



Suelen Torres da Silva <suelen.silva@supel.ro.gov.br>

SOLICITAÇÃO DE ESCLARECIMENTO - PREGÃO ELETRÔNICO Nº 90273/2024/CEL/SUPEL/RO

2 mensagens

Alana Gatti Pereira <alana.pereira@nexa.com.br>
Para: "atendimentosupel@gmail.com" <atendimentosupel@gmail.com>
Cc: NFE Comercial <nfe.comercial@nexa.com.br>

18 de dezembro de 2024 às 14:23

Prezados, boa tarde!

Segue em anexo nossa solicitação de esclarecimentos quanto ao pregão eletrônico Nº 90273/2024

Gentileza confirmarem o recebimento deste.

Desde já agradeço e fico no aguardo.

Atenciosamente

Alana Gatti Pereira

Comercial
+ 55 27 2104-8054
+ 55 27 99229-6984



"Esta mensagem é destinada exclusivamente a seu destinatário e pode conter informações privadas, privilegiadas e confidenciais. Se você a recebeu por engano, por favor, notifique imediatamente o remetente e elimine-a de seu computador. Qualquer disseminação, distribuição ou cópia desta comunicação é estritamente proibida."

"This message is for the designated recipient only and may contain privileged, proprietary, or otherwise private information. If you have received it in error, please notify the sender immediately and delete the original. Any other use of the email by you is prohibited."

 **Questionamentos.docx**
76K

Suelen Torres da Silva <suelen.silva@supel.ro.gov.br>
Para: Alana Gatti Pereira <alana.pereira@nexa.com.br>
Cc: "atendimentosupel@gmail.com" <atendimentosupel@gmail.com>, NFE Comercial <nfe.comercial@nexa.com.br>

19 de dezembro de 2024 às 06:43

Prezado Licitante, bom dia.

Acusamos o recebimento e informamos que seu pedido de esclarecimento foi encaminhado ao pregoeiro responsável, assim que possível retornaremos o contato com a resposta de sua solicitação.

Orientamos ainda que acompanhe através do site as futuras publicações a respeito do referido pregão, pois todas as respostas a esclarecimentos e impugnações serão devidamente publicadas em nossos site.
(<https://rondonia.ro.gov.br/supel/>)

Sem mais para o momento, ficamos à disposição.

Atenciosamente,

À
Comissão de Licitações e Contratos da SUPEL/RO

PEDIDO DE ESCLARECIMENTOS PREGÃO PE 90273/2024/CEL/SUPEL/RO

Assim considerando os itens abaixo e descrito de forma resumida, solicitaremos ao final de cada tópico se nosso entendimento está correto, ou seja:

TERMO DE REFERÊNCIA

4.6. "A Solução deve concentrar a gestão em um único equipamento, podendo esse appliance ser físico ou virtual, e que o mesmo possa gerenciar as funcionalidades de firewall de próxima geração (NGFW) com SD-WAN integrado, Switch e Access Point (Wi-Fi).

Questionamento:

A exigência de concentrar a gestão em um único equipamento, capaz de gerenciar funcionalidades de NGFW com SD-WAN integrado, Switch e Access Point, restringe a participação de fabricantes que utilizam arquiteturas de gerenciamento distribuídas e especializadas. Essa abordagem exclusiva favorece soluções específicas, como as da Fortinet, e ignora alternativas mais modernas e escaláveis disponíveis no mercado. Além disso, concentrar múltiplas funcionalidades críticas em um único dispositivo pode impactar a performance e a segurança da solução. Está correto nosso entendimento?

Sugestão:

O edital deve ser corrigido para permitir que as funcionalidades sejam gerenciadas por soluções integradas, mas não necessariamente concentradas em um único equipamento. Dessa forma, será possível ampliar a competitividade, considerando tecnologias que dividem o gerenciamento entre plataformas específicas (como firewalls, switches e Wi-Fi) enquanto mantêm a integração e a eficiência operacional.

4.7. A contratação de um Firewall NGFW (Next-Generation Firewall) com SD-WAN integrado e Wi-Fi Seguro para a Polícia Civil pode ser justificada com base na necessidade de garantir a segurança da rede e dos dados sensíveis da instituição. A Polícia Civil lida com informações altamente sensíveis, como investigações criminais, dados pessoais de vítimas e suspeitos, registros criminais, entre outros. Um Firewall NGFW é capaz de monitorar e filtrar o tráfego de rede, identificando e bloqueando potenciais ameaças, como ataques cibernéticos e invasões. Isso ajuda a garantir a confidencialidade e integridade dos dados, protegendo as informações confidenciais da Polícia Civil contra acessos não autorizados.

Questionamento:

A justificativa apresentada no edital para a contratação de um Firewall NGFW com SD-WAN integrado e Wi-Fi seguro, ainda que válida, restringe a competitividade ao especificar a integração de todas essas funcionalidades em um único equipamento. Soluções de fabricantes que utilizam arquiteturas distribuídas, permitindo a integração de tecnologias especializadas para firewall, SD-WAN e Wi-Fi, oferecem o mesmo nível de segurança e desempenho, sem a necessidade de concentrar tudo em um único dispositivo. Essa abordagem, além de ampliar as opções de fornecedores, favorece a flexibilidade, escalabilidade e otimização dos recursos. Está correto nosso entendimento?

Sugestão:

O edital deve ser ajustado para permitir que as funcionalidades de NGFW, SD-WAN e Wi-Fi seguro sejam entregues por meio de soluções integradas, mas não obrigatoriamente em um único equipamento. Essa correção amplia a competitividade, possibilitando a participação de fabricantes líderes de mercado que oferecem soluções robustas e especializadas, garantindo a segurança e eficiência exigidas pela Polícia Civil, sem direcionamento para um único fornecedor.

4.18.2.38 - 4.18.2.38. O Gerenciamento centralizado, deve possibilitar a visualização integrada de todas as ferramentas adquiridas, sendo que os equipamentos (Firewall, Switch e Access Point) podem ser gerenciados por esta plataforma integrada, ou plataforma distinta desde todos os log's destes dispositivos sejam enviados para uma Plataforma de Gestão de Log Centralizada;

Questionamento:

A exigência do edital de que o gerenciamento centralizado de firewall, switch e access point seja realizado preferencialmente por uma única plataforma integrada limita a competitividade e direciona para fabricantes específicos, como a Fortinet, que oferecem essa abordagem nativamente. Essa exigência desconsidera soluções de mercado que utilizam plataformas distintas para gerenciamento, mas que garantem integração plena através do envio de logs para uma plataforma centralizada, atendendo às mesmas necessidades de visibilidade e controle. Está correto nosso entendimento?

Sugestão:

O edital deve ser ajustado para aceitar tanto plataformas integradas quanto soluções distintas, desde que os dispositivos sejam capazes de enviar logs para uma Plataforma de Gestão de Log Centralizada. Essa abordagem amplia a competitividade, permitindo que soluções modernas e líderes de mercado participem, sem comprometer a eficiência na gestão e visibilidade centralizada dos ativos.

4.18.2.48. Dessa forma, a integração de um Antivírus NGAV (Next-Generation Antivirus) ao Firewall NGFW (Next-Generation Firewall) traz uma série de vantagens significativas para a segurança da rede:

Ao integrar um Antivírus NGAV ao Firewall NGFW, é possível obter uma camada adicional de detecção de malware. O Antivírus NGAV utiliza técnicas avançadas, como análise comportamental, machine learning e detecção baseada em assinaturas, para identificar e bloquear ameaças conhecidas e desconhecidas. Isso aumenta significativamente a eficácia na detecção e remoção de malware na rede:

A integração permite uma resposta mais rápida a ameaças em tempo real. Quando o Antivírus NGAV detecta uma ameaça, ele pode enviar alertas e informações de eventos de segurança para o Firewall NGFW, que pode agir imediatamente para bloquear o tráfego malicioso ou isolar dispositivos infectados. Isso ajuda a reduzir o tempo de resposta a incidentes e minimiza o impacto de ataques em potencial.

Ao integrar o Antivírus NGAV ao Firewall NGFW, é possível obter uma visão centralizada das atividades de segurança. Isso permite monitorar e analisar o tráfego de rede, eventos de segurança e alertas em um único console de gerenciamento. Essa visibilidade unificada simplifica a administração e facilita a identificação de possíveis ameaças ou padrões de comportamento malicioso

A integração facilita a criação de políticas de segurança unificadas. Sendo possível definir regras no Firewall NGFW para bloquear ou permitir o tráfego com base nas informações e detecções do Antivírus NGAV. Isso garante uma aplicação consistente das políticas de segurança em toda a rede, reduzindo as lacunas de segurança e as chances de exploração de vulnerabilidades.

A integração entre o Antivírus NGAV e o Firewall NGFW pode levar a uma melhor eficiência e desempenho da rede. Ao trabalharem em conjunto, eles podem otimizar a utilização de recursos, evitando a duplicação de tarefas e minimizando o impacto no desempenho da rede. Isso resulta em uma proteção mais eficaz, sem comprometer a velocidade e a qualidade da conectividade

Em suma, a integração de um Antivírus NGAV ao Firewall NGFW oferece uma camada adicional de proteção contra malware, aumenta a visibilidade e controle sobre as atividades de segurança, facilita a resposta rápida a ameaças e melhora a eficiência geral do ambiente de segurança da rede

Questionamento:

A exigência de integração de um Antivírus NGAV (Next-Generation Antivirus) ao Firewall NGFW (Next-Generation Firewall) no edital pode restringir a

competitividade e direcionar para um único fabricante, como a Fortinet. Embora a integração de funções de segurança possa ser vantajosa em alguns casos, muitos fornecedores líderes do mercado oferecem soluções altamente eficientes por meio de arquiteturas descentralizadas, com antivírus baseados em endpoints ou em soluções de segurança na nuvem (como EDRs ou XDRs) que complementam a funcionalidade do firewall, sem comprometê-lo. A centralização excessiva dessas funções em um único equipamento pode gerar limitações em termos de escalabilidade, flexibilidade e interoperabilidade. Está correto nosso entendimento?

Sugestão:

O edital deve ser corrigido para permitir soluções onde o Antivírus NGAV não precise estar diretamente integrado ao Firewall NGFW, mas possa interagir com ele por meio de protocolos de segurança, como syslogs ou APIs, para compartilhamento de informações e alertas de ameaças. Isso permite maior liberdade de escolha entre fabricantes, assegurando que soluções complementares, como EDRs ou XDRs, possam ser utilizadas para fornecer proteção avançada contra malware sem comprometer a capacidade de resposta e a eficiência da rede. Além disso, essa abordagem melhora a interoperabilidade e amplia a competitividade no processo licitatório.

2.5.6. Suportar proxy explícito;

Questionamento:

A exigência de suporte a proxy explícito restringe a participação de fornecedores que oferecem soluções de segurança mais modernas e eficientes. A maioria dos fabricantes líderes de segurança, como Cisco, não implementa mais o proxy explícito como parte de suas soluções de firewall, optando por arquiteturas mais avançadas de segurança em nuvem e inspeção de tráfego. O proxy explícito é uma tecnologia mais antiga, que está sendo substituída por abordagens mais dinâmicas e eficientes, como o uso de segurança baseada em nuvem (SASE), proxies transparentes e soluções de inspeção TLS. Essas abordagens modernas oferecem menor impacto na performance, melhor escalabilidade e uma experiência de usuário mais fluida, sem a necessidade de configurar os dispositivos dos usuários para um proxy explícito.

Sugestão:

O edital deve ser corrigido para permitir o uso de soluções de segurança mais modernas e eficientes, sem exigir o suporte a proxy explícito. Em vez disso, deve-se considerar abordagens atuais, como segurança baseada em nuvem (SASE), proxies transparentes e inspeção TLS, que são amplamente adotadas pelos principais fabricantes. Essas soluções oferecem maior escalabilidade, melhor performance e uma experiência de usuário mais simplificada, sem a necessidade de configurar um proxy explícito.

3.1. Throughput de, no mínimo, 79.5 Gbps com a funcionalidade de firewall, considerando 1518 bytes UDP;

Questionamento:

Throughput Exigido (79,5 Gbps): A exigência de 79,5 Gbps de throughput no ponto 3.1 do edital é exagerada para o uso prático e acaba direcionando para um fornecedor específico, como a Fortinet. O que realmente importa no ambiente é o desempenho com as funcionalidades de segurança ativadas (firewall, controle de aplicação, IPS, antivírus, etc.), que estaria mais próximo dos 9 Gbps, conforme o ponto 3.11 do edital. Esse tipo de requisito superdimensionado compromete a competitividade e pode aumentar os custos desnecessariamente. Está correto nosso entendimento?

Sugestão:

O edital deve ser corrigido para focar no throughput com funcionalidades de segurança ativadas, como firewall, controle de aplicação, IPS e antivírus, em vez de exigir um throughput nominal de 79,5 Gbps que não reflete o uso prático do ambiente. Um valor mais realista seria o de 9 Gbps, conforme mencionado no ponto 3.11, o que garantiria uma competitividade mais justa e evitaria o uso de equipamentos superdimensionados, resultando em economia para o projeto.

3.12. Possuir ao menos 18 interfaces 1 GE RJ45; / 3.13. Possuir ao menos 8 interfaces 10 GE SFP+; / 3.14. Possuir ao menos 8 interfaces 1 GE SFP; / 3.15. Possuir ao menos 1 interface console RJ45;

Questionamento:

Os itens 3.12, 3.13, 3.14 e 3.15 especificam um número exato de interfaces e tipos, o que pode direcionar a escolha para um fabricante específico. Essas exigências limitam a competitividade ao excluir soluções igualmente eficazes e compatíveis que possuem arquiteturas diferentes, mas atendem às mesmas necessidades funcionais. Além disso, exigir configurações específicas de portas pode não refletir as reais necessidades do ambiente. É importante priorizar a flexibilidade para que diferentes fabricantes possam propor soluções tecnicamente equivalentes e economicamente mais vantajosas, ajustadas à demanda do ambiente do cliente.

Sugestão:

O edital deve ser corrigido para permitir uma abordagem mais abrangente, baseada em requisitos funcionais e capacidade total de portas, como por exemplo:

Capacidade mínima de 10 portas 1 GE (RJ45 ou SFP);

Capacidade mínima de 8 portas 10 GE (SFP+);

1 interface para gerenciamento, seja RJ45 ou USB-C;

3.16. Permitir gerenciar até 512 Access Points

Questionamento:

Exigir que o firewall gerencie toda a infraestrutura de rede não só limita as opções de fornecedores, mas também pode comprometer a performance do firewall, que deveria focar em sua função principal de proteção e segurança. Soluções como o Cisco DNA Center proporcionam um gerenciamento mais robusto e flexível da rede, deixando a segurança para dispositivos dedicados e especializados.

Sugestão:

O edital deve ser corrigido para remover a exigência de que o firewall gerencie toda a infraestrutura de rede. Essa função deve ser destinada a soluções de gerenciamento dedicadas, como o Cisco DNA Center, que oferecem uma administração de rede mais robusta e eficiente, enquanto o firewall permanece focado em sua função principal de proteção e segurança. Separar essas responsabilidades melhora a performance e garante uma solução mais escalável e especializada para a rede.

3.17. Permitir gerenciar até 72 Switches;

Questionamento:

Exigir que o firewall gerencie toda a infraestrutura de rede não só limita as opções de fornecedores, mas também pode comprometer a performance do firewall, que deveria focar em sua função principal de proteção e segurança. Soluções como o Cisco DNA Center proporcionam um gerenciamento mais robusto e flexível da rede, deixando a segurança para dispositivos dedicados e especializados.

Sugestão:

O edital deve ser corrigido para remover a exigência de que o firewall gerencie toda a infraestrutura de rede. Essa função deve ser destinada a soluções de gerenciamento dedicadas, como o Cisco DNA Center, que oferecem uma administração de rede mais robusta e eficiente, enquanto o firewall permanece focado em sua função principal de proteção e segurança. Separar essas responsabilidades melhora a performance e garante uma solução mais escalável e especializada para a rede.

3.18. Estar licenciado e/ou ter incluído sem custo adicional, no mínimo, 10 sistemas virtuais lógicos (Contextos) por appliance;

Questionamento:

1. VDOMs não são a única opção para segmentação virtual no mercado. Soluções como multi-context da Cisco ou VRFs também atendem bem às necessidades de segurança e segmentação. Além disso, 10 VDOMs podem ser desnecessários dependendo da escala da rede, e outras soluções poderiam ser mais flexíveis e econômicas, sem perder performance ou segurança.

Sugestão:

O edital deve ser corrigido para permitir outras opções de segmentação virtual, como multi-context ou VRFs, em vez de exigir exclusivamente 10 VDOMs. Soluções como essas, presentes em tecnologias da Cisco e outros fabricantes, são igualmente eficazes em atender às necessidades de segurança e segmentação, proporcionando maior flexibilidade. Além disso, o número de 10 VDOMs pode ser excessivo para algumas redes e não é necessário impor essa exigência, uma vez que existem alternativas mais econômicas e adequadas para diferentes escalas de rede, mantendo a segurança e performance.

4.0.1. Throughput de, no mínimo, 5 Gbps com a funcionalidade de firewall, considerando 1518 bytes UDP;

Questionamento:

A exigência de 5 Gbps de throughput no ponto 4.0.1 do edital é exagerada para o uso prático e acaba direcionando para um fornecedor específico, como a Fortinet. O que realmente importa no ambiente é o desempenho com as funcionalidades de segurança ativadas (firewall, controle de aplicação, IPS, antivírus, etc.), que estaria mais próximo dos 600 Mbps, conforme o ponto 4.0.11 do edital. Esse tipo de requisito superdimensionado compromete a competitividade e pode aumentar os custos desnecessariamente.

Sugestão:

O edital deve ser corrigido para focar no throughput com funcionalidades de segurança ativadas, como firewall, controle de aplicação, IPS e antivírus, em vez de exigir um throughput nominal de 5 Gbps que não reflete o uso prático do ambiente. Um valor mais realista seria o de 600 Mbps, conforme mencionado no ponto 3.11, o que garantiria uma competitividade mais justa e evitaria o uso de equipamentos superdimensionados, resultando em economia para o projeto.

4.0.14. Permitir gerenciar ao menos 16 Access Points;

Questionamento:

Exigir que o firewall gerencie toda a infraestrutura de rede não só limita as opções de fornecedores, mas também pode comprometer a performance do firewall, que deveria focar em sua função principal de proteção e segurança. Soluções como o Cisco DNA Center proporcionam um gerenciamento mais robusto e flexível da rede, deixando a segurança para dispositivos dedicados e especializados.

Sugestão:

O edital deve ser corrigido para remover a exigência de que o firewall gerencie toda a infraestrutura de rede. Essa função deve ser destinada a soluções de gerenciamento dedicadas, como o Cisco DNA Center, que oferecem uma administração de rede mais robusta e eficiente, enquanto o firewall permanece focado em sua função principal de proteção e segurança. Separar essas responsabilidades melhora a performance e garante uma solução mais escalável e especializada para a rede.

4.0.15. Permitir gerenciar ao menos 8 Switches;

Questionamento:

Exigir que o firewall gerencie toda a infraestrutura de rede não só limita as opções de fornecedores, mas também pode comprometer a performance do firewall, que deveria focar em sua função principal de proteção e segurança. Soluções como o Cisco DNA Center proporcionam um gerenciamento mais robusto e flexível da rede, deixando a segurança para dispositivos dedicados e especializados.

Sugestão:

O edital deve ser corrigido para remover a exigência de que o firewall gerencie toda a infraestrutura de rede. Essa função deve ser destinada a soluções de gerenciamento dedicadas, como o Cisco DNA Center, que oferecem uma administração de rede mais robusta e eficiente, enquanto o firewall permanece focado em sua função principal de proteção e segurança. Separar essas responsabilidades melhora a performance e garante uma solução mais escalável e especializada para a rede.

4.0.16. Estar licenciado e/ou ter incluído sem custo adicional, no mínimo, 10 sistemas virtuais lógicos (Contextos) por appliance.

Questionamento:

VDOMs não são a única opção para segmentação virtual no mercado. Soluções como multi-context da Cisco ou VRFs também atendem bem às necessidades de segurança e segmentação. Além disso, 10 VDOMs podem ser desnecessários dependendo da escala da rede, e outras soluções poderiam ser mais flexíveis e econômicas, sem perder performance ou segurança.

Sugestão:

O edital deve ser corrigido para permitir outras opções de segmentação virtual, como multi-context ou VRFs, em vez de exigir exclusivamente 10 VDOMs. Soluções como essas, presentes em tecnologias da Cisco e outros fabricantes, são igualmente eficazes em atender às necessidades de segurança e segmentação, proporcionando maior flexibilidade. Além disso, o número de 10 VDOMs pode ser excessivo para algumas redes e não é necessário impor essa exigência, uma vez que existem alternativas mais econômicas e adequadas para diferentes escalas de rede, mantendo a segurança e performance.

5. ITEM 03 – MÓDULO DE GERENCIAMENTO CENTRALIZADO

Questionamento:

A exigência do edital que trata do módulo de gerenciamento centralizado (item 03) e do módulo de relatoria e retenção de logs (item 04) parece estar fortemente alinhada com uma solução específica (Fortinet), limitando a participação de outros fabricantes e restringindo a competitividade. Cada fabricante de soluções de segurança de rede, como Cisco, Palo Alto, ou Fortinet, possui diferentes abordagens e ferramentas para o gerenciamento e monitoramento de segurança e rede. Insistir em uma arquitetura específica impõe barreiras injustas a outros fornecedores, prejudicando o princípio de igualdade de condições em processos licitatórios.

Sugestão:

O edital deve ser corrigido para que cada fabricante possa propor suas soluções de gerenciamento centralizado e retenção de logs de acordo com seu próprio ecossistema e tecnologias, promovendo um processo mais justo e aberto a diferentes propostas.

6. ITEM 04 – MÓDULO DE RELATORIA E RETENÇÃO DE LOGS

Questionamento:

A exigência do edital que trata do módulo de gerenciamento centralizado (item 03) e do módulo de relatoria e retenção de logs (item 04) parece estar fortemente alinhada com uma solução específica (Fortinet), limitando a participação de outros fabricantes e restringindo a competitividade. Cada fabricante de soluções de segurança de rede, como Cisco, Palo Alto, ou Fortinet, possui diferentes abordagens e ferramentas para o gerenciamento e monitoramento de segurança e rede. Insistir em uma arquitetura específica impõe barreiras injustas a outros

fornecedores, prejudicando o princípio de igualdade de condições em processos licitatórios.

Sugestão:

O edital deve ser corrigido para que cada fabricante possa propor suas soluções de gerenciamento centralizado e retenção de logs de acordo com seu próprio ecossistema e tecnologias, promovendo um processo mais justo e aberto a diferentes propostas.

22.5. PARCELA DE MAIOR RELEVÂNCIA: a parcela de maior relevância e valor significativo dos lotes desta licitação ficam determinadas na forma abaixo:

b) Solução de Conectividade Wireless do tipo Indoor, com suporte aos padrões IEEE 802.11a, IEEE 802.11b, IEEE 802.11g, IEEE 802.11n e IEEE 802.11ac Wave 2, com garantia e suporte pelo período contratual de 60 meses

Questionamento:

Ao exigir apenas a tecnologia IEEE 802.11ac Wave 2 (Wi-Fi 5), o edital está selecionando uma tecnologia que já está em declínio e próxima de End of Life (EOL) em diversos fabricantes. Equipamentos baseados nesse padrão podem se tornar rapidamente obsoletos, principalmente considerando que o contrato é para um período de 60 meses (5 anos). Durante esse período, é altamente provável que os equipamentos baseados em Wi-Fi 5 deixem de ser suportados ou recebam atualizações limitadas, comprometendo a eficiência da rede no longo prazo.

Sugestão:

O edital deve ser corrigido para incluir a exigência de suporte aos padrões Wi-Fi 6 (IEEE 802.11ax) e Wi-Fi 6E, em vez de limitar a tecnologia ao Wi-Fi 5 (IEEE 802.11ac Wave 2). Esses padrões mais recentes oferecem melhorias significativas em termos de capacidade, eficiência e suporte a um maior número de dispositivos conectados, além de serem as tecnologias mais adequadas para suportar a evolução dos endpoints nos próximos anos. A adoção de Wi-Fi 6 e 6E garantirá que os equipamentos permaneçam atualizados e eficientes ao longo dos 60 meses de contrato, evitando obsolescência prematura e maximizando o retorno sobre o investimento.

11.2.51. Deve suportar modulação de até 1024 QAM para os rádios que operam em 2.4 e 5GHz servindo clientes wireless 802.11ax.

Questionamento:

O edital apresenta inconsistências ao solicitar tecnologias de Wi-Fi 5 (802.11ac) em algumas seções, sem especificar claramente a exigência de equipamentos mais modernos, como Wi-Fi 6 (802.11ax). Essa falta de clareza pode gerar propostas que não atendam às expectativas futuras do projeto ou resultem na entrega de equipamentos de diferentes categorias, comprometendo a padronização e a longevidade da solução.

Sugestão:

O edital deve ser atualizado para exigir explicitamente a adoção de soluções Wi-Fi 6 ou superiores, garantindo maior desempenho, suporte a novos dispositivos e alinhamento com as tendências tecnológicas para os próximos anos. Isso também evita ambiguidades e garante que todas as propostas apresentem equipamentos de mesma categoria, promovendo a equidade no processo de seleção.