o requisito técnico. Por não afetar a formulação das propostas, não implica reabertura do prazo legal, em observância ao princípio do formalismo moderado e ao art. 55, §1º, da Lei nº 14.133/2021. Para reforço da isonomia e da transparência, poderá a Administração, a seu critério, promover errata de mera correção material na apresentação da tabela do item 3.2, alinhando-a ao item 8.10.3.1.2, sem alteração do requisito técnico vinculante.

6. Em resposta ao pedido de esclarecimento, informa-se que o entendimento está correto. A exigência constante do item 17.1, alínea "c", referente à apresentação do ato constitutivo, estatuto ou contrato social em vigor, aplica-se às sociedades por ações (S/A), as quais deverão apresentar o respectivo Estatuto Social, devidamente registrado, acompanhado dos documentos comprobatórios da eleição ou designação de seus administradores, conforme a legislação aplicável. Ressalta-se que a expressão "ato constitutivo" abrange as diferentes espécies societárias previstas no ordenamento jurídico brasileiro.

(...)

2.3 SÍNTESE DO PEDIDO DE IMPUGNAÇÃO EMPRESA B, ID. (73205644):

(...)

1. I — DA EXIGÊNCIA DE FORNECIMENTO POR UM ÚNICO FABRICANTE

Desta forma, requer-se:

(a) a supressão da exigência de fornecimento por um único fabricante (itens 6.6 e 6.10.1 do Termo de Referência), admitindo-se solução composta por produtos de mais de um fabricante, desde que comprovada a integração funcional entre os componentes e o atendimento integral aos requisitos do edital;

(b) a supressão da vedação ao uso de consoles/plataformas de correlação de terceiros e da vinculação “do próprio fabricante” nos itens 8.10.1.1.116 e 8.10.2.1.174, conforme redação sugerida a seguir; e

(c) subsidiariamente, caso não acolhidas as medidas anteriores, a adoção da adjudicação por item (ou por lotes tecnicamente coerentes), nos termos da Súmula nº 247/TCU, de modo a permitir a disputa por componentes autônomos.

2. II — DO ITEM 1: PROTEÇÃO DE ENDPOINTS.

3. III — DO ITEM 2: PROTEÇÃO DE SERVIDORES

4. IV — DO ITEM 3: PROTEÇÃO CONTRA AMEAÇAS AVANÇADAS / NDR / SANDBOX

5. V — DO ITEM 4: SOLUÇÃO DE PREVENÇÃO DE INTRUSÃO DE PRÓXIMA

GERAÇÃO (NGIPS)

6. VI — DO ITEM 7: SOLUÇÃO DE VISIBILIDADE DE SUPERFÍCIE DE ATAQUE

7. DA DEMONSTRAÇÃO DO DIRECIONAMENTO DO EDITAL

requer-se:

1. o conhecimento e o acolhimento integral da presente impugnação;

2. a supressão da exigência de fornecimento por um único fabricante e da vedação a arquiteturas multi-fabricante interoperáveis (itens 6.6 e 6.10.1 do Termo de Referência e itens 8.10.1.1.116, 8.10.2.1.174 e 8.10.3.1.111) ou, subsidiariamente, a adoção da adjudicação por item, nos termos da Súmula nº 247/TCU;

3. a alteração dos dispositivos técnicos apontados (Itens 1, 2, 3, 4 e 7), conforme as redações sugeridas, e a exclusão/flexibilização dos itens 8.10.2.1.67, 8.10.4.38, 8.10.4.39 e 8.10.4.62;

4. que a comprovação do atendimento aos requisitos técnicos seja admitida por meio da documentação técnica oficial do fabricante (datasheets, guias e manuais), vedada a exigência de declarações, cartas ou atestados específicos para funcionalidades já descritas em tal documentação, e que o detalhe de implementação não essencial ao resultado funcional não seja tratado como critério eliminatório;

5. a consequente republicação do edital, com reabertura do prazo legal, assegurando-se igualdade de condições a todos os licitantes.

(...)

2.4 DA MANIFESTAÇÃO DO SESAU-NSC, ID. (74288553):

(...)

1. **(a) Não assiste razão à Requerente.**

A exigência de fornecimento dos componentes por um único fabricante foi estabelecida em razão da arquitetura da solução pretendida pela Administração, cuja finalidade é disponibilizar uma plataforma integrada de proteção, detecção, investigação e resposta a incidentes cibernéticos.

Embora seja tecnicamente possível integrar produtos de fabricantes distintos mediante APIs, conectores ou protocolos padronizados, tais integrações não asseguram o mesmo nível de interoperabilidade, compartilhamento de inteligência de ameaças, sincronização de políticas de segurança, automação de respostas e compatibilidade operacional proporcionados por uma solução concebida originalmente como plataforma única.

Além disso, a utilização de múltiplos fabricantes aumenta significativamente a complexidade de administração da solução, eleva o risco de incompatibilidades decorrentes de atualizações independentes e dificulta a identificação de responsabilidades durante o suporte técnico e a resolução de incidentes.

A Administração definiu, durante a fase de planejamento da contratação, que a solução deveria possuir integração nativa entre seus componentes, visando garantir maior confiabilidade operacional, simplificação da gestão, redução do tempo de resposta a incidentes e maior disponibilidade dos serviços de segurança.

Dessa forma, a exigência não constitui direcionamento a fabricante específico, mas requisito técnico decorrente da arquitetura definida para atendimento das necessidades institucionais.

Não se acolhe o pedido de alteração, mantendo-se os itens 6.6 e 6.10.1 do Termo de Referência.

(b) Também não merece acolhimento.

Os requisitos previstos no Termo de Referência objetivam assegurar que a correlação de eventos, a investigação de incidentes e as ações automatizadas de resposta sejam executadas de forma nativa pela própria plataforma de segurança, sem dependência de ferramentas intermediárias desenvolvidas por terceiros.

A utilização de consoles de correlação externos pode introduzir limitações funcionais, atrasos na disponibilização de novos recursos, dependência de conectores específicos, incompatibilidades decorrentes de atualizações entre fabricantes e aumento da complexidade operacional da solução.

A utilização de plataforma integrada do próprio fabricante permite maior consistência na correlação de eventos, compartilhamento imediato da inteligência de ameaças entre todos os componentes da solução, além de assegurar suporte técnico unificado durante toda a vigência contratual.

Ressalta-se que tal exigência decorre de necessidade operacional da Administração e não da intenção de restringir fabricantes ou tecnologias específicas.

Não se acolhe o pedido de exclusão da exigência constante dos itens 8.10.1.1.116 e 8.10.2.1.174, mantendo-se a redação originalmente prevista no Termo de Referência.

(c) O pedido também não merece prosperar.

Conforme demonstrado na justificativa de parcelamento constante do próprio Termo de Referência, a contratação foi estruturada em grupo único em razão da interdependência técnica existente entre todos os componentes da solução de segurança cibernética.

Embora os equipamentos e licenças possam ser individualmente identificados, sua efetividade operacional depende da atuação integrada dos diversos módulos, compartilhando inteligência de ameaças, políticas de segurança, telemetria, mecanismos de investigação e respostas automatizadas.

O parcelamento da contratação poderia resultar na responsabilização de múltiplos fornecedores por componentes distintos da mesma arquitetura, aumentando a complexidade da implantação, da operação, do suporte técnico e da gestão contratual, além de dificultar a apuração de responsabilidades em situações de indisponibilidade ou falhas de integração.

Nesse contexto, o agrupamento em lote único decorre de justificativa técnica previamente demonstrada no planejamento da contratação, não configurando afronta ao princípio da competitividade.

A Súmula nº 247 do TCU recomenda o parcelamento sempre que técnica e economicamente viável. No presente caso, entretanto, restou demonstrado que a integração funcional dos componentes constitui requisito essencial da solução pretendida, justificando a adoção do julgamento pelo menor valor global.

2. A) **Item 8.10.1.1.10 - Aceitar e Formatar para.** A solução deve realizar a análise de malware no interior de arquivos compactados pelo menos nos formatos: ZIP, RAR, TAR e CAB, removendo seletivamente apenas o(s) arquivo(s) malicioso(s).

B) Item 8.10.1.1.11 - Aceitar e Formatar para. A solução deve inspecionar, em tempo real (real-time), os arquivos gravados em disco por qualquer aplicação, incluindo aplicações de mensageria e de transferência de arquivos.

C) Item 8.10.1.1.13 - Não se acolhe a alteração proposta. A proposta substitui requisitos objetivos de desempenho buscando atender a heterogeneidade de recursos de estações no ambiente. Considerando que diferentes fabricantes utilizam tecnologias próprias para otimização de desempenho, a redação atual mostra-se mais adequada por privilegiar o resultado esperado e não o método empregado.

D) Item 8.10.1.1.22 - Não se acolhe a alteração proposta. O mecanismo de cache por hash constitui apenas uma das tecnologias existentes para evitar reanálises. A Administração busca o resultado funcional, independentemente da tecnologia empregada, razão pela qual a redação atual permanece mais abrangente e tecnologicamente neutra.

E) Item 8.10.1.1.27 - Aceitar e Formatar para. A redação sugerida consolida duas funcionalidades distintas em um único requisito, podendo gerar interpretações divergentes quanto à comprovação do atendimento. A separação das funcionalidades prevista no Termo de Referência facilita a verificação técnica durante a fase de aceitação. Parece ter sido escrito dois itens juntos (Acatar). Sugestão: Separar os itens da seguinte forma:

8.10.1.1.27. Deve possuir capacidade de escaneamento de arquivos compactados e, em caso de identificação de um arquivo malicioso, apenas este deve ser removido, mantendo os demais intactos;

8.10.1.1.28. Deve ser capaz de bloquear o acesso a qualquer site não previamente analisado pelo fabricante;

F) Item 8.10.1.1.29 - Não se acolhe a alteração proposta. A inclusão da criação automática de exceções constitui funcionalidade adicional, não essencial ao objetivo principal do requisito, podendo inclusive reduzir o nível de proteção caso utilizada inadequadamente. A redação original atende plenamente às necessidades da Administração.

G) Item 8.10.1.1.40 - Não se acolhe a alteração proposta. A redação proposta amplia as formas de distribuição de atualizações. Entretanto, o Termo de Referência já admite soluções que atendam ao resultado esperado de distribuição eficiente das atualizações, não sendo necessária a indicação de tecnologias específicas como cache, replicação ou nuvem.

H) Item 8.10.1.1.41 - Não se acolhe a alteração proposta. A proposta apenas altera a forma de redação, sem modificar o requisito funcional originalmente previsto, inexistindo ganho técnico que justifique a alteração.

I) Item 8.10.1.1.42 - Não se acolhe a alteração proposta. A atualização incremental representa uma das alternativas existentes para otimização do consumo de banda quando acessada localmente. A Administração busca garantir eficiência na distribuição das atualizações, sem que necessariamente todo o parque necessite buscar atualizações na nuvem, aumentando o consumo de banda.

J) Item 8.10.1.1.50 - Não se acolhe a alteração proposta. A redação atual sugere uma

implementação eficiente, exigindo a capacidade da remoção da solução de antivírus atual de forma remota e automática, dispensando a necessidade de utilizar outro software.

K) Item 8.10.1.1.60 - Não se acolhe a alteração proposta. As informações sugeridas no item buscam obter dados sobre o usuário logado para fins de controle, análise, resposta, correlação e auditoria, uma vez que um evento seja registrado na console.

L) Item 8.10.1.1.63 - Não se acolhe a alteração proposta. A substituição da integração específica com Active Directory por autenticação genérica via LDAP amplia o escopo do requisito. Entretanto, considerando que o ambiente corporativo da Administração utiliza Active Directory como serviço oficial de diretório, a redação original permanece aderente à infraestrutura existente.

M) Item 8.10.1.1.75 - Não se acolhe a alteração proposta. A alteração limita o escaneamento apenas quando o acesso ao dispositivo estiver previamente habilitado, reduzindo o alcance da proteção originalmente pretendida pela Administração.

N) Item 8.10.1.1.77 - Não se acolhe a alteração proposta. A redação sugerida substitui requisito objetivo de bloqueio da funcionalidade Autorun por mecanismo genérico de mitigação. A especificação original oferece maior nível de proteção contra execução automática de códigos maliciosos.

O) Item 8.10.1.1.78 - Aceitar Parcialmente e Formatar para. Deve permitir controle de permissão ou bloqueio para dispositivos que não armazenam dados tendo, pelo menos, os seguintes tipos de dispositivos: adaptadores bluetooth, dispositivos de imagem, modems, interfaces wireless externas, cartões PCMCIA, dispositivos infravermelhos e portas COM/LPT. Módulo de Proteção Anti-Malware para estações MacOS: O cliente para instalação deverá possuir compatibilidade com os sistemas operacionais: macOS 12 (Monterey); macOS 11 (Big Sur) macOS 10.15 (Catalina); macOS 10.14 (Mojave); macOS 10.13 (High Sierra);

P) Item 8.10.1.1.79 - Não se acolhe a alteração proposta. A exigência visa garantir que a solução ofertada seja implantável remotamente no parque macOS atualmente administrado pelo órgão, sem necessidade de aquisição, implantação ou reestruturação de ferramenta adicional de gerenciamento.

Q) Item 8.10.1.1.93 - Não se acolhe a alteração proposta. A redação sugerida simplifica os modos de operação do HIPS, enquanto a redação original estabelece requisitos mais completos quanto aos níveis de proteção disponíveis. Não se verifica vantagem técnica na alteração.

R) Item 8.10.1.1.97 - Não se acolhe a alteração proposta. A inclusão da expressão "virtual patching" constitui exemplo de tecnologia empregada por determinados fabricantes. O Termo de Referência foi elaborado com foco na funcionalidade requerida, preservando neutralidade tecnológica.

S) Item 8.10.1.1.102 - Aceitar Parcialmente - Erro de digitação e itens misturados, A sugestão não será acolhida integralmente, pois altera o escopo técnico do requisito**:** Separar os itens, mas com a resposta de não alteração de redação:

Item 8.10.1.1.102 - Busca assegurar que a solução possua mecanismo de controle de aplicações com base ou catálogo previamente classificado, permitindo a criação de políticas por categorias de aplicações. A identificação por assinatura digital, hash e caminho do executável é mecanismo complementar e útil para regras específicas, mas não substitui a capacidade de classificação por categorias, necessária para administração centralizada, escalabilidade operacional e aplicação uniforme de políticas de segurança no ambiente corporativo.

T) Item 8.10.1.1.104 - Não se acolhe a alteração proposta. A redação proposta substitui critérios objetivos previstos no Termo de Referência por exemplos de aplicações. O objetivo do item é garantir que a solução disponha de base previamente categorizada, mantida e atualizada pelo fabricante, contendo, no mínimo, categorias relevantes para proteção do ambiente, como keyloggers, anonimizadores de proxy, ferramentas P2P e ferramentas de quebra de senha. Tais categorias são necessárias para permitir a aplicação de políticas centralizadas, escaláveis e verificáveis, sem depender exclusivamente de regras manuais ou customizações posteriores.

U) Item 8.10.1.1.139 - Não se acolhe a alteração proposta, mantendo-se a redação original do Termo de Referência. O objetivo do item é garantir que, ao término de uma sessão remota de shell, o órgão possa obter evidência completa e portátil da atividade realizada, para fins de auditoria, investigação, responsabilização e documentação de resposta a incidentes. Logs consultáveis são desejáveis, mas não substituem a necessidade de exportação do histórico da sessão.

3. A) **III.1 — Do Item 8.10.2.1.67 (Microsoft Application Protection Program – MAPP) - Não se acolhe a impugnação.** A requerente sustenta que a exigência de participação do fabricante no Microsoft Active Protections Program — MAPP restringiria a competitividade, sob o argumento de que nem todos os fabricantes de soluções de segurança participam formalmente desse programa. Após análise técnica, verifica-se que o requisito foi estabelecido com a finalidade de assegurar maior capacidade de resposta preventiva a vulnerabilidades divulgadas pela Microsoft, permitindo

que fabricantes de soluções de segurança tenham acesso antecipado a informações técnicas relevantes para o desenvolvimento de mecanismos de proteção antes da disponibilização pública das correções ou em momento compatível com a sua publicação. Trata-se de característica diretamente relacionada ao nível de maturidade da solução de segurança, à capacidade de proteção preventiva e à redução da janela de exposição dos ativos da Administração, especialmente considerando a predominância de sistemas operacionais, aplicações e serviços Microsoft no ambiente tecnológico do órgão. A exigência não impõe marca, modelo, fabricante específico ou fornecedor determinado, tampouco restringe o certame a uma única solução de mercado. O requisito busca aferir a capacidade técnica do fabricante de prover mecanismos de proteção antecipada contra vulnerabilidades do ecossistema Microsoft, tais como assinaturas, regras de prevenção, mecanismos de virtual patching, inteligência de ameaças e demais controles de mitigação aplicáveis. Ressalta-se que a participação no programa MAPP é facultada pela própria Microsoft aos fabricantes que atendam aos critérios estabelecidos para participação, não constituindo exigência criada exclusivamente para favorecer determinado fornecedor. Ao contrário, trata-se de critério técnico objetivo, verificável e compatível com a natureza do objeto contratado, voltado à obtenção de maior nível de segurança cibernética para o ambiente institucional. Além disso, a Administração identificou que há pluralidade de fabricantes de soluções de segurança que participam do referido programa ou que possuem capacidade técnica compatível com o nível de proteção exigido, não se caracterizando direcionamento ou restrição indevida à competitividade. A redação sugerida pela requerente, ao substituir a exigência por expressão genérica relativa à "proteção tempestiva contra a exploração de vulnerabilidades conhecidas", não confere o mesmo grau de objetividade, rastreabilidade e segurança na avaliação técnica da proposta. A mera alegação de existência de virtual patching ou inteligência de ameaças própria do fabricante, sem comprovação de acesso antecipado a informações técnicas oficiais ou equivalentes, não assegura o atendimento da necessidade administrativa que motivou o requisito. Dessa forma, a exigência guarda pertinência com o objeto contratado, mostra-se proporcional à criticidade do ambiente a ser protegido e está alinhada ao interesse público de reduzir o tempo de exposição a vulnerabilidades críticas, razão pela qual não se verifica ilegalidade, direcionamento ou restrição indevida à competitividade.

B) III.2 — Dos Itens 8.10.2.1.16, 8.10.2.1.47 e 8.10.2.1.68 (Integração nativa com VMware vCloud/vCenter) - Não se acolhe a impugnação. A requerente solicita a exclusão ou flexibilização da exigência de integração nativa com os ambientes **VMware vCloud/vCenter**, sob o argumento de que tal requisito restringiria a competitividade ao privilegiar fabricantes que possuam integração específica com essas plataformas. Após análise, verifica-se que a exigência foi estabelecida em razão da infraestruturaatualmenteutilizadapelaAdministração,aqualcontemplaambientevirtualizadobaseado em tecnologias VMware. A integração nativa permite a comunicação direta entre a solução de segurança e o ambiente de virtualização, possibilitando maior eficiência operacional, automação de políticas de proteção, gerenciamento centralizado e melhor desempenho na proteção das máquinas virtuais. A utilização de integrações indiretas, por meio de ferramentas intermediárias ou desenvolvimento de conectores adicionais, pode acarretar aumento da complexidade operacional, maior custo de manutenção, dependência de componentes de terceiros e riscos à compatibilidade e ao suporte técnico durante a vigência contratual. Cumpre destacar que a Administração possui discricionariedade para definir requisitos técnicos compatíveis com sua infraestrutura tecnológica, desde que devidamente justificados e relacionados ao atendimento de sua necessidade, não havendo obrigatoriedade de adequação do ambiente para acomodar limitações de determinadas soluções disponíveis no mercado. Assim, a exigência não se destina a restringir a competição, mas a assegurar plena compatibilidade com o ambiente corporativo existente, reduzir riscos operacionais e garantir maior eficiência na gestão da solução de segurança.

C) **III.3 — Dos Itens 8.10.2.1.116 e 8.10.2.1.134 (Recursos de Firewall de Host de Fabricante Específico) - Não se acolhe a impugnação.** A requerente sustenta que os itens 8.10.2.1.116 e 8.10.2.1.134 restringiriam a competitividade por supostamente descreverem recursos específicos de firewall de host de determinado fabricante, defendendo que os objetivos de mitigação de ataques de inundação e detecção de ameaças em tráfego criptografado poderiam ser atendidos por mecanismos alternativos, inclusive em nível de rede, gateway ou proxy. Após análise técnica, verifica-se que os requisitos foram definidos em razão da necessidade de proteção integrada dos endpoints e servidores da Administração, com aplicação de políticas, monitoramento, geração de eventos, auditoria e resposta a incidentes de forma centralizada pela solução de segurança contratada. O item 8.10.2.1.116, ao exigir a possibilidade de limitar o número de meias-conexões oriundas de um computador, busca mitigar comportamentos associados a ataques de negação de serviço, exaustão de recursos e tentativas de inundação, inclusive em cenários nos quais a proteção exclusivamente perimetral não seja suficiente para identificar ou bloquear tráfego malicioso direcionado a cargas específicas. A existência de controles em firewall de rede, appliance, gateway ou balanceador não substitui, necessariamente, a necessidade de controle local no host, sobretudo

em ambientes com múltiplos segmentos, comunicação interna, cargas virtualizadas, tráfego leste-oeste e ativos que podem operar fora do perímetro tradicional. O item 8.10.2.1.134, por sua vez, visa assegurar que a solução possua capacidade de identificar ameaças associadas a tráfego criptografado de entrada, considerando que ataques, comunicações maliciosas e tentativas de exploração podem se valer de canais cifrados para dificultar a visibilidade dos mecanismos tradicionais de segurança. A inspeção ou análise desse tráfego no contexto do host protegido complementa os controles de rede e reduz pontos cegos de segurança, especialmente quando a comunicação não transita por gateway/proxy corporativo, ocorre entre ativos internos ou é direcionada diretamente ao servidor protegido. A proposta da requerente desloca a proteção para mecanismos genéricos "no host ou na rede" e para inspeção "em gateway/proxy", o que não assegura o mesmo nível de cobertura, rastreabilidade, correlação de eventos e aplicação uniforme de políticas pela solução de proteção de endpoints. Embora mecanismos de rede sejam relevantes e complementares, eles não substituem integralmente controles locais gerenciados de forma centralizada, especialmente em cenários de movimentação lateral, segmentação interna, acesso remoto, cargas virtualizadas e tráfego que não passa obrigatoriamente por pontos centralizados de inspeção. Ressalta-se que a Administração não exige produto, marca ou fabricante específico, mas sim funcionalidades técnicas compatíveis com a necessidade de proteção do ambiente institucional. Os requisitos são voltados à capacidade da solução de prover mecanismos integrados de controle, inspeção, detecção e resposta, com administração centralizada e responsabilização contratual única, evitando a fragmentação operacional decorrente da dependência de múltiplas ferramentas, consoles, fornecedores ou componentes externos. Quanto à alegação de elevado custo de processamento, observa-se que as funcionalidades exigidas devem ser configuráveis e aplicadas conforme política de segurança, criticidade do ativo e perfil da carga de trabalho, cabendo à Administração definir sua ativação, exceções e parâmetros de uso de acordo com a necessidade operacional. A mera possibilidade de consumo adicional de recursos não invalida o requisito, sobretudo diante da criticidade dos ativos a serem protegidos e da finalidade de redução de riscos de indisponibilidade, exploração de vulnerabilidades e comprometimento do ambiente. Assim, os itens impugnados guardam pertinência com o objeto contratado, são proporcionais à criticidade do ambiente de TI da Administração e visam assegurar proteção em profundidade, com controles no próprio endpoint/servidor, complementares aos mecanismos de segurança de rede. Diante do exposto, mantém-se a redação dos itens 8.10.2.1.116 e 8.10.2.1.134.

D) III.4 — Demais Itens do Item 2 - Não se acolhe a impugnação quanto aos demais itens do Item 2. A requerente solicita a alteração de diversos itens do Termo de Referência, sob o argumento genérico de que as redações atuais conteriam formas de implementação específicas, parâmetros numéricos ou citações aptas a restringir a competitividade, sugerindo a substituição por expressões mais amplas ou por critérios considerados equivalentes. Após análise técnica, verifica-se que os requisitos impugnados foram definidos com base nas necessidades reais do ambiente tecnológico da Administração, considerando a diversidade de sistemas operacionais, plataformas, aplicações, servidores, cargas virtualizadas, mecanismos de proteção, políticas de segurança, rotinas de administração e requisitos de auditoria necessários à adequada proteção dos ativos institucionais. No que se refere aos itens relacionados à compatibilidade com sistemas operacionais e plataformas, a especificação de versões não tem por finalidade restringir a competição, mas assegurar que a solução ofertada seja efetivamente compatível com o parque computacional existente e com as cargas de trabalho que deverão ser protegidas. A substituição por expressões genéricas, como "versões com suporte ativo", "derivados equivalentes" ou "e superiores", pode gerar incerteza quanto à comprovação objetiva da compatibilidade, especialmente porque versões futuras ou derivadas podem não estar homologadas pelo fabricante da solução no momento da contratação. A Administração necessita de comprovação objetiva de suporte às plataformas indicadas no edital, não sendo suficiente a afirmação genérica de compatibilidade com famílias de sistemas operacionais ou versões superiores. Em ambientes críticos, a compatibilidade deve ser verificável em documentação oficial, matriz de suporte, declaração técnica do fabricante ou prova de conceito, de forma a evitar riscos de incompatibilidade, indisponibilidade, perda de suporte ou falhas na implantação. Quanto aos itens relativos à distribuição de agentes, atualização de componentes, geração e distribuição de relatórios, isolamento de rede, aplicação de políticas, regras de firewall, exceções, controle de tráfego, registro de eventos, captura de evidências, inspeção de logs, monitoramento de integridade e execução automatizada de scripts, observa-se que todos esses requisitos estão relacionados à necessidade de gestão centralizada, padronizada e auditável da solução de proteção de servidores. As redações sugeridas pela requerente , em diversos casos, substituem critérios objetivos por expressões abertas, tais como "a exemplo de", "ou equivalentes", "no host ou na rede", "complementarmente", "quando habilitado" ou "critério desejável". Embora tais expressões possam aparentar ampliação da competitividade, elas reduzem a precisão técnica do objeto, dificultam a avaliação isonômica das propostas e podem permitir o fornecimento de soluções que não atendam integralmente às necessidades de segurança da Administração. A proteção pretendida não se limita à existência isolada de mecanismos de mercado, ferramentas de terceiros ou controles perimetrais. O objetivo da Administração é

contratar uma solução integrada de proteção de servidores, capaz de aplicar políticas de forma centralizada, distribuir atualizações, controlar comunicações, detectar ameaças, gerar eventos, produzir evidências, apoiar resposta a incidentes e manter rastreabilidade operacional a partir de uma arquitetura unificada de gestão. No tocante aos requisitos de firewall de host, IDS/IPS, controle de conexões, detecção de varreduras, proteção contra anomalias de protocolo, blindagem de vulnerabilidades, captura de pacotes e análise de tráfego, não se mostra adequado substituir a proteção local do servidor por mecanismos genéricos "no nível de rede". Controles de rede são relevantes e complementares, mas não substituem integralmente os controles aplicados no próprio host, especialmente em ambientes com tráfego interno, movimentação lateral, múltiplos segmentos, cargas virtualizadas, servidores expostos, acesso remoto e comunicações que não necessariamente transitam por pontos centrais de inspeção. Da mesma forma, os requisitos relacionados à inspeção de arquivos compactados, objetos incorporados, scripts maliciosos, ameaças sem arquivo, exclusões de antimalware e minimização de impacto de varredura foram definidos para assegurar proteção efetiva das cargas de trabalho sem comprometer a disponibilidade dos serviços. Tais funcionalidades são compatíveis com a natureza do objeto e refletem práticas usuais de proteção de servidores corporativos. A Administração também não acolhe a tentativa de converter determinados requisitos obrigatórios em critérios meramente desejáveis, como proposto em alguns itens. As funcionalidades indicadas foram classificadas como obrigatórias em razão da criticidade do ambiente protegido, da necessidade de reduzir riscos de indisponibilidade, exploração de vulnerabilidades, movimentação lateral, perda de visibilidade e dificuldade de resposta a incidentes. Ressalta-se que os itens impugnados não exigem marca, modelo ou fabricante específico. As exigências descrevem capacidades técnicas necessárias à solução de segurança a ser contratada, sendo passíveis de atendimento por diferentes fabricantes que possuam arquitetura integrada, recursos de proteção de servidores, suporte multiplataforma e gerenciamento centralizado. A Administração poderá aceitar terminologias, nomenclaturas comerciais ou implementações tecnicamente equivalentes, desde que a licitante comprove, de forma objetiva, o atendimento integral ao requisito, sem prejuízo da funcionalidade exigida, da gestão centralizada, da geração de eventos, da rastreabilidade, da aplicação de políticas e da responsabilização contratual pela solução ofertada. Dessa forma, as alterações propostas pela requerente não se mostram necessárias nem adequadas, pois reduzem a precisão do objeto, fragilizam a comprovação técnica e podem comprometer o nível de proteção pretendido pela Administração. Diante do exposto, mantém-se a redação dos itens impugnados.

4. A) **Do item 8.10.3.1.18 -** A requerente questiona a exigência de verificação em tempo real da reputação de URLs e servidores SMTP. O pleito não merece acolhimento integral. O requisito objetiva assegurar que a solução possua mecanismos de inteligência de ameaças capazes de avaliar a reputação de recursos utilizados em campanhas maliciosas, phishing, distribuição de malware, spam, comunicação com infraestrutura de comando e controle e demais ameaças associadas aos vetores web e e-mail. A exigência não impõe fabricante específico nem método exclusivo de implementação. Poderão ser aceitas arquiteturas que realizem a verificação por reputação de URL, IP, domínio, DNS, servidores de correio ou mecanismos equivalentes aplicados ao fluxo SMTP, desde que preservada a capacidade de análise reputacional em tempo real. Assim, mantém-se a finalidade do requisito, admitindo-se interpretação técnica equivalente quanto ao mecanismo de reputação utilizado.

B) Do item 8.10.3.1.19 - A requerente requer que seja admitida análise de SMTP em sensor multiprotocolo único, alegando que a análise em solução separada imporia arquitetura específica. O pleito não merece acolhimento nos termos propostos. A redação atual utiliza a expressão "poderá", não impondo obrigatoriamente que a análise de SMTP seja realizada em solução fisicamente separada. A finalidade do requisito é admitir flexibilidade arquitetural, assegurando que a solução possa tratar adequadamente diferentes vetores de ataque, com desempenho, escalabilidade e capacidade de inspeção compatíveis com o ambiente da Administração. Dessa forma, esclarece-se que a análise de SMTP poderá ocorrer em componente separado ou em sensor multiprotocolo integrado, desde que comprovado o atendimento integral às capacidades de inspeção, análise, correlação e desempenho exigidas.

C) Do item 8.10.3.1.20 - A requerente questiona o requisito relativo à análise de artefatos em sandbox e ao mecanismo de conhecimento de senhas com vocabulário mínimo de 90 palavras-chave para derivação de arquivos protegidos. Assiste razão parcial à requerente. A capacidade obrigatória essencial para a Administração é a análise de artefatos suspeitos em ambiente controlado de sandbox, de forma a permitir a identificação de comportamento malicioso, evasivo ou desconhecido. O mecanismo de derivação de senhas de arquivos protegidos por dicionário de palavras-chave pode agregar valor à análise de determinados artefatos, mas o parâmetro numérico mínimo de 90 palavras-chave não se mostra indispensável como critério eliminatório. Assim, a Administração acolhe parcialmente a impugnação para ajustar o requisito, mantendo como obrigatória a capacidade de análise de artefatos em sandbox e tratando mecanismos de tratamento de arquivos protegidos por senha como funcionalidade complementar, quando disponível.

D) Do item 8.10.3.1.24 - A requerente questiona a exigência de detecção e análise de uma relação nominal extensa de protocolos e aplicações, sustentando que a lista conteria aplicações legadas ou descontinuadas e poderia caracterizar vinculação a base de assinaturas específica de determinado fabricante. Após análise técnica, verifica-se que a finalidade do requisito é legítima e pertinente ao objeto contratado. A Administração necessita que a solução possua capacidade de identificar, classificar, analisar e registrar protocolos, aplicações e serviços de rede utilizados no ambiente monitorado, inclusive aqueles associados a transferência de arquivos, mensageria, acesso remoto, compartilhamento P2P, serviços de infraestrutura, navegação web, correio eletrônico e demais comunicações potencialmente exploradas para evasão, comando e controle, exfiltração de dados, movimentação lateral ou violação de políticas de segurança. A identificação de aplicações e protocolos é funcionalidade relevante em soluções de detecção e resposta de rede, prevenção de intrusão e análise avançada de ameaças, pois permite maior visibilidade sobre o tráfego, contextualização de eventos, aplicação de políticas, priorização de alertas e apoio à investigação de incidentes. Assim, não procede a alegação de que a Administração não possuiria necessidade técnica relacionada à detecção desses protocolos e aplicações. Contudo, assiste razão parcial à requerente quanto à conveniência de aperfeiçoamento redacional. A manutenção de lista nominal extensa e fechada, especialmente contendo aplicações legadas, descontinuadas ou de baixa relevância atual, pode gerar interpretação excessivamente restritiva, dificultar o julgamento objetivo e não refletir adequadamente a evolução dinâmica do tráfego de rede e das aplicações utilizadas por agentes maliciosos. A capacidade pretendida pela Administração não está vinculada à identificação literal de cada aplicação constante da lista, tampouco a base de assinaturas específica de determinado fabricante. O requisito busca assegurar que a solução possua motor de identificação de protocolos e aplicações, inspeção profunda de pacotes, análise comportamental, assinaturas atualizáveis ou mecanismo equivalente capaz de reconhecer tráfego de rede em diferentes camadas, inclusive quando utilizado para evasão, comunicação maliciosa, transferência não autorizada de dados ou violação de política corporativa. Dessa forma, a Administração acolhe parcialmente a impugnação para ajustar a redação do item, preservando o resultado funcional pretendido e afastando interpretação de lista exaustiva ou vinculada a catálogo específico de fabricante.

E) Do item 8.10.3.1.27 - A requerente questiona funcionalidade de detecção e identificação de ameaças. O requisito representa capacidade mínima esperada para soluções de detecção avançada, permitindo maior efetividade na identificação de incidentes, artefatos maliciosos, comportamentos suspeitos e comunicações associadas a ameaças. Não há vinculação a tecnologia proprietária ou fabricante específico, sendo admitidas diferentes metodologias de implementação, desde que preservado o resultado funcional esperado. Dessa forma, mantém-se a redação do item.

F) Do item 8.10.3.1.38 - A requerente questiona a exigência de suporte para balanceamento de carga no sensor de inspeção de tráfego, sustentando que tal redação descreveria forma específica de arquitetura e que o objetivo de sustentação de performance poderia ser atendido por outros mecanismos, como escalabilidade horizontal mediante adição de instâncias de inspeção. Após análise técnica, verifica-se que a finalidade do requisito é legítima e pertinente ao objeto contratado. A Administração necessita que a solução possua capacidade de manter a inspeção de tráfego em níveis compatíveis com o volume do ambiente monitorado, sem degradação relevante de desempenho, perda de visibilidade ou comprometimento da detecção de ameaças. Em soluções de detecção e resposta de rede, sandbox e análise avançada, a capacidade de escalar a inspeção é essencial para assegurar cobertura adequada do tráfego, especialmente em ambientes com grande volume de dados, múltiplos segmentos de rede e comunicações simultâneas. O balanceamento de carga no sensor de inspeção constitui uma forma tecnicamente válida de atender a essa necessidade, pois permite distribuir o processamento entre recursos disponíveis e otimizar a performance da solução. Contudo, assiste razão parcial à requerente quanto à conveniência de não limitar o atendimento do requisito a uma única arquitetura de implementação, desde que preservado o resultado funcional pretendido. A capacidade exigida não está vinculada, necessariamente, à existência de balanceamento interno em um único sensor ou a modelo proprietário específico. O que se pretende assegurar é que a solução seja capaz de sustentar a capacidade de inspeção exigida para o ambiente, podendo fazê-lo por balanceamento de carga, clusterização, múltiplos sensores, distribuição de tráfego, escalabilidade horizontal, adição de instâncias de inspeção ou outro mecanismo tecnicamente equivalente. Dessa forma, acolhe-se parcialmente a impugnação para aperfeiçoamento redacional do item, preservando-se a exigência de capacidade de sustentação de performance da inspeção de tráfego, mas afastando-se interpretação de que somente arquitetura baseada em balanceamento de carga interno ao sensor seria aceita.

G) Do item 8.10.3.1.46 - A requerente questiona a exigência de que o ambiente controlado de sandbox contemple, no mínimo, os sistemas operacionais CentOS, Windows 10, Windows 7, Windows Server 2003, 2008, 2012 R2, 2016 e 2019, sustentando que a enumeração de versões específicas, inclusive legadas, poderia vincular o certame ao catálogo de imagens de determinado

fabricante. Após análise técnica, verifica-se que o requisito guarda pertinência com a necessidade concreta da Administração. A enumeração de sistemas operacionais e versões não foi estabelecida com a finalidade de direcionar o certame, mas de assegurar que a solução seja capaz de analisar artefatos suspeitos em ambientes representativos do parque tecnológico a ser protegido, inclusive considerando a existência de sistemas legados ou versões ainda relevantes para a operação institucional. Em soluções de sandbox, a versão do sistema operacional utilizado no ambiente de análise pode influenciar diretamente o comportamento do artefato analisado. Determinados códigos maliciosos podem alterar sua execução conforme a versão do sistema, bibliotecas disponíveis, APIs, serviços, configurações, arquitetura, mecanismos de segurança presentes ou ausentes e características do ambiente virtualizado. Assim, a análise em ambientes representativos é essencial para aumentar a fidelidade da detecção e reduzir o risco de falsos negativos. A presença de versões legadas no requisito não caracteriza, por si só, restrição indevida. Ao contrário, decorre da necessidade de proteção de ambiente heterogêneo, no qual podem coexistir sistemas atuais e sistemas legados, especialmente em razão de dependências sistêmicas, aplicações críticas, restrições de migração, compatibilidade com sistemas corporativos ou continuidade operacional. Tais ativos, justamente por sua condição de legado, demandam maior atenção quanto à análise de ameaças, uma vez que podem apresentar maior exposição a vulnerabilidades conhecidas e limitações quanto à aplicação de correções. A substituição da exigência por expressão genérica, como “ambientes representativos baseados em Windows e Linux, sem vinculação a versões específicas”, reduziria a objetividade do julgamento e poderia permitir o fornecimento de solução incapaz de simular adequadamente os cenários de risco efetivamente existentes no ambiente da Administração. A exigência de versões específicas permite comprovação técnica mais clara, avaliação isonômica entre licitantes e maior segurança quanto à aderência da solução ao ambiente real a ser protegido. Ressalta-se que o requisito não impõe fabricante específico, tampouco exige solução de marca determinada. O que se exige é capacidade técnica de análise em sandbox contemplando ambientes compatíveis com os sistemas indicados, sendo tal funcionalidade passível de atendimento por diferentes arquiteturas, imagens, templates, perfis de análise ou mecanismos equivalentes disponibilizados pelas soluções de mercado. No tocante à possibilidade de habilitação e desabilitação individual de regras de inspeção por interface de gerenciamento web, mantém-se a pertinência da exigência, por se tratar de funcionalidade necessária à administração da solução, ajuste fino das análises, redução de falsos positivos, adequação ao perfil do ambiente e operação segura da plataforma. Dessa forma, considerando a existência de ambiente tecnológico heterogêneo, a necessidade de análise de artefatos em sistemas representativos do parque protegido e a relevância da simulação de versões legadas para detecção de ameaças, mantém-se a redação do item impugnado.

H) Do item 8.10.3.1.54 - A requerente requer a exclusão da exigência de disponibilização de estatísticas por segmento de mercado e recomendações de segurança. A Administração entende que informações sobre ameaça, família da ameaça, recomendações de segurança, vetores de disseminação e contexto de inteligência agregada são relevantes para apoiar a resposta a incidentes, a priorização de ações e a avaliação do risco associado aos eventos detectados. Contudo, acolhe-se parcialmente a impugnação para esclarecer que tais informações poderão ser fornecidas diretamente pela solução, por portal ou base de inteligência do fabricante, ou por integração com serviço de inteligência de ameaças. As estatísticas por segmento de mercado serão consideradas informações complementares, não devendo ser interpretadas como requisito eliminatório isolado, desde que a solução forneça informações suficientes para contextualização e mitigação da ameaça.

I) Do item 8.10.3.1.56 - O requisito trata da identificação de ameaças direcionadas a dispositivos móveis. Não se verifica restrição indevida. A menção à plataforma Android possui caráter exemplificativo e não limita a solução a sistema operacional específico. O objetivo é permitir a identificação de ameaças relacionadas a dispositivos móveis, inclusive por meio da detecção de comunicações anômalas, maliciosas, C&C, exfiltração ou outros indicadores observáveis no tráfego de rede. Dessa forma, mantém-se o requisito, admitindo-se mecanismos equivalentes de identificação de ameaças móveis independentemente do sistema operacional do dispositivo.

J) Do item 8.10.3.1.69 - A requerente questiona a funcionalidade de sugestão de termos de busca durante investigações. O requisito tem por objetivo agilizar a atividade investigativa, reduzindo o tempo necessário para localização, correlação e análise de eventos relacionados a incidentes de segurança. A sugestão de termos de busca é uma forma de atendimento da necessidade, mas não deve ser interpretada como a única possível. Assim, admite-se que a funcionalidade seja atendida por sugestão automática de termos, pesquisa avançada, filtros estruturados, campos pré-definidos, pivoteamento investigativo ou mecanismos equivalentes que acelerem a obtenção de resultados durante a análise de incidentes. Dessa forma, acolhe-se parcialmente a impugnação, para esclarecer que o requisito poderá ser atendido por sugestão automática de termos de busca ou por mecanismos equivalentes de pesquisa avançada, filtros estruturados, campos pré-definidos, pivoteamento investigativo ou funcionalidades similares que acelerem a investigação de incidentes,

preservando-se o resultado funcional pretendido pela Administração.

K) Do item 8.10.3.1.71 - O requisito estabelece funcionalidade de sugestão de consultas a bases de reputação e WHOIS quando identificados hosts e nomes de domínio. O objetivo da exigência é enriquecer a investigação com informações contextuais sobre endereços IP, domínios, URLs e demais indicadores observados nos eventos de segurança. Não há direcionamento a fabricante específico. Poderão ser aceitos mecanismos equivalentes de enriquecimento automático ou assistido de eventos com reputação, inteligência de ameaças, WHOIS, geolocalização, histórico de domínio, classificação de URL ou demais informações correlatas que auxiliem a investigação.

L) Do item 8.10.3.1.80 - A requerente questiona o requisito de envio de alertas via e-mail para pelo menos 100 endereços diferentes e a configuração de alarmes personalizados. Assiste razão parcial à requerente. A funcionalidade essencial para a Administração é a capacidade de notificação a múltiplos destinatários, grupos ou listas de distribuição, bem como a configuração de alarmes personalizados conforme critérios definidos durante investigações ou políticas de segurança. O número fixo de 100 e-mails poderá ser substituído por critério funcional, desde que a solução permita notificação a múltiplos destinatários configuráveis, listas de distribuição ou mecanismos equivalentes de alerta, sem prejuízo da rastreabilidade e da efetividade operacional.

M) Do item 8.10.3.1.87 - A requerente questiona a exigência de que a console de gerenciamento seja acessível por Internet Explorer, Google Chrome e Firefox. Assiste razão à requerente quanto à compatibilidade obrigatória com Internet Explorer, considerando tratar-se de navegador descontinuado pelo respectivo fabricante. A exigência de suporte a navegador obsoleto pode gerar incompatibilidade com soluções modernas, aumentar riscos de segurança e reduzir indevidamente a competitividade. Assim, a Administração acolhe a impugnação neste ponto para ajustar a redação, exigindo compatibilidade da console com navegadores modernos e suportados de mercado, tais como Google Chrome, Mozilla Firefox, Microsoft Edge ou navegadores baseados em mecanismos equivalentes, em versões atualmente suportadas.

N) Do item 8.10.3.1.107 - A requerente questiona a exigência de que a funcionalidade seja licenciada para analisar o throughput total do appliance. O pleito não merece acolhimento integral. A finalidade do requisito é impedir que a Administração contrate equipamento com capacidade nominal superior, mas com licença limitada a throughput inferior, o que poderia comprometer a inspeção do tráfego e gerar subdimensionamento da solução. A exigência não impõe modelo comercial específico. Poderão ser aceitos modelos de licenciamento por appliance, por capacidade, por assinatura, por equipamento ou equivalentes, desde que cubram integralmente o throughput contratado e não imponham teto artificial de inspeção inferior à capacidade exigida para o ambiente.

O) Do item 8.10.3.1.111 - A requerente questiona a exigência relacionada à possibilidade de direcionamento de parte do licenciamento para outros módulos da plataforma de Detecção e Resposta, como monitoramento de e-mail, endpoint ou servidores, sem acréscimos ou mudanças de licenciamento. Assiste razão parcial à requerente quanto à necessidade de evitar vinculação a modelo comercial exclusivo de determinado fabricante. A finalidade da Administração é obter flexibilidade operacional, integração entre módulos de detecção e resposta e capacidade de adequar a cobertura aos vetores relevantes do ambiente, sem prejuízo do escopo contratado. Assim, admite-se que o requisito seja atendido por modelo de licenciamento flexível, suíte integrada, plataforma unificada ou arranjo equivalente que permita cobertura dos vetores de e-mail, endpoint, servidores e detecção/resposta, desde que observadas as quantidades contratadas, a cobertura exigida e a ausência de custos adicionais não previstos para as funcionalidades obrigatórias. Dessa forma, a Administração acolhe parcialmente a impugnação apenas para aperfeiçoar a redação dos itens em que foram identificados parâmetros numéricos excessivamente específicos, referências a tecnologia descontinuada ou necessidade de maior clareza funcional, mantendo-se os demais requisitos por sua pertinência técnica, proporcionalidade e aderência ao objeto contratado. As alterações não implicam redução do nível de segurança pretendido, mas apenas ajuste de redação para privilegiar critérios funcionais, preservar a isonomia, garantir julgamento objetivo e assegurar que soluções tecnicamente equivalentes possam ser avaliadas, desde que comprovem o atendimento integral às capacidades exigidas.

5.

V.1 — Do item 8.10.4.1 (vedação a NGFW/UTM e exigência de appliance dedicado)

A requerente sustenta que a vedação ao emprego de soluções NGFW ou UTM e a exigência de appliance dedicado em hardware do próprio fabricante restringiriam a competitividade, requerendo a aceitação de soluções consolidadas em plataforma única de segurança de rede.

O pleito não merece acolhimento.

A especificação constante do edital decorre de estudo técnico previamente realizado pela Administração, no qual se concluiu pela necessidade de contratação de solução de prevenção de intrusão de próxima geração — NGIPS — em arquitetura dedicada, especializada e independente

das funções de firewall perimetral, UTM ou plataforma consolidada de segurança de rede.

A opção técnica por appliance dedicado não decorre de preferência por fabricante, marca ou modelo específico, mas da necessidade de preservar desempenho previsível, baixa latência, alta disponibilidade, segregação de funções críticas, isolamento operacional e responsabilização técnica integral pela solução de prevenção de intrusão. Trata-se de decisão de arquitetura de segurança definida na fase de planejamento da contratação, em conformidade com a criticidade do ambiente institucional e com os requisitos de disponibilidade, desempenho e continuidade operacional dos serviços protegidos.

Embora soluções NGFW e UTM possam incorporar funcionalidades de prevenção de intrusão, tais plataformas possuem finalidade arquitetural distinta, normalmente consolidando múltiplas funções de segurança em um mesmo equipamento, tais como firewall, VPN, controle de aplicações, filtragem web, inspeção SSL, antimalware, roteamento, NAT e prevenção de intrusão. Em ambientes de maior criticidade e volume de tráfego, a consolidação dessas funções pode gerar competição por CPU, memória, armazenamento, interfaces, filas de processamento e capacidade de inspeção, especialmente em cenários de tráfego criptografado, ataques volumétricos, picos de sessão, atualização de assinaturas e geração intensiva de logs.

A Administração busca evitar que a função de prevenção de intrusão concorra com demais funções perimetrais, reduzindo riscos de degradação de desempenho, impacto em serviços críticos, perda de pacotes, aumento de latência, indisponibilidade em janelas de atualização ou limitação artificial decorrente de licenciamento compartilhado. A adoção de appliance dedicado permite que o NGIPS opere como camada especializada de inspeção e bloqueio, com recursos computacionais próprios, ciclo de atualização próprio, bypass, alta disponibilidade e capacidade de expansão compatíveis com a função de prevenção de intrusão em tempo real.

A arquitetura dedicada também favorece a segregação de responsabilidades operacionais. Em uma plataforma consolidada, alterações em políticas de firewall, roteamento, VPN, filtragem ou inspeção SSL podem impactar direta ou indiretamente a função de prevenção de intrusão. No modelo dedicado, a Administração obtém maior previsibilidade na administração das políticas de IPS, nas janelas de manutenção, na análise de eventos, na atualização de assinaturas, na coleta de evidências e na resposta a incidentes, reduzindo o risco de efeitos colaterais entre funções de segurança distintas.

A exigência de hardware do próprio fabricante visa assegurar integração validada entre hardware e software, suporte técnico único, matriz de compatibilidade oficial, atualização coordenada de firmware e sistema, desempenho homologado pelo fabricante e responsabilização contratual clara em caso de falhas. A aceitação de hardwares genéricos ou apenas homologados por terceiros poderia introduzir riscos de incompatibilidade, degradação de performance, divergência de suporte, fragmentação de responsabilidades e maior complexidade na apuração de incidentes técnicos.

Ressalta-se que o item não exige fabricante específico, tampouco indica marca ou modelo determinado. A exigência recai sobre a arquitetura considerada adequada pela Administração em seu estudo técnico: solução NGIPS dedicada, em appliance especializado, com capacidade de importação ou conversão de regras no padrão SNORT, desempenho dimensionado, baixa latência, alta disponibilidade, bypass, atualização de assinaturas, gerenciamento centralizado e demais funcionalidades previstas no Termo de Referência.

A vedação a NGFW e UTM, portanto, não tem por finalidade excluir competidores de forma indevida, mas preservar a arquitetura definida no planejamento da contratação. O objeto pretendido não é a aquisição de firewall de próxima geração ou plataforma UTM com módulo de IPS habilitado, mas sim de camada especializada de prevenção de intrusão, dedicada à inspeção e bloqueio de ameaças em rede, de forma independente das funções de firewall perimetral.

Também não procede a alegação de direcionamento pelo simples fato de determinado fabricante ou categoria de produto não atender à arquitetura definida. A Administração não está obrigada a redesenhar sua infraestrutura de segurança para acomodar modelos comerciais diversos, desde que a especificação esteja tecnicamente motivada, seja compatível com o objeto, proporcional à criticidade do ambiente e passível de atendimento por soluções existentes no mercado.

Quanto à importação de regras no padrão SNORT, a exigência possui finalidade operacional legítima, pois permite maior flexibilidade para criação, reaproveitamento, conversão ou adaptação de assinaturas de prevenção de intrusão, ampliando a capacidade de resposta da equipe técnica diante de ameaças, vulnerabilidades e indicadores específicos do ambiente. O requisito não impõe tecnologia proprietária, mas busca assegurar interoperabilidade e capacidade de customização de regras em padrão amplamente conhecido no mercado de segurança.

Dessa forma, considerando o estudo técnico realizado, a criticidade do ambiente protegido, a necessidade de segregação da camada de prevenção de intrusão, a previsibilidade de desempenho, a redução de riscos operacionais, a responsabilização técnica única e a adequação da arquitetura dedicada ao modelo de segurança pretendido pela Administração, mantém-se integralmente a

redação do item 8.10.4.1 do edital.

A exigência também encontra respaldo no princípio do planejamento previsto na Lei nº 14.133/2021, segundo o qual compete àAdministração definir tecnicamente a solução que melhor atende
àssuasnecessidades,desdequeaespecificaçãopossuajustificativatécnicaenãoimponhadirecionamento indevido, o que não se verifica no presente caso.

Dessa forma, por se tratar de requisito tecnicamente justificado, proporcional às necessidades daAdministração e amplamente atendido pelo mercado, mantém-se integralmente a redação do item 8.10.4.1 do edital.

V.2 — Dos itens 8.10.4.38 e 8.10.4.39 (credenciais de mercado do fabricante)

A requerente questiona as exigências constantes dos itens 8.10.4.38 e 8.10.4.39, que estabelecem requisitos relacionados à apresentação de estatísticas de vulnerabilidades de dia zero, existência de equipe de pesquisa com quantitativo mínimo de pesquisadores e posicionamento em ranking de entidade específica.

O pleito merece acolhimento parcial.

A Administração possui interesse legítimo em contratar solução proveniente de fabricante com capacidade contínua de pesquisa, inteligência de ameaças, atualização de assinaturas e resposta a vulnerabilidades emergentes. Em soluções de prevenção de intrusão, a maturidade do fabricante e a existência de estrutura de pesquisa impactam diretamente a velocidade de criação de filtros, a qualidade das assinaturas, a cobertura de vulnerabilidades e a efetividade da proteção contra ameaças novas ou em exploração ativa.

Assim, é tecnicamente pertinente exigir que o fabricante demonstre capacidade de pesquisa de vulnerabilidades, análise de ameaças, produção de inteligência, atualização contínua de assinaturas e manutenção evolutiva da solução. Tais elementos são essenciais para reduzir a janela de exposição da Administração diante de novas vulnerabilidades, exploits, malwares, campanhas de ataque e técnicas de evasão.

Entretanto, assiste razão parcial à requerente quanto à necessidade de evitar que a comprovação dessa capacidade fique limitada a quantitativo fixo de pesquisadores, a ranking de entidade determinada ou a modelo específico de divulgação de estatísticas. Tais elementos podem ser indicativos de maturidade, mas não constituem o único meio idôneo para comprovar a capacidade técnica do fabricante.

A fixação de número mínimo de pesquisadores e a vinculação obrigatória a posição em ranking específico podem privilegiar porte institucional ou estratégia de marketing de determinados fabricantes, sem necessariamente representar, de forma exclusiva, a eficácia da solução para o ambiente da Administração. O objetivo administrativo não é contratar o fabricante com maior equipe declarada ou melhor posição em ranking mercadológico, mas solução capaz de manter proteção atualizada, tempestiva e tecnicamente consistente contra ameaças emergentes.

Dessa forma, acolhe-se parcialmente a impugnação para admitir comprovação equivalente da capacidade de pesquisa e inteligência de ameaças do fabricante, mediante laboratório próprio, equipe dedicada, serviço de threat intelligence, publicações técnicas, boletins de segurança, histórico de descobertas, atualizações contínuas de assinaturas, base de reputação, participação em programas de divulgação coordenada de vulnerabilidades, documentação oficial do fabricante ou outros meios objetivos que demonstrem aptidão para manter a solução atualizada contra ameaças emergentes.

Preserva-se, portanto, a finalidade técnica dos itens 8.10.4.38 e 8.10.4.39, sem limitar a comprovação a número específico de pesquisadores ou posição em ranking de entidade determinada.

V.3 — Do item 8.10.4.62 (correlação de relatórios de pentest com políticas)

A requerente questiona o requisito constante do item 8.10.4.62, que exige capacidade da solução de gerenciamento centralizado para relacionar relatórios de testes de penetração realizados no ambiente com as políticas de segurança em uso, indicando quais regras ou filtros são necessários ativar para alinhar a política às vulnerabilidades identificadas.

O pleito merece acolhimento parcial.

A finalidade do requisito é tecnicamente pertinente. A Administração busca aproximar a operação da solução de prevenção de intrusão dos achados reais de segurança do ambiente, permitindo que vulnerabilidades identificadas em testes, varreduras, auditorias ou avaliações técnicas sejam tratadas por meio de políticas, filtros, assinaturas ou recomendações de mitigação.

Tal capacidade contribui para priorização de riscos, redução do tempo de remediação, melhoria da postura de segurança e maior efetividade das políticas implementadas. Não se trata, portanto, de funcionalidade desnecessária, mas de recurso voltado à melhoria operacional e à gestão contínua

da segurança.

Contudo, a forma como a funcionalidade está descrita pode ser interpretada como fluxo específico de determinada plataforma de gerenciamento. A finalidade pretendida pela Administração pode ser atendida por diferentes mecanismos, tais como integração com ferramentas de avaliação de vulnerabilidades, importação de relatórios, APIs, correlação manual assistida, recomendações de política, mapeamento de vulnerabilidades para assinaturas, dashboards de priorização ou outros recursos equivalentes.

Dessa forma, acolhe-se parcialmente a impugnação para admitir mecanismos tecnicamente equivalentes que permitam correlacionar vulnerabilidades identificadas no ambiente com políticas, filtros, assinaturas ou recomendações de mitigação aplicáveis à solução, preservando-se o resultado funcional pretendido pela Administração e afastando-se interpretação de vinculação a fluxo proprietário específico.

V.4 — Do item 8.10.4.63 (citação nominal de ferramentas e número fixo de relatórios)

A requerente questiona o item 8.10.4.63, alegando que a referência nominal às ferramentas Qualys, Nessus e Nexpose, bem como a exigência de pelo menos 20 modelos pré-estabelecidos de relatório, configurariam direcionamento indevido e restrição à competitividade.

O pleito merece acolhimento parcial.

A integração com ferramentas de avaliação de vulnerabilidades é pertinente ao objeto, pois permite correlacionar exposição do ambiente, vulnerabilidades conhecidas, ativos afetados e políticas de prevenção de intrusão, contribuindo para priorização de riscos e ajuste das proteções. Da mesma forma, a existência de relatórios técnicos, executivos e operacionais é relevante para auditoria, governança, acompanhamento de incidentes e apoio à tomada de decisão.

Todavia, a citação nominal de ferramentas específicas deve ser compreendida como referência a soluções amplamente utilizadas no mercado, e não como rol taxativo ou obrigatório. A Administração não pretende restringir a participação a soluções compatíveis apenas com os produtos nominalmente indicados, mas assegurar capacidade de integração com ferramentas de avaliação de vulnerabilidades por meios tecnicamente adequados.

Quanto ao número mínimo de relatórios, reconhece-se que a exigência busca assegurar capacidade analítica mínima da solução. Contudo, o atendimento da necessidade pode ocorrer por relatórios pré-definidos, modelos customizáveis, painéis exportáveis ou outros mecanismos equivalentes que permitam evidenciar os principais riscos, eventos, ataques, ativos afetados, tendências e recomendações.

Dessa forma, acolhe-se parcialmente a impugnação para admitir integração com ferramentas de avaliação de vulnerabilidades por API, conectores suportados, formatos padronizados ou mecanismos equivalentes, bem como relatórios pré-definidos ou customizáveis que atendam à finalidade operacional pretendida, sem vinculação exclusiva às ferramentas nominalmente citadas ou a catálogo específico de relatórios.

V.5 — Dos demais itens da Seção 8.10.4 (itens 8.10.4.2 a 8.10.4.70), decorrentes do item 8.10.4.1

A requerente sustenta que os demais requisitos técnicos constantes da Seção 8.10.4 decorreriam da exigência prevista no item 8.10.4.1, razão pela qual requer sua flexibilização para admitir a entrega das funcionalidades em plataforma consolidada de segurança de rede.

O pleito não merece acolhimento integral.

Conforme demonstrado na análise do item 8.10.4.1, a Administração definiu, na fase de planejamento da contratação, a necessidade de solução NGIPS dedicada, em razão das características do ambiente institucional, da criticidade dos ativos protegidos, da necessidade de operação inline, da previsibilidade de desempenho, da baixa latência, da disponibilidade, do bypass, da segregação das funções de segurança e da responsabilização técnica pela camada de prevenção de intrusão.

Nesse contexto, os requisitos constantes dos itens 8.10.4.2 a 8.10.4.70 não constituem exigências arbitrárias ou desconectadas do objeto, mas especificações técnicas necessárias para assegurar que a solução NGIPS dedicada entregue as capacidades funcionais, operacionais e de desempenho pretendidas pela Administração.

As funcionalidades relacionadas a interfaces, expansão, bypass, armazenamento, throughput, latência, conexões simultâneas, inspeção SSL, redundância, regras, filtros, políticas, reputação, geolocalização, proteção contra malware, alta disponibilidade, gerenciamento centralizado, integração com SIEM, dashboards, APIs, relatórios, sandbox, autenticação, versionamento e rollback de políticas representam elementos necessários à operação de uma solução corporativa de prevenção de intrusão de próxima geração.

A substituição desses requisitos por expressões genéricas vinculadas apenas à “demanda real do

órgão" reduziria a objetividade do julgamento, dificultaria a comparação isonômica entre propostas e poderia permitir o fornecimento de solução subdimensionada ou incapaz de atender aos níveis de desempenho e disponibilidade previstos no estudo técnico. As métricas e características indicadas no Termo de Referência decorrem do dimensionamento realizado pela Administração e representam parâmetros mínimos para garantir que a solução opere de forma adequada no ambiente protegido.

Também não procede a alegação de que tais requisitos seriam inválidos por estarem associados à arquitetura dedicada. Uma vez tecnicamente justificada a necessidade de NGIPS dedicado, mostram-se igualmente pertinentes os requisitos de hardware, capacidade, alta disponibilidade, gerenciamento, integração, atualização e resposta que asseguram a efetividade dessa arquitetura.

Ressalta-se que a Administração não exige marca ou modelo específico, mas características técnicas mínimas compatíveis com a arquitetura definida no planejamento da contratação. O fato de plataformas consolidadas, NGFW ou UTM não atenderem a determinados requisitos próprios de uma solução NGIPS dedicada não caracteriza, por si só, restrição indevida à competitividade, mas apenas incompatibilidade com a solução tecnicamente definida como necessária.

Todavia, assiste razão parcial à requerente quanto à conveniência de afastar interpretações que possam vincular o atendimento de determinados itens a nomenclaturas comerciais, integrações nominais ou ferramentas específicas, quando a finalidade técnica puder ser atendida por mecanismos equivalentes.

Assim, eventuais referências nominais a ferramentas de mercado, a exemplo de soluções de SIEM, ferramentas de avaliação de vulnerabilidades ou integrações específicas, deverão ser compreendidas como referências funcionais ou exemplos de mercado, admitindo-se mecanismos equivalentes por meio de API, syslog, formatos padronizados, conectores suportados, integração nativa ou outro meio tecnicamente adequado, desde que preservada a finalidade operacional do requisito.

Da mesma forma, nomenclaturas de ações, categorias, filtros, relatórios, dashboards ou mecanismos de resposta não deverão ser interpretadas como exigência de terminologia proprietária de fabricante específico, mas como descrição da capacidade funcional esperada, admitindo-se nomenclaturas equivalentes desde que a solução comprove atendimento integral ao resultado pretendido.

Em especial, quanto a itens que contenham referência nominal a solução de SIEM, ferramentas de terceiros, relatórios, APIs ou integrações, a Administração admite mecanismos equivalentes que assegurem a mesma capacidade de monitoramento, correlação, exportação, alerta, resposta ou integração operacional. Tal interpretação não reduz o nível técnico exigido, apenas evita que nomes comerciais ou exemplos de mercado sejam tratados como rol taxativo.

Quanto aos itens que exigem integração com sandbox, reputação, inteligência de ameaças, quarentena, APIs, listas de reputação e mecanismos de resposta, mantém-se a necessidade de integração efetiva e operacionalmente suportada, uma vez que tais capacidades são essenciais para fechamento do ciclo de detecção, prevenção, investigação e resposta. Contudo, quando a finalidade puder ser atingida por integração oficialmente suportada, mecanismo nativo, API documentada ou conector do fabricante, não se deve interpretar a redação de modo a restringir indevidamente a solução a fluxo proprietário específico, desde que preservadas a rastreabilidade, a automação, a segurança e a responsabilização contratual.

A Administração não está obrigada a reduzir o nível técnico da solução pretendida ou alterar a arquitetura de segurança definida em estudo técnico para acomodar modelos comerciais distintos, desde que as exigências estejam motivadas, sejam proporcionais, guardem pertinência com o objeto e possam ser atendidas por soluções existentes no mercado.

Dessa forma, mantém-se a arquitetura NGIPS dedicada definida no planejamento da contratação e mantêm-se as capacidades funcionais, operacionais e de desempenho previstas na Seção 8.10.4, acolhendo-se parcialmente a impugnação apenas para afastar interpretação de que referências nominais, nomenclaturas comerciais, rankings, quantitativos de estrutura de pesquisa ou fluxos específicos constituam, por si sós, exigência exclusiva de fabricante determinado, desde que a licitante comprove o atendimento integral ao resultado funcional pretendido pela Administração.

6.

Acolhe-se parcialmente a impugnação.

A requerente sustenta que os itens 8.10.4.71 a 8.10.4.85 descreveriam plataforma de gestão de superfície de ataque com características próprias de produto específico de mercado, apontando, em especial, a citação nominal de fabricantes no item 8.10.4.76 e a exigência de funcionalidades como índice global de risco, análise baseada em grafos, detecção de contas na dark web e avaliação CASB de aplicações em nuvem.

Sustenta, ainda, que o edital, analisado de forma sistêmica, revelaria direcionamento a fabricante

único, em razão da presença conjunta de requisitos de arquitetura, credenciais de mercado, terminologias, métricas, playbooks e integrações supostamente proprietárias.

A alegação não merece acolhimento integral.

Após análise técnica, verifica-se que a necessidade da Administração é legítima e permanece íntegra. O objetivo dos requisitos é dotar o ambiente institucional de capacidade de visibilidade, correlação e priorização de riscos, relacionando ativos, vulnerabilidades, identidades, ameaças, exposições externas, aplicações em nuvem, eventos de segurança e possíveis caminhos de ataque.

Em ambientes corporativos complexos, a simples listagem de vulnerabilidades, alertas ou eventos isolados não é suficiente para orientar a resposta da equipe técnica. É necessário identificar quais ativos estão mais expostos, quais identidades ampliam o risco, quais vulnerabilidades possuem maior probabilidade de exploração, quais controles estão ausentes ou mal configurados e quais ações reduzem de forma mais efetiva a superfície de ataque da Administração.

A exigência é de plataforma integrada e de capacidades funcionais de gestão de exposição, não de fabricante único. A Administração busca uma solução concebida para operar de forma unificada, com administração centralizada, integração nativa entre componentes, compartilhamento de inteligência de ameaças, correlação de eventos, sincronização de políticas, automação de respostas, rastreabilidade operacional e responsabilização técnica clara.

A exigência de unificação arquitetural e operacional não se confunde com exclusividade mercadológica. Diversos fabricantes e players do mercado de segurança cibernética disponibilizam plataformas integradas ou ecossistemas nativamente interoperáveis capazes de atender, em tese, aos requisitos funcionais do edital. O objetivo da Administração é evitar a entrega de conjunto heterogêneo de produtos independentes, integrados apenas por conectores pontuais, APIs ou mecanismos externos que não assegurem o mesmo nível de consistência operacional.

VI.1 — Dos itens 8.10.4.72 a 8.10.4.74 — Abordagens de análise, grafos e índice de risco

A requerente sustenta que os requisitos relativos a abordagens de análise, análise baseada em grafos e índice global de risco corresponderiam a terminologias e métricas próprias de determinada plataforma de mercado.

O pleito merece acolhimento apenas parcial.

A Administração entende que tais funcionalidades são pertinentes ao objeto, pois permitem transformar dados dispersos em priorização operacional. A correlação entre ativos, identidades, vulnerabilidades, ameaças, exposições, eventos e impactos é essencial para que a equipe técnica compreenda a criticidade real de cada risco e possa priorizar ações de mitigação.

A análise relacional, inclusive por meio de grafos ou mecanismos equivalentes, permite visualizar dependências, caminhos de ataque, relações entre ativos, contas privilegiadas, vulnerabilidades exploráveis e controles ausentes. Essa capacidade é especialmente relevante em ambientes complexos, nos quais a avaliação isolada de vulnerabilidades pode gerar excesso de alertas e baixa efetividade na priorização.

Da mesma forma, a existência de índice, score, pontuação ou métrica consolidada de risco é funcionalidade relevante para apoiar a tomada de decisão, a comunicação executiva, a priorização de remediação e o acompanhamento da evolução da postura de segurança ao longo do tempo.

Todavia, tais expressões não deverão ser interpretadas como exigência de nomenclatura, métrica proprietária ou modelo exclusivo de determinado fabricante. Serão admitidos mecanismos equivalentes de pontuação, score, índice, matriz de risco, priorização contextual, análise relacional, grafo, caminho de ataque ou visualização equivalente que permitam relacionar ativos, identidades, vulnerabilidades, ameaças e impactos, desde que atendam ao resultado funcional pretendido.

VI.2 — Do item 8.10.4.76 — Citação nominal de fabricantes como fontes de dados de terceiros

A requerente questiona a citação nominal de fabricantes de firewall, segurança web e serviços correlatos como fontes de dados de terceiros, sustentando que tal redação indicaria direcionamento a plataforma específica.

O pleito merece acolhimento parcial.

A Administração reconhece que a citação nominal de fabricantes deve ser compreendida como referência exemplificativa a fontes de dados de mercado, e não como rol taxativo ou obrigatório. A finalidade do requisito é assegurar que a solução seja capaz de ingerir, correlacionar e analisar dados provenientes de soluções de segurança utilizadas no ambiente, tais como firewalls, gateways web, DNS security, proxy, CASB, SWG, EDR, SIEM, ferramentas de vulnerabilidade e demais fontes relevantes.

Não há intenção de exigir integração exclusiva com os fabricantes nominalmente citados, tampouco de posicioná-los como únicos exemplos válidos de soluções de terceiros. O objetivo é garantir interoperabilidade e capacidade de correlação com fontes heterogêneas de dados de

segurança.

Dessa forma, serão admitidos mecanismos equivalentes de integração por API, syslog, conectores suportados, formatos abertos, integrações nativas ou outros meios tecnicamente adequados, desde que preservada a capacidade de ingestão, correlação e análise dos dados necessários à gestão da superfície de ataque.

VI.3 — Do item 8.10.4.80 — Detecção de contas e credenciais expostas

A requerente sustenta que a detecção de contas expostas em dark web seria recurso proprietário de determinada plataforma de gestão de risco.

O pleito não merece acolhimento integral.

A finalidade do requisito é permitir a identificação tempestiva de credenciais comprometidas, vazamentos, exposição indevida de identidades e riscos associados ao uso de contas corporativas. Tal capacidade guarda pertinência com a proteção institucional, especialmente diante do uso recorrente de credenciais vazadas ou comprometidas em ataques cibernéticos, acessos indevidos, movimentação lateral e comprometimento de serviços em nuvem.

Contudo, a Administração esclarece que a funcionalidade não precisa ser entregue necessariamente por mecanismo proprietário ou nativo exclusivo de determinada plataforma. Poderá ser provida diretamente pela solução, por serviço de inteligência de ameaças do fabricante, por integração com base externa especializada ou por mecanismo equivalente, desde que haja capacidade de alerta, contextualização e correlação com as identidades, domínios ou ativos do ambiente institucional.

VI.4 — Do item 8.10.4.84 — Playbooks e ações de resposta

A requerente sustenta que o conjunto de ações de resposta descrito no item reproduziria playbook específico de determinada plataforma.

O pleito merece acolhimento parcial.

A Administração entende que a capacidade de resposta operacional, contenção e automação é pertinente ao objeto. A efetividade de uma solução de gestão de exposição e resposta depende não apenas da identificação do risco, mas também da possibilidade de acionar medidas de contenção, mitigação, bloqueio, isolamento, alteração de política, notificação ou integração com fluxos de resposta a incidentes.

Contudo, a Administração esclarece que não pretende exigir reprodução literal de sequência, nomenclatura ou fluxo proprietário de determinado fabricante. Serão admitidas ações equivalentes de resposta, tais como bloqueio, liberação, isolamento, quarentena, redefinição de credenciais, revogação de sessão, alteração de política, bloqueio de aplicação ou URL, registro de evento, notificação, abertura de incidente ou mecanismos similares compatíveis com o ambiente e suportados pela solução ofertada.

O requisito deverá ser interpretado pelo resultado funcional pretendido: permitir que a plataforma apoie ações de resposta e contenção de riscos identificados, de modo integrado à arquitetura de segurança da Administração.

VI.5 — Do item 8.10.4.85 — Avaliação CASB, aplicações em nuvem e conformidades

A requerente questiona a exigência de avaliação CASB de aplicações em nuvem com referência a conformidades como CSA STAR, FINRA e HIPAA, sustentando que tais exigências refletiriam características de plataforma específica.

O pleito merece acolhimento parcial.

A Administração reconhece a pertinência da visibilidade sobre aplicações SaaS, uso de serviços em nuvem, riscos de configuração, exposição de dados, reputação de aplicações, postura de segurança e aderência a políticas institucionais. O uso de aplicações em nuvem representa vetor relevante de exposição, devendo ser considerado na gestão da superfície de ataque.

Todavia, referências a conformidades específicas, como CSA STAR, FINRA, HIPAA ou outras, deverão ser compreendidas como exemplos de bases, critérios ou frameworks de avaliação, e não como exigência eliminatória vinculada a regulamentações estrangeiras sem relação direta com a Administração.

O atendimento poderá ocorrer por avaliação de risco, classificação de aplicações, análise de exposição, reputação, conformidade, postura de segurança em nuvem, controle de uso de aplicações SaaS, integração com CASB ou mecanismo equivalente que permita identificar riscos associados ao uso de aplicações em nuvem.

VI.6 — Da alegação de direcionamento sistêmico a fabricante único

A requerente sustenta que o conjunto de requisitos do edital demonstraria direcionamento sistêmico a fabricante único, mencionando itens relativos a NGIPS dedicado, credenciais de pesquisa, ações de resposta, atualização de assinaturas, integração com SIEM, exigência de componentes do mesmo fabricante e julgamento por menor valor global.

A alegação não merece acolhimento.

A presença conjunta de requisitos de proteção, detecção, investigação, resposta, gestão de exposição, inteligência de ameaças, integração, automação e administração centralizada não caracteriza, por si só, direcionamento a fabricante único. Tais requisitos refletem a arquitetura de plataforma integrada definida pela Administração, cujo objetivo é reduzir fragmentação operacional e permitir atuação coordenada entre os componentes de segurança.

A exigência de plataforma integrada decorre de necessidade operacional legítima: simplificar a administração, reduzir incompatibilidades, evitar múltiplas consoles desconexas, permitir compartilhamento nativo de inteligência, sincronizar políticas, automatizar respostas, melhorar a rastreabilidade e assegurar responsabilização técnica clara durante a execução contratual.

A Administração não pretende limitar o certame a um fornecedor determinado. A exigência é de arquitetura unificada, nativamente integrada e operacionalmente consistente, passível de atendimento por diferentes fabricantes ou players que possuam plataforma integrada de segurança cibernética capaz de cumprir os requisitos do Termo de Referência.

No que se refere às citações nominais, nomenclaturas comerciais, rankings, quantitativos, playbooks ou referências específicas, a Administração admite o aperfeiçoamento interpretativo e redacional necessário para afastar eventual compreensão de que tais elementos constituam exigência exclusiva de determinado fabricante, preservando-se, entretanto, a finalidade técnica de cada requisito.

Não se acolhe, contudo, a pretensão de converter todo o núcleo da solução de gestão de superfície de ataque em critério meramente desejável. A Administração considera essenciais as capacidades de descoberta, correlação, priorização, análise de risco, integração com fontes de dados, identificação de exposição, visibilidade de aplicações em nuvem, detecção de credenciais expostas e apoio à resposta. A transformação integral desses requisitos em opcionais poderia reduzir o nível de segurança pretendido e comprometer a utilidade operacional da solução.

Dessa forma, acolhe-se parcialmente a impugnação para afastar interpretação de que citações nominais, nomenclaturas comerciais, métricas específicas, playbooks, rankings ou referências regulatórias constituam exigências exclusivas de fabricante determinado, admitindo-se mecanismos tecnicamente equivalentes que preservem o resultado funcional pretendido pela Administração.

Mantém-se, entretanto, a exigência de solução capaz de prover visibilidade, correlação, priorização de risco, gestão de exposição, integração com fontes de segurança, análise de identidades, ativos e vulnerabilidades, identificação de exposições externas, avaliação de aplicações em nuvem e apoio à resposta, por se tratar de necessidade técnica compatível com a criticidade do ambiente protegido e com a arquitetura de plataforma integrada definida no planejamento da contratação.

A requerente sustenta que o conjunto das especificações técnicas constantes do Termo de Referência conduziria ao direcionamento da contratação para fabricante específico, em afronta aos princípios da isonomia e da competitividade.

A alegação de direcionamento sistêmico não merece prosperar.

Inicialmente, cumpre destacar que a Administração, ao elaborar o Termo de Referência, observou os princípios previstos na Lei nº 14.133/2021, especialmente os da legalidade, isonomia, competitividade, eficiência, planejamento e seleção da proposta mais vantajosa, estabelecendo requisitos técnicos compatíveis com as necessidades operacionais do ambiente a ser protegido.

As especificações impugnadas não foram definidas com base em determinado fabricante, mas a partir das necessidades técnicas identificadas durante a fase de planejamento da contratação, considerando o elevado grau de criticidade dos ativos de tecnologia da informação, a complexidade do ambiente computacional, a necessidade de integração operacional entre os componentes da solução e os riscos inerentes às ameaças cibernéticas enfrentadas pela Administração.

A exigência de plataforma integrada não se confunde com direcionamento a fabricante único. O que se busca é uma arquitetura unificada de proteção, detecção, investigação, resposta e gestão de riscos cibernéticos, com administração centralizada, compartilhamento de inteligência de ameaças, correlação de eventos, sincronização de políticas, automação de respostas, rastreabilidade operacional e responsabilização técnica clara.

Embora seja tecnicamente possível integrar produtos de fabricantes distintos mediante APIs, conectores ou protocolos padronizados, tais integrações nem sempre asseguram o mesmo nível de interoperabilidade, compatibilidade operacional, governança, suporte, atualização coordenada, automação e correlação proporcionado por uma solução concebida originalmente como plataforma integrada.

É importante ressaltar que a existência de determinado fabricante que atenda integralmente às especificações do edital não constitui, por si só, prova de direcionamento. Da mesma forma, o fato de alguns fabricantes não atenderem à integralidade dos requisitos técnicos não caracteriza

restrição indevida à competitividade, sobretudo quando tais requisitos possuem justificativa técnica, guardam pertinência com o objeto contratado e são proporcionais às necessidades da Administração.

A Administração possui discricionariedade técnica para definir as características do objeto licitado, desde que apresente motivação suficiente e demonstre que as exigências decorrem das necessidades da contratação, não estando obrigada a flexibilizar especificações apenas para ampliar artificialmente o universo de potenciais fornecedores, especialmente quando tal flexibilização puder comprometer o desempenho, a integração, a segurança, a disponibilidade ou a operacionalização da solução pretendida.

No presente caso, as funcionalidades questionadas possuem fundamentação técnica individualizada, conforme demonstrado nos tópicos anteriores desta resposta, estando relacionadas a aspectos de desempenho, integração, disponibilidade, inteligência de ameaças, automação, governança de segurança, gerenciamento centralizado, priorização de riscos e capacidade operacional da solução pretendida.

Ressalte-se, ainda, que o mercado de segurança cibernética é composto por diversos fabricantes globais que disponibilizam soluções com elevado grau de maturidade tecnológica e plataformas integradas de proteção cibernética, sendo possível a participação de diferentes fornecedores capazes de atender à arquitetura pretendida, desde que comprovem o atendimento integral às especificações técnicas estabelecidas.

A requerente não demonstrou, de forma objetiva e conclusiva, que apenas um único fabricante seja capaz de atender ao conjunto dos requisitos. As alegações apresentadas partem, em grande medida, da comparação entre a arquitetura pretendida pela Administração e modelos alternativos de mercado, o que não é suficiente para caracterizar direcionamento, quando a opção técnica adotada está motivada e vinculada às necessidades institucionais.

Não obstante, no exercício de sua autotutela administrativa e em observância aos princípios da eficiência, da razoabilidade, da economicidade, da competitividade e do julgamento objetivo, a Administração realizou análise técnica detalhada dos apontamentos apresentados e identificou a conveniência de promover ajustes pontuais em determinadas especificações.

Tais ajustes não implicam reconhecimento de direcionamento do certame, tampouco redução do nível de segurança pretendido. Tratam-se de aperfeiçoamentos redacionais e interpretativos destinados a afastar eventual compreensão de que referências nominais, nomenclaturas comerciais, métricas específicas, rankings, quantitativos, playbooks, ferramentas ou integrações mencionadas no Termo de Referência constituam exigências exclusivas de determinado fabricante.

Dessa forma, rejeita-se a alegação de direcionamento sistêmico do certame, por não restar demonstrada restrição indevida à competitividade ou afronta aos princípios da isonomia e da ampla participação.

Contudo, acolhe-se parcialmente a impugnação para promover ajustes pontuais nas especificações técnicas indicadas pela área técnica, preservando-se a arquitetura integrada definida no planejamento da contratação e mantendo-se as capacidades funcionais, operacionais, de desempenho, disponibilidade, integração e segurança necessárias ao atendimento do interesse público.

(...)

2.5 SÍNTESE DO PEDIDO DE ESCLARECIMENTO EMPRESA C, ID. (73366751 e 73025772):

(...)

Esclarecimento nº 1 – Da forma de cálculo do percentual de capital social e patrimônio líquido de 5%: Após análise do objeto licitado, verificamos que a redação indica claramente que o período de prestação de serviços será de 3 anos, conforme abaixo, sendo certo que a empresa licitante irá considerar em sua proposta 36 meses de prestação de serviços para composição de seus custos: Objeto: Registro de Preços para contratação de empresa para fornecimento, sob demanda, de solução de segurança para proteção de e-mail, Endpoint e proteção contra-ataques avançados, incluindo instalação, configuração, repasse de conhecimento, suporte técnico e garantia, para atender às necessidades da Secretaria de Estado da Saúde - SESAU/RO, por um período de 3 (três) anos. Ao considerarmos a determinação expressa do Tribunal de Contas da União, por meio do recente acórdão Acórdão 1087/2025-Plenário e posicionamentos anteriores (conforme texto transcrito abaixo), compreendemos que para atendimento ao percentual de Patrimonio líquido ou capital social de 5% indicado em edital, será considerado para o cálculo dos 5% o valor estimado

da licitação para o período anual do contrato. Logo, ao considerarmos que o valor total estimado é de R$ 21.660.280,76 para 3 anos,temos que o valor estimado para 12 meses (1 ano), por lógica do cálculo seria de R$ 7.220.093,58 por ano, sendo, portanto, este o valor que será considerado para o cálculo de 5% de comprovação, segue abaixo a transcrição exata do posicionamento do TCU sobre o tema: 40. Então, a questão apresentada pelo Inmetro não é inovadora e não resta dúvidas de que esta Corte tem entendimento, assentado e anterior à edição da Lei 14.133/2021, de que as exigências econômicofinanceiras devem se ater ao valor estimado para o período de 12 (doze) meses de contrato, independente da sua duração, sob o risco de restrição à competitividade e direcionamento do certame. Acórdão 1087/2025-Plenário Importante destacar que essa administração já se posicionou favorável a este entendimento em processo recente, em que concluir que estava correto o nosso entendimento, conforme documento abaixo: "III – RESPOSTA AO QUESTIONAMENTO PREGÃO ELETRÔNICO N.° 90220/2025 Em atenção ao Pedido de Esclarecimento nº 1, referente à forma de apuração do percentual mínimo de 5% (cinco por cento) de capital social ou patrimônio líquido exigido no subitem 10.6.2 do Edital, informa-se que está correto o entendimento apresentado pela empresa. Resposta Ao Pedido de Esclarecimento - FRANCISCO GANDIN (68705641) SEI 0029.064405/2024-33 / pg. 2 O Tribunal de Contas da União, por meio do Acórdão nº 1087/2025 – Plenário, reafirmou entendimento jurisprudencial pacífico no sentido de que as exigências de qualificação econômico-financeira devem ser calculadas com base no valor estimado da contratação para o período de 12 (doze) meses, independentemente do prazo total de vigência do contrato, sob pena de restrição à competitividade e afronta aos princípios que regem as contratações públicas. Dessa forma, considerando que o valor total estimado da contratação para 36 (trinta e seis) meses é de R$ 29.688.131,50, o valor de referência para fins de cálculo do percentual mínimo de 5% será o valor proporcional correspondente a 12 (doze) meses, qual seja, R$ 9.896.043,83." Assim, com base no contexto apresentado, compreendemos que a comprovação do capital social ou do patrimônio líquido mínimo exigido deverá, assim como no caso análogo apresentado, observar o referido valor por ano (de R$ 7.220.093,58), em estrita conformidade com o entendimento consolidado do Tribunal de Contas da União e com o disposto na Lei nº 14.133/2021.

Esclarecimento nº 1 – Da comprovação de capital social e patrimônio líquido de 5%: Verificamos que o subitem 17.3 do edital exige a comprovação de capital social ou patrimônio líquido na ordem de 5% do valor total estimado da licitação, a ser comprovado por meio do balanço dos 2 últimos exercícios, que resultaria na comprovação de capacidade financeira na ordem de R$ 1.083.014,03. Compreendemos que a exigência é lícita e busca salvaguardar os interesses dessa administração na contratação de empresa que possua capacidade financeira compatível com o contrato. No entanto, embora nossa empresa possua sólida capacidade financeira e diversos contratos de grande vulto, sendo um deles com o próprio estado de Rondônia e possua patrimônio líquido comprovado em 2023 superior a 5 milhões de reais, passamos por reestruturações e em 2024 não possuímos o PL exigido a ser comprovado, o que não significa dizer que a capacidade da empresa está prejudicada, uma vez que há alta liquidez comprovada por meio dos índices contábeis, bem como possuímos R$ 1.000.000,00 de Capital social comprovado nos últimos exercícios. Nesse sentido, para que haja uma ampliação da competitividade e sem qualquer prejuízo a solidez exigida pelo edital, compreendemos que será aceito, para atendimento ao item 17.3, empresas já constituídas que possuam comprovação de capital social na ordem de R$ 1.000.000,00 (hum milhão de reais) em relação aos 2 últimos exercícios. Estamos corretos neste entendimento? Esclarecimento nº 2 – Da apresentação das demonstrações contábeis Em relação a apresentação do balanço patrimonial dos 2 últimos exercícios, compreendemos, com base na determinação da a Instrução Normativa RFB nº 2.003/2021, com redação dada pela Instrução Normativa RFB nº 2.142/2023, bem como pela orientação do próprio portal COMPRASNET que as empresas obrigadas ao envio do SPED Contábil ECD, possuem prazo até 30.06.2026 para apresentação das demonstrações contábeis de 2025, sendo portanto aceita a apresentação das demonstrações de 2023 e 2024 para a presente licitação, haja vista que não se encerrou o prazo para o envio do SPED contábil (ECD) referente a 2025, confira-se: Instrução Normativa RFB nº 2.003/2021, com redação dada pela Instrução Normativa RFB nº 2.142/2023: "Art. 5º A ECD deve ser transmitida ao Sistema Público de Escrituração Digital (Sped) até o último dia útil do mês de junho do ano subsequente ao ano-calendário a que se refere a escrituração." Orientação do portal de compras (COMPRASNET OU COMPRASGOVERNAMENTAIS) Portanto, com base na orientação normativa e tema já pacificado por diversos tribunais e pelo próprio portal federal, será aceita a apresentação das demonstrações de 2023 e 2024 para empresas obrigadas a entrega da ECD (Sped Contábeis). Estamos corretos neste entendimento?

(...)

2.6 DA MANIFESTAÇÃO DO SESAU-NSC, ID. (74290105 **e 73033710)**:

(...)

RESPOSTA 1: Em atenção ao pedido de esclarecimento, informa-se que o entendimento apresentado pela empresa está correto no que se refere às contratações com vigência superior a 12 (doze) meses, conforme entendimento consolidado pelo Tribunal de Contas da União, especialmente no Acórdão nº 1087/2025-Plenário, segundo o qual a exigência de patrimônio líquido ou capital social deve ser calculada com base no valor estimado correspondente aos primeiros 12 (doze) meses da contratação.

Entretanto, esclarece-se que tal entendimento não altera as condições do presente certame, uma vez que o objeto previsto no Termo de Referência contempla contratação com vigência de 12 (doze) meses, sendo o valor total estimado da contratação correspondente ao período anual.

Dessa forma, recomenda-se que a SUPEL promova a retificação das informações constantes do instrumento convocatório, caso necessário, a fim de adequá-las às disposições estabelecidas no Termo de Referência, considerando que este constitui o documento técnico que fundamenta a contratação e ao qual o edital deve guardar estrita conformidade.

Assim, considerando que a vigência prevista para a contratação é de 12 (doze) meses, a exigência de patrimônio líquido ou capital social mínimo de 5% deverá incidir sobre o valor total estimado da contratação, correspondente ao período de 1 (um) ano, não sendo aplicável, no presente caso, a divisão do valor estimado em razão de uma suposta vigência de 36 (trinta e seis) meses.

RESPOSTA 2: Em atenção ao questionamento apresentado, esclarecemos que o subitem 17.3 do Edital foi elaborado em conformidade com o disposto no art. 69 da Lei nº 14.133/2021, que autoriza a Administração a exigir a comprovação da qualificação econômico-financeira por meio da apresentação do balanço patrimonial, demonstrações contábeis e patrimônio líquido mínimo.

Nos termos do Edital e do Termo de Referência, exige-se a comprovação de Patrimônio Líquido mínimo correspondente a 5% do valor total estimado da contratação para empresas constituídas há mais de um ano, ou Capital Social mínimo correspondente a 5% do valor estimado para empresas constituídas há menos de um ano.

Considerando que o valor estimado da contratação é de R$ 21.660.280,76 (vinte e um milhões, seiscentos e sessenta mil, duzentos e oitenta reais e setenta e seis centavos), o valor mínimo exigido corresponde a R$ 1.083.014,04 (um milhão, oitenta e três mil, quatorze reais e quatro centavos).

Dessa forma, para as empresas constituídas há mais de um ano, a comprovação deverá ocorrer mediante a demonstração do patrimônio líquido mínimo exigido, não sendo admitida a sua substituição pela simples comprovação de capital social.

Portanto, não procede o entendimento de que empresas constituídas há mais de um ano possam atender ao disposto no subitem 17.3 exclusivamente mediante a comprovação de capital social no valor de R$ 1.000.000,00. Isso porque o Edital estabelece, para essas empresas, a obrigatoriedade de comprovação de patrimônio líquido mínimo equivalente a 5% do valor estimado da contratação, em observância às condições previstas no instrumento convocatório e à legislação pertinente.

Observação: A análise da documentação de habilitação econômico-financeira será realizada pela Pregoeira e equipe de apoio da SUPEL durante a fase de habilitação do certame, observando-se a legislação vigente, as disposições editalícias e a documentação efetivamente apresentada pela licitante.

Em atenção ao questionamento apresentado, esclarecemos que, para as empresas obrigadas à entrega da Escrituração Contábil Digital (ECD), serão aceitas, para fins de habilitação econômico-financeira, as demonstrações contábeis relativas aos exercícios de 2023 e 2024, desde que observados os prazos legalmente estabelecidos para a apresentação da escrituração referente ao exercício de 2025.

Tal entendimento observa o disposto no art. 5º da Instrução Normativa RFB nº 2.003/2021, com redação dada pela Instrução Normativa RFB nº 2.142/2023, segundo o qual a ECD deve ser transmitida ao Sistema Público de Escrituração Digital (SPED) até o último dia útil do mês de junho do ano subsequente ao ano-calendário a que se refere a escrituração.

Assim, enquanto não exigível a apresentação das demonstrações contábeis referentes ao exercício de 2025, serão considerados válidos os balanços patrimoniais e demais demonstrações contábeis dos exercícios de 2023 e 2024, observadas as demais exigências previstas no Edital e na legislação aplicável.

Observação: Caso na fase de habilitação e na análise da documentação econômico-financeira ocorram após o encerramento do prazo legal para entrega da ECD referente ao exercício de 2025, a documentação correspondente a esse exercício poderá ser objeto de análise pela Pregoeira e equipe de apoio da SUPEL, observadas as disposições legais e editalícias aplicáveis ao certame.

(...)

2.7 SÍNTESE DO PEDIDO DE ESCLARECIMENTO EMPRESA D, ID. (73529991):

(...)

01- Esclarecimento

Item 8.10.1.1.3. A proteção para estações de trabalho deverá prover Anti-Malware, Firewall, Host IPS, Controle de Aplicações e Controle de dispositivos em um único agente.

Solicitamos esclarecimento acerca do item 8.10.1.1.3, que estabelece a obrigatoriedade de disponibilização de Anti-Malware, Firewall, Host IPS, Controle de Aplicações e Controle de Dispositivos em um único agente.

Entendemos que o mercado de soluções de proteção de endpoints evoluiu significativamente, existindo atualmente plataformas que substituem tecnologias tradicionais de Host IPS por mecanismos avançados de prevenção de exploits, análise comportamental, inteligência artificial, machine learning e indicadores de ataque (IOAs), oferecendo nível de proteção equivalente ou superior às soluções HIPS convencionais.

Dessa forma, questiona-se:

Serão aceitas soluções que não utilizem especificamente a nomenclatura "Host IPS", mas que comprovadamente entreguem funcionalidades equivalentes ou superiores de prevenção de intrusão, exploração de vulnerabilidades e proteção comportamental em endpoint, por meio de tecnologias modernas de EPP/EDR/XDR, desde que atendam integralmente ao objetivo de segurança pretendido pela Administração?

Nosso entendimento é que serão aceitas soluções com equivalência funcional devidamente comprovada por documentação oficial do fabricante, ainda que a funcionalidade não seja comercialmente denominada "Host IPS". Está correto o entendimento?

02- Esclarecimento

2.1. Item 8.10.3.1.46.

O ambiente controlado de sandbox deve contemplar, pelo menos, os sistemas operacionais CentOS, Windows 10, Windows 7, Windows Server 2003, 2008, 2012 R2, 2016 e 2019; Deve possuir possibilidade de habilitação e desabilitação de regras de inspeção, individualmente, através de interface de gerenciamento web;

Em relação ao item 8.10.3.1.46, solicitamos esclarecer se serão aceitas soluções que realizem análise comportamental avançada e detecção de ameaças em ambiente sandbox por meio de sistemas operacionais equivalentes e suportados pelo fabricante, sem a necessidade de contemplar especificamente versões descontinuadas pelo mercado, tais como Windows Server 2003 e Windows 7. (Verificar a possibilidade de inserir a questão de compatibilidade)

Entendemos que a efetividade da análise comportamental está relacionada à capacidade de detecção das ameaças e não necessariamente à presença de versões específicas de sistemas operacionais já descontinuadas pelos respectivos fabricantes.

Nosso entendimento está correto?

2.2. Item 8.10.3.1.111.

Caso necessário, a CONTRATANTE pode optar em direcionar parte do licenciamento deste módulo para outros módulos da plataforma de Detecção e Resposta, como o monitoramento do e-mail, endpoint ou servidores, sem acréscimos ou mudanças de licenciamento;

Em relação ao item 8.10.3.1.111, que estabelece a possibilidade de direcionamento de parte do licenciamento do módulo de monitoramento de rede para outros módulos da plataforma de Detecção e Resposta (e-mail, endpoint ou servidores), sem alteração de licenciamento, solicitamos esclarecer:

Entendemos que soluções líderes de mercado podem atender integralmente às funcionalidades de NDR, XDR, sandbox, investigação e correlação de eventos exigidas no Termo de Referência, embora adotem modelos comerciais distintos de licenciamento. Dessa forma, visando ampliar a competitividade do certame e assegurar a observância ao princípio da isonomia, será aceito o fornecimento de solução que atenda integralmente às funcionalidades técnicas exigidas, ainda que não possua mecanismo de remanejamento de licenças entre módulos?

2.3. Item 17.6.2.1.

Deverá apresentar Atestado(s) ou Certidão(ões) de Capacidade Técnico operacional, emitido(s)

por pessoa jurídica de direito público ou privado, comprovando que a licitante forneceu, instalou e configurou solução de segurança em características e pelo menos 10% do item 3, Solução de Segurança Avançada para Mitigação de Ameaças na Rede, uma vez que este representa o componente mais complexo e tecnicamente exigente do edital .

O item 17.6.2.1 exige a apresentação de atestado ou certidão de capacidade técnico-operacional que comprove o fornecimento, instalação e configuração de solução correspondente ao Item 3 – Solução de Segurança Avançada para Mitigação de Ameaças na Rede.

Entretanto, considerando que o objetivo da qualificação técnica é comprovar a aptidão da licitante para executar objeto compatível em características, complexidade e relevância tecnológica, entendemos que soluções modernas de segurança cibernética possuem funcionalidades convergentes e complementares, especialmente no contexto de detecção, prevenção, correlação e resposta a ameaças.

Dessa forma, questiona-se:

Serão aceitos atestados de capacidade técnica que comprovem o fornecimento, implantação, configuração e suporte de soluções de segurança cibernética de complexidade equivalente, tais como plataformas de XDR (Extended Detection and Response), EDR (Endpoint Detection and Response), NDR (Network Detection and Response), Gestão de Vulnerabilidades, Threat Intelligence, SIEM, SOC ou outras soluções correlatas de monitoramento, detecção, prevenção e resposta a ameaças, soluções com compatibilidade tecnológica e operacional com o objeto licitado?

Entendemos que a aceitação de atestados de soluções equivalentes atende aos princípios da razoabilidade, competitividade e ampla participação previstos na legislação vigente, sem prejuízo à comprovação da capacidade técnica necessária para a execução contratual.

Caso o entendimento esteja correto, solicitamos a adequação da redação do item para prever expressamente a aceitação de atestados de soluções equivalentes ou similares em características, funcionalidades, complexidade tecnológica e operacional.

2.4. Item 8.10.4.3.

Os módulos disponíveis para a solução NGIPS devem contemplar, pelo menos, expansão até 20 interfaces 10/100/1000Gbps, expansão até 20 interfaces 1Gbps SFP, expansão até 16 interfaces 10Gbps SFP+ e expansão até 4 interfaces.

Solicitamos esclarecimentos e eventual revisão do requisito técnico em referência, uma vez que o item, conforme atualmente redigido, apresenta inconsistências que podem restringir indevidamente a competitividade do certame e dificultar a adequada compreensão do escopo da solução requerida.

A exigência simultânea de expansão para 20 interfaces 10/100/1000 Mbps RJ-45, 20 interfaces 1 Gbps SFP, 16 interfaces 10 Gbps SFP+ e 4 interfaces 40 Gbps QSFP+ resulta em uma capacidade de conectividade significativamente superior ao throughput mínimo exigido de 4 Gbps, criando requisitos potencialmente contraditórios e de difícil atendimento por soluções NGIPS disponíveis no mercado.

Adicionalmente, observa-se que interfaces dedicadas de 1 Gbps SFP, sem suporte a 10 Gbps, não são mais adotadas como padrão nos appliances NGIPS corporativos de última geração. Atualmente, os fabricantes utilizam predominantemente interfaces SFP+ dual-speed (1G/10G), capazes de operar em ambas as velocidades, proporcionando maior flexibilidade e aderência às arquiteturas modernas de rede.

Diante do exposto, solicitamos informar:

Qual a quantidade efetiva de interfaces que deverá estar disponível na implantação inicial da solução;

Qual a quantidade de interfaces prevista para expansão futura;

Quais tipos de interfaces serão efetivamente utilizados no ambiente (RJ-45, SFP, SFP+ e QSFP+);

Se serão aceitas interfaces SFP+ dual-speed (1G/10G) em substituição às interfaces SFP dedicadas de 1 Gbps, considerando tratar-se da tecnologia atualmente disponibilizada pelos principais fabricantes do mercado;

Se o órgão poderá disponibilizar o planejamento de crescimento e o dimensionamento que fundamentaram a exigência das quantidades de interfaces solicitadas, permitindo o correto entendimento da necessidade operacional e o adequado dimensionamento das propostas.

Entendemos que tais esclarecimentos contribuirão para ampliar a competitividade do certame, garantir a isonomia entre os licitantes e possibilitar a oferta de soluções tecnicamente aderentes às necessidades da Administração.

(...)

2.8 DA MANIFESTAÇÃO DO SESAU-NSC, ID. (74291183):

(...)

1.O Entendimento está parcialmente correto. A funcionalidade não precisa, necessariamente, ser denominada comercialmente como “Host IPS”. Serão aceitas soluções que comprovadamente entreguem funcionalidade equivalente ou superior, desde que atendam ao objetivo de segurança previsto no item, incluindo a capacidade de bloquear tentativas de exploração, prevenir intrusões em endpoints e aplicar virtual patching em endpoints, quando aplicável.

A equivalência funcional deverá ser comprovada por documentação oficial do fabricante e/ou documentação técnica da solução ofertada, cabendo à Administração avaliar o atendimento aos requisitos estabelecidos no edital.

2.O Entendimento está parcialmente correto. A Administração esclarece que a relação de sistemas operacionais indicada no item 8.10.3.1.46 tem por objetivo assegurar que a solução de sandbox possua capacidade de análise de ameaças em diferentes contextos operacionais, incluindo ambientes legados que ainda podem existir em infraestruturas corporativas e que, por sua natureza, demandam especial atenção quanto à detecção de códigos maliciosos e tentativas de exploração.

Dessa forma, a solução deverá contemplar os sistemas operacionais indicados ou comprovar, por meio de documentação oficial do fabricante, que possui capacidade técnica equivalente para analisar, identificar e classificar ameaças direcionadas a esses ambientes, ainda que por meio de versões suportadas, perfis de execução, emulação, instrumentação, imagens equivalentes ou outros mecanismos técnicos.

A aceitação da equivalência ficará condicionada à avaliação da Administração, desde que não haja prejuízo ao objetivo de segurança pretendido e seja mantida a exigência de habilitação e desabilitação individual de regras de inspeção por interface de gerenciamento web.

3.**O Entendimento está Correto.** Serão aceitas soluções que atendam integralmente às funcionalidades técnicas exigidas no Termo de Referência, ainda que não possuam mecanismo de remanejamento de licenças entre módulos da plataforma, tais como monitoramento de rede, e-mail, endpoint ou servidores.

A previsão constante do item 8.10.3.1.111 deverá ser interpretada como característica desejável, voltada à flexibilidade operacional e comercial da solução, não constituindo requisito obrigatório para fins de habilitação, classificação ou aceitação da proposta.

Dessa forma, a ausência de mecanismo de remanejamento de licenças entre módulos não será, por si só, motivo de desclassificação, desde que a solução ofertada atenda integralmente aos requisitos técnicos obrigatórios previstos no certame.

4.O Entendimento está incorreto. A exigência prevista no item 17.6.2.1 não impõe a apresentação de atestado referente a solução idêntica ao objeto licitado, nem exige comprovação integral de todas as funcionalidades previstas para o Item 3 – Solução de Segurança Avançada para Mitigação de Ameaças na Rede.

O requisito tem por finalidade comprovar a capacidade técnico-operacional da licitante para fornecer, instalar, configurar e sustentar solução compatível com a parcela de maior relevância técnica do objeto, considerando sua complexidade, criticidade e pertinência para a execução contratual.

Nesse sentido, em observância aos princípios da razoabilidade, da isonomia e da ampliação da competitividade, a Administração exige apenas a comprovação de, no mínimo, 10% das características do Item 3, não sendo necessária a comprovação de atendimento integral ou de solução exatamente idêntica à especificada no edital.

Dessa forma, não serão aceitos atestados genéricos de soluções de segurança cibernética ou de plataformas correlatas, tais como XDR, EDR, NDR, Gestão de Vulnerabilidades, ThreatIntelligence, SIEM, SOC ou outras, quando não demonstrarem, de forma objetiva, compatibilidade técnica e operacional com pelo menos 10% das características exigidas para o Item 3.

A análise dos atestados será realizada pela Administração com base na documentação apresentada, devendo restar comprovadas a pertinência, a similaridade e a compatibilidade das soluções anteriormente fornecidas, instaladas e configuradas com a Solução de Segurança Avançada para Mitigação de Ameaças na Rede.

5. Esta Coordenadoria esclarece que o requisito em questão se refere à capacidade máxima de expansão física e lógica da solução NGIPS, não significando que todas as interfaces indicadas

deverão estar necessariamente disponíveis ou habilitadas na implantação inicial.

A quantidade efetiva de interfaces exigida para a implantação inicial deverá ser aquela necessária ao atendimento da arquitetura proposta, ao throughput mínimo requerido(vide o item 8.10.4.6), à topologia de rede da Contratante e aos demais requisitos técnicos previstos no edital, cabendo à licitante dimensionar adequadamente a solução ofertada.

Quanto à expansão futura, a solução deverá possuir capacidade de crescimento compatível com os módulos de interface previstos no item, de forma a permitir evolução da conectividade sem substituição integral da plataforma, quando tecnicamente aplicável.

Serão aceitas interfaces SFP+ dual-speed, com suporte à operação em 1Gbps e 10Gbps, em substituição às interfaces SFP dedicadas de 1Gbps, desde que comprovada a compatibilidade com transceptores, velocidades e modos de operação exigidos pela Administração.

A exigência de interfaces visa assegurar flexibilidade de implantação em diferentes cenários de conectividade, incluindo portas metálicas RJ-45, interfaces ópticas de 1Gbps, interfaces ópticas de 10Gbps e interfaces de maior capacidade, quando aplicável.

Eventuais propostas que utilizem arranjos equivalentes de interfaces, módulos combinados ou portas dual-speed/multi-speed poderão ser aceitas, desde que comprovem atendimento funcional e operacional ao requisito, sem prejuízo ao desempenho mínimo, à alta disponibilidade, à capacidade de inspeção e aos demais parâmetros técnicos exigidos no edital.

(...)

2.9 SÍNTESE DO PEDIDO DE ESCLARECIMENTO EMPRESA E, ID. (72666763):

(...)

Do Edital, página 60

17.6.2. 2. Documentação Relativos à Qualificação Técnica

17.6.2.1. Deverá apresentar Atestado(s) ou Certidão(ões) de Capacidade Técnico-operacional, emitido(s) por pessoa jurídica de direito público ou privado, comprovando que a licitante forneceu, instalou e configurou solução de segurança em características e pelo menos 30% do item 3, Solução de Segurança Avançada para Mitigação de Ameaças na Rede, uma vez que este representa o componente mais complexo e tecnicamente exigente do edital

Do Termo de Referência, página 122

17.6.2. Documentação Relativos à Qualificação Técnica

17.6.2.1. 2. Documentação Relativos à Qualificação Técnica Deverá apresentar Atestado(s) ou Certidão(ões) de Capacidade Técnico-operacional, emitido(s) por pessoa jurídica de direito público ou privado, comprovando que a licitante forneceu, instalou e configurou solução de segurança em características e pelo menos 10% do item 3, Solução de Segurança Avançada para Mitigação de Ameaças na Rede, uma vez que este representa o componente mais complexo e tecnicamente exigente do edital.

(...)

2.10 DA MANIFESTAÇÃO DO SESAU-NSC, ID. (72913387):

(...)

Em atenção ao questionamento apresentado, esclarecemos que o quantitativo correto a ser considerado para fins de comprovação da qualificação técnica é aquele constante no Termo de Referência (ID 70923055), qual seja, **10% do Item 3 – Solução de Segurança Avançada para Mitigação de Ameaças na Rede**.

Assim, encaminham-se os autos para conhecimento e adoção das providências cabíveis pela Pregoeira/SUPEL, visando à retificação do Instrumento Convocatório (72609716), de modo a adequá-lo às disposições constantes no Termo de Referência (70923055).

(...)

2.11 SÍNTESE DO PEDIDO DE ESCLARECIMENTO EMPRESA F, ID. (72960383):

(...)

Questionamento 1) Existe contrato semelhante vigente ou recém encerrado? Questionamento 2) Se sim, qual o número do contrato? Questionamento 3) Se sim, com qual empresa? Questionamento 4) Se sim, qual o valor atual do contrato?

(...)

2.12 DA MANIFESTAÇÃO DO SESAU-NSC, ID. (73018034):

(...)

Em atenção aos questionamentos apresentados pela empresa F,, esclarecemos que não há contrato semelhante vigente ou recentemente encerrado no âmbito desta Secretaria relacionado ao objeto da presente contratação.

Diante da inexistência de contratação anterior com características equivalentes, informa-se, com a devida consideração, que não há elementos para atendimento dos Questionamentos 2, 3 e 4, uma vez que não existem instrumentos contratuais correlatos dos quais possam ser extraídas informações referentes ao número do contrato, empresa contratada ou valor contratual.

Permanecemos à disposição para prestar quaisquer esclarecimentos adicionais que se façam necessários.

(...)

DA DECISÃO

Tendo em vista o exposto acima, bem como os fatos e argumentos jurídicos apresentados, **RECEBO as arguições do pedido de esclarecimento,** das empresas interessadas, assim, com fulcro nas leis pertinentes, e ainda pelas regras do Edital e total submissão à Lei 14.133/2021, em especial ao art. 5º, em que aborda os princípios: da legalidade, da impessoalidade, da moralidade, da publicidade, da eficiência, do interesse público, da probidade administrativa, da igualdade, do planejamento, da transparência, da eficácia, da segregação de funções, da motivação, da vinculação ao edital, do julgamento objetivo, da segurança jurídica, da razoabilidade, da competitividade, da proporcionalidade, da celeridade, da economicidade e do desenvolvimento nacional sustentável, assim como as disposições do Decreto-Lei nº 4.657, de 4 de setembro de 1942 (Lei de Introdução às Normas do Direito Brasileiro). **Tendo em vista às respostas do setor SESAU-NSC**, com o consequente **a Reabertura da sessão pública**, que ocorrerá no **dia 08 de setembro de 2026, às 10:30 (horário de Brasília/DF)**, por meio da plataforma eletrônica disponível no site: https://www.gov.br/compras/pt-br, permanecendo inalterados os dizeres contidos no Instrumento Convocatório **PREGÃO ELETRÔNICO Nº 90236/2025/LEI Nº 14.133/2021** e anexos.

Colocamo-nos a disposição para quaisquer outros esclarecimentos que se façam necessários através do telefone (69)3212-9269 e e-mail: supelcotec@gmail.com**.**

Publique-se.

Dê ciência a todas as empresas interessadas por meio de regular publicação.

Porto Velho, data e hora do sistema.

GABRIEL ALVES DA SILVA GAMA
Pregoeiro da Comissão de Tecnologia - COTEC
Superintendência Estadual de Compras e Licitações - SUPEL|RO

Documento assinado eletronicamente por **Gabriel Alves Da Silva Gama**, **Pregoeiro(a)**, em 21/08/2026, às 09:49, conforme horário oficial de Brasília, com fundamento no artigo 18 caput e seus §§ 1º e 2º, do Decreto nº 21.794, de 5 Abril de 2017.

A autenticidade deste documento pode ser conferida no site portal do SEI, informando o código verificador **75339151** e o código CRC **2C4D2094**.