DECISÃO SOBRE A IMPUGNAÇÃO AO EDITAL DO PREGÃO ELETRÔNICO Nº 021/2024-EMAP

Trata-se de pedido de impugnação ao Edital do Pregão Eletrônico nº 021/2024 - EMAP, cujo objeto é a contratação de empresa para o fornecimento de evolução tecnológica de proteção de borda, estações de trabalho e servidores da EMAP- Empresa Maranhense de Administração Portuária, bem como serviço de instalação e configuração, conforme quantitativos e especificações do Termo de Referência, Anexo I deste Edital.

Sobre a matéria, prestam-se as seguintes informações e decisão:

I – DA ADMISSIBILIDADE

A previsão legal do instituto da impugnação de instrumento convocatório em processo licitatório jaz na Lei Federal nº 13.303/2016, §1, art. 87, conforme o excerto seguinte:

> § 1º Qualquer cidadão é parte legítima para impugnar edital de licitação por irregularidade na aplicação desta Lei, devendo protocolar o pedido **até 5 (cinco) dias úteis antes da data fixada para a ocorrência do certame**, devendo a entidade julgar e responder à impugnação em até 3 (três) dias úteis, sem prejuízo da faculdade prevista no § 2º. (grifo nosso)

Em semelhantes termos, consigna o item 2.1 do instrumento convocatório ora impugnado que:

> 2.1. Qualquer cidadão ou interessado poderá solicitar esclarecimentos ou impugnar o ato convocatório do Pregão, no prazo de **até 5 (cinco) dias úteis antes da data fixada para a ocorrência do certame**, devendo a impugnação ser julgada e respondida em até 3 (três) dias úteis, nos termos do art. 94 do Regulamento de Licitações e Contratos da EMAP. (grifo nosso)

A par dos regramentos de admissibilidade acima explicitados, em sucinto exame preliminar acerca do pedido de impugnação formulado, tem-se que:

1.1 LEGITIMIDADE: Entende-se que a empresa é parte legítima, por interpretação extensiva do §1º do artigo 87 da Lei Federal nº 13.303/2016.

1.2 FORMA: o pedido da recorrente foi formalizado pelo meio previsto no subitem 2.2 do Edital, com identificação da licitante (subscrito por pessoa indicada como representante legal da empresa), em forma de arrazoado com identificação do ponto a ser atacado e com fundamentação para o pedido.

1.3 TEMPESTIVIDADE: A data de abertura da sessão pública do certame, no sistema compras governamentais do Banco do Brasil (Licitações-e), marcada para ocorrer em **08/07/2024**, conforme extrato

publicado no Diário Oficial do Estado. Assim, conforme a condição decadente de lastro temporal, o pedido de impugnação em exame foi protocolizado na forma **INTEMPESTIVA**, posto que recebido em **04/07/2024**.

II – DAS ALEGAÇÕES

Em apertada síntese, a Impugnante argumenta vícios de isonomia, ampla competitividade e objetivos da EMAP, em vista de a solução apresentada no objeto refletir as especificações de apenas um fabricante, restringindo e direcionando a abrangência da licitação a um grupo seleto dentro do segmento, favorecendo exclusivamente um fabricante específico, conferindo vantagens inquestionáveis devido à maneira como o documento foi delineado. Acrescenta várias características do objeto que segundo a impugnante só se encontram na marca PALO ALTO.

Ao final, requer a Impugnante que a presente IMPUGNAÇÃO seja recebida, avaliada e julgada, não como recurso de impugnação e sim como uma revisão de ato a pedido da parte interessada – cidadão - enquanto não extinto pelo tempo o direito de a Administração rever os seus atos, a pedido ou de ofício.

III - DA ANÁLISE DO MÉRITO

De conhecimento da impugnação apresentada, passa-se a analisar as alegações da Impugnante:

De início, cumpre esclarecer que a Administração procura sempre atender ao interesse público, respeitando todos os princípios basilares da licitação e dos atos administrativos, mormente o da legalidade, considerando-se, ainda, a finalidade total da aquisição ou serviço que se pretende, para o alcance dos objetivos motivadores da contratação e a produção dos benefícios pretendidos da forma mais eficiente e eficaz.

Submetido o presente questionamento ao conhecimento da área técnica requisitante, a fim de subsidiar a decisão da impugnação ora apresentada, a Coordenadoria de Suporte e Redes da EMAP (CORED), setor responsável pela elaboração do Termo de Referência e pesquisa de preços, prestou a seguinte informação:

> "Em resposta ao pedido de impugnação fora do prazo, referente ao edital do Pregão Eletrônico N° 021/2024 – EMAP, que alega direcionamento para um único fabricante, apresentamos seguintes justificativas:
> 1. Sobre o Prazo da Impugnação A impugnação foi apresentada fora do prazo estipulado no edital. O item 2.1 do edital define claramente os prazos para apresentação de impugnações, que foram amplamente divulgados para garantir a transparência do processo. O recorrente, no entanto, não respeitou esses prazos, causando atrasos e transtornos desnecessários ao certame. Esse comportamento parece visar atrapalhar o andamento do processo, prejudicando sua eficiência.
> 2. Legalidade e Transparência do Edital O edital foi elaborado conforme os princípios

de igualdade, impessoalidade, legalidade, moralidade e publicidade, visando sempre a competitividade entre os licitantes. A assinatura digital no documento de impugnação não pôde ser verificada conforme os padrões técnicos da ICP Brasil, comprometendo a autenticidade do documento. Isso sugere que a impugnação foi feita para atrasar o processo, o que é prejudicial ao interesse público.
O Tribunal de Contas da União (TCU) já se pronunciou sobre impugnações abusivas em vários acórdãos, destacando que essas práticas são anticompetitivas e prejudiciais à administração pública.

3 – Dos Critérios Técnicos Justificados Os requisitos técnicos especificados no edital têm como base a necessidade de garantir a qualidade, durabilidade e funcionalidade do objeto licitado. Tais especificações não visam restringir a competição, mas assegurar que o produto atenda às necessidades específicas do órgão.
Contrariamente ao alegado, o edital permite a participação de diversos fabricantes que atendam aos critérios estabelecidos. A comissão de licitação tomou o cuidado de não incluir especificações que favorecessem indevidamente qualquer fornecedor específico.

Quanto aos itens mencionados pelo recorrente apresentamos abaixo a comprovação de atendimento de outros fabricantes:
2.3.2. Deve possuir throughput de, no mínimo, 4 (quatro) Gbps com funcionalidades de controle de aplicação, IPS, Antivírus e Anti-Spyware habilitadas simultaneamente na solução. A comprovação se dará através de documentação técnica do fabricante de acesso público informando os throughput aferidos com tráfego HTTP ou blend de protocolos definidos pelo fabricante como tráfego real;
- O item em questão é atendido tanto pelo Fortigate 400E ou o Checkpoint 6700 conforme pode ser verificado nos datasheet dos produtos e assim não caracteriza um edital direcionado para Palo Alto.
https://www.fortinet.com/content/dam/fortinet/assets/data-sheets/FortiGate_400E.pdf
https://www.checkpoint.com/downloads/products/6700-security-gateway-datasheet.pdf

2.3.6. Deve possuir, no mínimo, 8 (oito) interfaces físicas de rede de 1/10 Gbps do tipo SFP/SFP+;
- O item em questão é atendido tanto pelo Fortigate 400E ou o Checkpoint 6700 conforme pode ser verificado nos datasheet dos produtos e assim não caracteriza um edital direcionado para Palo Alto.
https://www.fortinet.com/content/dam/fortinet/assets/data-sheets/FortiGate_400E.pdf
https://www.checkpoint.com/downloads/products/6700-security-gateway-datasheet.pdf

2.3.10. Deve possuir armazenamento interno de, no mínimo, 240 (duzentos e quarenta) GB para registro de logs;
- O item em questão é atendido tanto pelo Fortigate 401E ou o Checkpoint 6700 conforme pode ser verificado nos datasheet dos produtos e assim não caracteriza um

edital direcionado para Palo Alto.
https://www.fortinet.com/content/dam/fortinet/assets/data-sheets/FortiGate_400E.pdf
https://www.checkpoint.com/downloads/products/6700-security-gateway-datasheet.pdf

2.3.12. Possuir interface dedicada e física para gerenciamento do equipamento fora de banda. Essa interface deve ser um canal de gerenciamento que funcione mesmo quando o dispositivo não responda. Caso o equipamento não possua essa interface física/dedicada, deverá ser composta com outro equipamento de terceiro onde faça essa função. Não sendo permitido qualquer tipo de configuração via software ou uso da interface dedicada de gerenciamento;
- O item em questão é atendido tanto pelo Fortigate ou Checkpoint conforme pode ser verificado nos links dos produtos e assim não caracteriza um edital direcionado para Palo Alto.
https://docs.fortinet.com/document/fortigate/7.0.0/ngfw-deployment/436050/configuring-the-manageme nt-interface

https://sc1.checkpoint.com/documents/R81/WebAdminGuides/EN/CP_R81_Gaia_AdminGuide/Topics-GAG/Management-Interface.htm

2.3.19. O hardware e software que executem funcionalidades de proteção de rede, bem como a console de gerência e monitoração, devem ser do tipo appliance. Não serão aceitos equipamentos servidores e sistema operacional de uso genérico.
- O item em questão é atendido tanto pelo Fortigate ou Checkpoint, pois os equipamentos desses fabricantes são do tipo appliance e assim não caracteriza um edital direcionado para Palo Alto.

2.3.21. Deve suportar os seguintes tipos de NAT:
- O item em questão é atendido tanto pelo Fortigate ou Checkpoint conforme pode ser verificado nos links dos produtos e assim não caracteriza um edital direcionado para Palo Alto.
https://docs.fortinet.com/document/fortigate/7.4.4/administration-guide/188051/source-nat
https://sc1.checkpoint.com/documents/R81/WebAdminGuides/EN/CP_R81_SecurityManagement_AdminGuide/Topics-ECMG/Configuring-NAT-Policy.htm

2.3.21.9. Suportar NAT de Origem e NAT de Destino simultaneamente
- O item em questão é atendido tanto pelo Fortigate ou Checkpoint conforme pode ser verificado nos links dos produtos e assim não caracteriza um edital direcionado para Palo Alto.
https://community.fortinet.com/t5/FortiGate/Technical-Tip-Configuration-example-of-source-and-destination/ta-p/192769
https://sc1.checkpoint.com/documents/R81/WebAdminGuides/EN/CP_R81_SecurityM

anagement_AdminGuide/Topics-SECMG/Working_with_Manual_NAT_Rules.htm

2.3.26. Proteção contra anti-spoofing;
- O item em questão é atendido tanto pelo Fortigate ou Checkpoint conforme pode ser verificado nos links dos produtos e assim não caracteriza um edital direcionado para Palo Alto.
https://community.fortinet.com/t5/FortiGate/Technical-Tip-Confirm-antispoofing-is-functioning-as-intended/ta-p/256880
https://sc1.checkpoint.com/documents/R81.10/WebAdminGuides/EN/CP_R81.10_SecurityManagement_AdminGuide/Topics-SECMG/Preventing-IP-Spoofing.htm

2.3.28. Para IPv6, deve suportar roteamento estático e dinâmico (OSPFv3);
- O item em questão é atendido tanto pelo Fortigate ou Checkpoint conforme pode ser verificado nos
links dos produtos e assim não caracteriza um edital direcionado para Palo Alto.
https://docs.fortinet.com/document/fortigate/7.4.4/administration-guide/106098/ospfv3-and-ipv6
https://sc1.checkpoint.com/documents/R80.30/WebAdminGuides/EN/CP_R80.30_Gaia_Advanced_Routing_AdminGuide/html_frameset.htm?topic=documents/R80.30/WebAdminGuides/EN/CP_R80.30_Gaia_Advanced_Routing_AdminGuide/162202

2.3.30. Deve suportar o protocolo MP-BGP (MultiprotocolBGP) permitindo que o firewall possa anunciar rotas multicast para IPv4 e rotas unicast para IPv6;
- O item em questão é atendido tanto pelo Fortigate ou Checkpoint conforme pode ser verificado nos links dos produtos e assim não caracteriza um edital direcionado para Palo Alto.
https://docs.fortinet.com/document/fortigate/7.4.0/new-features/52499/using-mp-bgp-evpn-with-vxlan
https://sc1.checkpoint.com/documents/R80.40/WebAdminGuides/EN/CP_R80.40_Gaia_Advanced_Routin g_AdminGuide/Topics-GARG/IPv6-BGP.htm

2.3.34. Modo Camada – 3 (L3), para inspeção de dados em linha e ter visibilidade e controle do tráfego em nível de aplicação operando como default gateway das redes protegidas;
- O item em questão é atendido tanto pelo Fortigate ou Checkpoint conforme pode ser verificado nos links dos produtos e assim não caracteriza um edital direcionado para Palo Alto.
https://docs.fortinet.com/document/fortigate/7.4.0/ips-architecture-guide/756476/l3-nat-route-mode#:~:text=In%20this%20mode%2C%20the%20FortiGate,where%20the%20traffic%20is%20routed.
https://sc1.checkpoint.com/documents/R81/WebAdminGuides/EN/CP_R81_Installation

_and_Upgrade_Guide/Topics-IUG/Routing-and-Bridge-Interfaces.htm

2.3.38.10. Deve suportar offload de certificado em inspeção de conexões SSL de entrada (Inbound);
- O item em questão é atendido tanto pelo Fortigate ou Checkpoint conforme pode ser verificado nos links dos produtos e assim não caracteriza um edital direcionado para Palo Alto.
https://docs.fortinet.com/document/fortigate/7.4.0/best-practices/598577/ssl-tls-deep-inspection
https://sc1.checkpoint.com/documents/SMB_R80.20/AdminGuides/Locally_Managed/EN/Content/Topics/SSL-Inspection-Policy.htm

2.3.38.11. Deve de-criptografar tráfego Inbound e Outbound em conexões negociadas com HTTP/2, TLS
1.2 e 1.3;
- O item em questão é atendido tanto pelo Fortigate ou Checkpoint conforme pode ser verificado nos links dos produtos e assim não caracteriza um edital direcionado para Palo Alto.
https://docs.fortinet.com/document/fortigate/7.0.0/new-features/710924/http-2-support-in-proxy-mode-ssl-inspection
https://support.checkpoint.com/results/sk/sk116022
https://sc1.checkpoint.com/documents/R81/WebAdminGuides/EN/CP_R81_SecurityManagement_AdminGuide/Topics-SECMG/HTTPS-Inspection.htm
https://docs.fortinet.com/document/fortigate/6.2.0/new-features/35927/tls-1-3-support

2.3.39.1.2. Reconhecer pelo menos 3000 aplicações diferentes, incluindo, mas não limitado: a tráfego relacionado a peer-to-peer, redes sociais, acesso remoto, update de software, protocolos de rede, voip, áudio, vídeo, proxy, mensageiros instantâneos, compartilhamento de arquivos, e-mail;
- O item em questão é atendido tanto pelo Fortigate ou Checkpoint conforme pode ser verificado nos links dos produtos e assim não caracteriza um edital direcionado para Palo Alto.
https://www.fortiguard.com/appcontrol
https://www.checkpoint.com/quantum/application-control/

2.3.39.1.4. Para tráfego criptografado SSL, deve de-criptografar pacotes a fim de possibilitar a leitura de payload para checagem de assinaturas de aplicações conhecidas pelo fabricante;
- O item em questão é atendido tanto pelo Fortigate ou Checkpoint conforme pode ser verificado nos links dos produtos e assim não caracteriza um edital direcionado para Palo Alto.
https://docs.fortinet.com/document/fortigate/7.4.0/best-practices/598577/ssl-tls-deep-

inspection

https://sc1.checkpoint.com/documents/SMB_R80.20/AdminGuides/Locally_Managed/EN/Content/Topics/SSL-Inspection-Policy.htm

2.3.39.1.5. Deve permitir o controle, sem instalação de cliente de software, em máquinas/computadores que solicitem saída à internet para que antes de iniciar a navegação, expandase um portal de autenticação residente no Firewall (Captive Portal);
- O item em questão é atendido tanto pelo Fortigate ou Checkpoint conforme pode ser verificado nos links dos produtos e assim não caracteriza um edital direcionado para Palo Alto.
https://docs.fortinet.com/document/fortigate/7.4.4/administration-guide/934626/captive-portals
https://sc1.checkpoint.com/documents/R81/WebAdminGuides/EN/CP_R81_IdentityAwareness_AdminGuide/Topics-IDAG/Configuring-Identity-Sources-Configuring-Browser-Based-Authentication-in-SmartConsole.htm

2.3.39.1.10. Os dispositivos de proteção de rede devem possuir a capacidade de identificar o usuário de rede com integração ao Microsoft Active Directory, sem a necessidade de instalação de agente no Domain Controller, nem nas estações dos usuários;
- O item em questão é atendido tanto pelo Fortigate ou Checkpoint conforme pode ser verificado nos links dos produtos e assim não caracteriza um edital direcionado para Palo Alto.
https://docs.fortinet.com/document/fortigate/6.4.2/administration-guide/795593/use-active-directory-objects-directly-in-policies
https://sc1.checkpoint.com/documents/R81/WebAdminGuides/EN/CP_R81_IdentityAwareness_AdminGuide/Topics-IDAG/Acquiring-Identities-for-Active-Directory-Users.htm

2.3.39.1.14. Permitir nativamente a criação de assinaturas personalizadas para reconhecimento de aplicações proprietárias na própria interface gráfica da solução, sem a necessidade de ação do
fabricante, mantendo a confidencialidade das aplicações customizadas;
- O item em questão é atendido tanto pelo Fortigate ou Checkpoint conforme pode ser verificado nos links dos produtos e assim não caracteriza um edital direcionado para Palo Alto.
https://docs.fortinet.com/document/ipsengine/7.4.0/custom-ips-and-application-control-signature-syntaxguide/274110/creating-ips-and-application-control-signatures
https://sc1.checkpoint.com/documents/R81/WebAdminGuides/EN/CP_R81_ThreatPrevention_AdminGuide/Topics-TPG/SNORT-Signature-Support.htm

2.3.40.2. Deve ter a capacidade de bloquear ameaças desconhecidas em tempo real;

- O item em questão é atendido tanto pelo Fortigate ou Checkpoint conforme pode ser verificado nos links dos produtos e assim não caracteriza um edital direcionado para Palo Alto.
https://docs.fortinet.com/document/fortigate/7.4.2/ips-concept-guide/756476/signature-based-detection
https://sc1.checkpoint.com/documents/R81/WebAdminGuides/EN/CP_R81_ThreatPrevention_AdminGuide/Topics-TPG/IPS_Protections.htm

2.3.40.10. Deverá possuir os seguintes mecanismos de inspeção de IPS;
2.3.40.10.2. Análise de decodificação de protocolo;
- O item em questão é atendido tanto pelo Fortigate ou Checkpoint conforme pode ser verificado nos links dos produtos e assim não caracteriza um edital direcionado para Palo Alto.
https://www.checkpoint.com/quantum/intrusion-prevention-system-ips/
https://docs.fortinet.com/document/fortigate/7.4.4/administration-guide/419589/ips-configuration-options#:~:text=The%20FortiGate%20Intrusion%20Prevention%20system,meet%20the%20HTTP%20protocol%20standards.

2.3.40.10.4. Análise heurística;
- O item em questão é atendido tanto pelo Fortigate ou Checkpoint conforme pode ser verificado nos links dos produtos e assim não caracteriza um edital direcionado para Palo Alto.
https://docs.fortinet.com/document/fortigate/7.4.4/administration-guide/565562/intrusion-prevention
https://www.checkpoint.com/cyber-hub/network-security/what-is-ips/

2.3.40.10.7. Bloqueio de pacotes malformados”
- O item em questão é atendido tanto pelo Fortigate ou Checkpoint conforme pode ser verificado nos links dos produtos e assim não caracteriza um edital direcionado para Palo Alto.
https://community.fortinet.com/t5/FortiGate/Technical-Tip-How-does-the-IPS-engine-determine-if-a-packet/ta-p/199692
https://support.checkpoint.com/results/sk/sk163481

2.3.40.17. Deverá possibilitar a criação de assinaturas customizadas pela interface gráfica do produto;
- O item em questão é atendido tanto pelo Fortigate ou Checkpoint conforme pode ser verificado nos links dos produtos e assim não caracteriza um edital direcionado para Palo Alto.
https://docs.fortinet.com/document/ipsengine/7.4.0/custom-ips-and-application-control-signature-syntaxguide/274110/creating-ips-and-application-control-signatures

https://sc1.checkpoint.com/documents/R81/WebAdminGuides/EN/CP_R81_ThreatPrevention_AdminGuide/Topics-TPG/SNORT-Signature-Support.htm

2.3.40.19. Deve ser capaz de analisar em tempo real através de mecanismos baseados em Machine
Learning o tráfego de ameaças avançadas de C2 (comando e controle) e spyware para proteção de
ameaças de dia zero;
- O item em questão é atendido tanto pelo Fortigate ou Checkpoint conforme pode ser verificado nos links dos produtos e assim não caracteriza um edital direcionado para Palo Alto.
https://www.checkpoint.com/cyber-hub/cyber-security/what-is-ai-cyber-security/
https://www.fortinet.com/resources/cyberglossary/what-is-machine-learning

2.3.40.21. Deve suportar a captura de pacotes (PCAP), por assinatura de Malware e aplicação;
- O item em questão é atendido tanto pelo Fortigate ou Checkpoint conforme pode ser verificado nos links dos produtos e assim não caracteriza um edital direcionado para Palo Alto.
https://docs.fortinet.com/document/fortigate/7.4.4/administration-guide/462154/using-the-packet-capture-tool
https://support.checkpoint.com/results/sk/sk141412

Conclusão
O edital foi elaborado de forma justa e transparente, sem direcionamento para um único fabricante.
Com base na intempestividade da impugnação, solicitamos sua rejeição sumária, garantindo a continuidade do processo licitatório de maneira justa e competitiva."

De acordo com as lições de Marçal Justen Filho:

" (...) O requisito previsto no edital se identifica como instrumento de assegurar (ou reduzir o risco de não se obter) o interesse público. Assim, o interesse público concreto a que se orienta a licitação se identifica como o ´fim´ a ser atingido. Todas as exigências se caracterizam como ´meios´ de conseguir aquele fim. Logo, **a inexistência de vínculo lógico entre a exigência e o fim acarreta a invalidade daquela. Somente se admite a previsão de exigência se ela for qualificável, em um juízo lógico, como necessária à consecução do ´fim´.**" (Justen Filho, Marçal Comentários à lei de licitações e contratos administrativos. 9. Ed. São Paulo: Dialética, 2002. p. 446). (*grifo nosso*)

Desse modo, se infere que é dever da Administração observar, por ocasião da elaboração do

termo de referência, os requisitos que satisfaçam as necessidades da Administração, devendo o gestor público, no esteio de sua competência discricionária, decidir qual é a solução mais adequada ao caso concreto.

Conforme aludido na justificativa da contratação, o cenário atual, marcado por uma evolução constante e crescente sofisticação das ameaças cibernéticas, torna-se imperativo para nós, na Empresa Maranhense de Administração Portuária (EMAP), reconhecer e reforçar a segurança da Tecnologia da Informação e Comunicação (TIC) como um pilar fundamental. Esta necessidade não apenas abrange a preservação da integridade, confidencialidade e disponibilidade de nossos recursos tecnológicos, mas também implica uma abordagem proativa e especializada para a segurança dos dados e sistemas críticos que sustentam nossa operação.

Com efeito, a contratação pretendida visa, dentre outros, a melhoria e, sobretudo, uma abordagem integrada de segurança, que inclui a necessidade de um sistema de gerenciamento centralizado e integrado.

Desta feita, repise-se, trata de um objeto com especificações que abrange mais de um fornecedor, contrariando qualquer irregularidade que venha comprometer a competitividade da licitação, cumprindo condições que viabilizam a participação de interessados.

Dessa forma, as especificações do objeto estipulados no edital não visa, sob qualquer aspecto, a restrição à competividade, nem fere os princípios norteadores do sistema jurídico vigente, mas o atendimento do interesse público.

Acerca das alegações apresentadas pela impugnante, não foi verificado pela área requisitante a indicação na peça impugnatória de qualquer justificativa técnica que demonstre a necessidade de alteração do Termo de Referência, mas, tão somente, foi apresentada uma dificuldade operacional personalíssima do reclamante.

Destarte, não ficou demonstrado que o edital apresenta qualquer indício de direcionamento e predileção por marca única, nem, tão pouco, ausência dos princípios da impessoalidade, da moralidade, da igualdade e da obtenção de competitividade, não havendo, portanto, que se falar em alteração do Termo de Referência.

De todo o exposto, com base na manifestação da unidade técnica responsável pela elaboração do Termo de Referência, por entender que as especificações do objeto estipulados no edital se encontram dentro dos parâmetros legais e razoáveis, não merecem acolhimento as alegações da Impugnante.

IV – DA DECISÃO DO PREGOEIRO

Diante do exposto e pelas razões aqui apresentadas, **DESCONHECE,** em razão da

intempestividade, para no mérito julgar **IMPROCEDENTE** a impugnação interposta, não havendo necessidade, no ponto aqui apresentado, de reformulação do Edital.

São Luís-MA, 18 de julho de 2024.

Maria de Fátima Chaves Bezerra
Pregoeira da EMAP