

Quadro informativo

**Pregão Eletrônico N° 19/2026 (SRP)** (Lei 14.133/2021)**UASG 927919 - DEFENSORIA PÚBLICA DO EST DO RIO DE JANEIRO** Critério julgamento: **Menor Preço / Maior Desconto**Modo disputa: **Aberto**Contratação em período de cadastramento de proposta **Avisos (0)****Impugnações (0)****Esclarecimentos (6)**

04/09/2026 10:06



1. CAPACIDADE E ALTA DISPONIBILIDADE DA SOLUÇÃO DE GERENCIAMENTO



O item 3.2.2 estabelece que a solução de gerenciamento da infraestrutura wireless poderá ser fornecida por meio de CONTROLADORA WIRELESS em formato de appliance físico ou virtual, devendo atender às características técnicas mínimas previstas nos respectivos subitens.

O item 3.2.2.3 determina que a solução deverá possuir capacidade mínima para gerenciamento de 800 (oitocentos) Pontos de Acesso e suporte a 20.000 (vinte mil) usuários simultâneos.

Por sua vez, o item 3.2.2.4 prevê mecanismo de alta disponibilidade nativa baseado em gerenciamento distribuído (Virtual Controller), mediante formação de clusters entre os Pontos de Acesso, com eleição automática de mestre e redundância lógica, estabelecendo ainda que esse mecanismo deverá operar de forma independente de hardware de controladora física ou virtual centralizada dedicada.

Observa-se, entretanto, que controladora wireless centralizada, física ou virtual, e gerenciamento distribuído mediante formação de cluster entre os Pontos de Acesso representam arquiteturas tecnológicas distintas para implementação do gerenciamento da rede wireless.

Em uma arquitetura centralizada, as funções de configuração, gerenciamento, monitoramento e aplicação de políticas são desempenhadas por uma controladora física ou virtual, podendo sua disponibilidade ser assegurada mediante mecanismos próprios de redundância e Alta Disponibilidade – HA.

Em uma arquitetura distribuída, por outro lado, essas funções podem ser executadas de forma distribuída entre os próprios Pontos de Acesso, mediante mecanismos de eleição, redundância e failover, sem dependência de uma controladora física ou virtual centralizada dedicada.

Dessa forma, a eventual exigência cumulativa das duas arquiteturas obrigaria uma mesma solução a implementar simultaneamente gerenciamento centralizado por controladora física ou virtual e gerenciamento distribuído entre os Pontos de Acesso, ainda que qualquer uma dessas arquiteturas, isoladamente, possa atender integralmente às capacidades, funcionalidades e requisitos de disponibilidade pretendidos pela Administração.

Considerando a necessária neutralidade tecnológica e a possibilidade de diferentes fabricantes adotarem arquiteturas distintas para alcançar os mesmos objetivos funcionais, entende-se que os requisitos de gerenciamento e alta disponibilidade deverão ser avaliados pela capacidade e pelas funcionalidades efetivamente proporcionadas pela solução ofertada, e não pela obrigatoriedade de coexistência de duas arquiteturas distintas de gerenciamento.

Diante disso, solicita-se esclarecer: Está correto o entendimento de que será admitida solução baseada, alternativamente, em uma das seguintes arquiteturas de gerenciamento:

a) CONTROLADORA WIRELESS centralizada, fornecida em formato de appliance físico ou virtual, a qual deverá possuir, individualmente, capacidade mínima para gerenciamento de 800 APs e 20.000 usuários simultâneos, além de atender aos demais requisitos técnicos, funcionais, de disponibilidade, gerenciamento, segurança e desempenho estabelecidos no Termo de Referência; ou

b) mecanismo de gerenciamento distribuído entre os Pontos de Acesso, mediante Virtual Controller, formação de cluster ou tecnologia funcionalmente equivalente, o qual deverá suportar, por cluster, no mínimo 800 APs e 20.000 usuários simultâneos, além de atender aos demais requisitos técnicos, funcionais, de disponibilidade, gerenciamento, segurança e desempenho estabelecidos no Termo de Referência, independentemente da arquitetura, tecnologia, nomenclatura ou forma de implementação adotada pelo fabricante?

Entende-se, portanto, que não será exigido o fornecimento cumulativo das duas arquiteturas, bastando que a solução ofertada adote uma delas e que a arquitetura escolhida atenda, de forma autônoma e integral, à capacidade mínima de 800 APs e 20.000 usuários simultâneos, bem como aos demais requisitos estabelecidos no Termo de Referência.

Está correto esse entendimento?

gerenciamento em caso de indisponibilidade de uma de suas instâncias.

Em caso afirmativo, entende-se que deverão estar contemplados na proposta todos os licenciamentos, recursos e componentes de software necessários à implementação dessa arquitetura de HA, sem custos adicionais para a Contratante.

Por fim, caso a Administração entenda que as arquiteturas previstas nos itens 3.2.2.3 e 3.2.2.4 devam ser obrigatoriamente fornecidas de forma cumulativa, solicita-se apresentar a justificativa técnica para a necessidade simultânea de controladora física ou virtual centralizada e mecanismo independente de gerenciamento distribuído entre os Pontos de Acesso, indicando quais funcionalidades, capacidades ou requisitos objetivos não poderiam ser atendidos por apenas uma dessas arquiteturas quando devidamente dimensionada e dotada dos mecanismos de alta disponibilidade exigidos.

2. APRESENTAÇÃO DA MATRIZ DE ADERÊNCIA TÉCNICA NA FASE DE PROPOSTA

O item 7.5 do Edital estabelece que será desclassificada a proposta vencedora que não obedecer às especificações técnicas contidas no Termo de Referência.

Entretanto, o item 4.2.1.3 do Termo de Referência estabelece que o manual do fabricante ou documento similar, acompanhado de instrumento descritivo — matriz, ofício ou índice — indicando de forma clara a comprovação de cada requisito técnico dos itens 3.2.1 e 3.2.2 deverá ser apresentado no ato da entrega dos equipamentos.

Considerando a quantidade, especificidade e relevância dos requisitos técnicos estabelecidos para os Pontos de Acesso e para a Controladora Wireless, entende-se que a verificação da aderência integral da solução somente no momento da entrega poderá gerar significativo risco e transtorno para a Administração caso seja constatado, nessa etapa, que o produto adjudicado não atende integralmente às especificações técnicas obrigatórias.

Nessa hipótese, a constatação de eventual não conformidade poderá ocorrer somente após a conclusão das etapas de julgamento, adjudicação, homologação, assinatura da Ata de Registro de Preços, emissão da ordem de fornecimento ou nota de empenho e entrega física dos equipamentos.

Diante disso, sugere-se que a Matriz de Aderência Técnica prevista no item 4.2.1.3 seja exigida já na fase de apresentação e julgamento da proposta, antes da adjudicação, acompanhada da respectiva documentação técnica comprobatória oficial do fabricante.

Assim, solicita-se esclarecer:

Está correto o entendimento de que poderá ser exigido do licitante provisoriamente classificado em primeiro lugar, juntamente com sua proposta detalhada, a apresentação de Matriz de Aderência Técnica contemplando individualmente todos os requisitos dos itens 3.2.1 e 3.2.2, com indicação do documento técnico oficial do fabricante e respectiva página ou referência onde se encontra comprovado o atendimento de cada requisito?

Caso tal exigência ainda não esteja prevista para essa fase, sugere-se sua inclusão, de forma a permitir à Administração verificar previamente a conformidade técnica da solução antes da adjudicação e contratação, mantendo-se a documentação exigida no ato da entrega como mecanismo adicional de conferência entre os produtos efetivamente entregues e aqueles tecnicamente aprovados no certame.

Solicita-se ainda esclarecer se, para requisitos cuja funcionalidade não esteja expressamente descrita em datasheet ou manual comercial, poderão ser utilizados como comprovação outros documentos técnicos oficiais do fabricante, tais como guias de administração, feature guides, feature matrix ou declaração técnica oficial específica para o modelo ofertado.

3. LICENCIAMENTO PERPÉTUO E CONTINUIDADE DAS FUNCIONALIDADES O item 3.2.2 determina que a CONTROLADORA WIRELESS, física ou virtual, seja fornecida com licenciamento perpétuo, enquanto o item 3.2.2.2 estabelece que deverão estar incluídas todas as licenças de software necessárias para conexão, configuração e gerenciamento.

Por sua vez, o item 5.2.10 estabelece que deverá ser garantido acesso a todas as atualizações de firmware, correções de segurança e resoluções de bugs disponibilizadas pelo fabricante durante o período de 60 (sessenta) meses.

Dessa forma, entende-se que o prazo de 60 meses corresponde ao período de garantia, suporte e direito às atualizações, enquanto as licenças necessárias à operação e gerenciamento da solução possuem caráter perpétuo.

Está correto o entendimento de que, após o encerramento dos 60 meses, os Pontos de Acesso e a solução de gerenciamento deverão continuar plenamente operacionais, mantendo todas as capacidades e funcionalidades adquiridas e licenciadas, sem necessidade de renovação de subscrição ou pagamento periódico obrigatório para continuidade de seu funcionamento?

impossibilidade de gerenciamento dos equipamentos.
Está correto esse entendimento?

4. MECANISMOS DE PROTEÇÃO WIDS/WIPS – NEUTRALIDADE TECNOLÓGICA E EQUIVALÊNCIA FUNCIONAL.

O item 3.2.2.24 estabelece que a solução deverá implementar mecanismos de proteção capazes de identificar ataques à infraestrutura wireless, relacionando expressamente:

- I – EAPOL Flooding;
- II – Association Flood, Authentication Flood, Broadcast Deauthentication e Spoofed Deauthentication;
- III – ASLEAP;
- IV – Null Probe Response ou Null SSID Probe Response;
- V – Long Duration;
- VI – ataques contra Wireless Bridges;
- VII – Weak WEP; e
- VIII – Invalid MAC OUI.

Não se questiona a pertinência de a Administração exigir mecanismos avançados de Wireless Intrusion Detection/Prevention – WIDS/WIPS, destinados à proteção da infraestrutura wireless contra ataques, comportamentos anômalos, tentativas de indisponibilidade e falsificação de identidade.

Entretanto, observa-se que a nomenclatura utilizada para classificação de ataques, alarmes e assinaturas WIDS/WIPS não é padronizada entre os diferentes fabricantes. Uma mesma ameaça pode ser identificada ou mitigada por meio de análise comportamental, inspeção de quadros 802.11, correlação de eventos, thresholds de autenticação e EAP, detecção de flooding, spoofing, rogue devices, proteção de quadros de gerenciamento ou outros mecanismos, sem que a solução utilize necessariamente a mesma denominação atribuída à ameaça no Termo de Referência. Cabe registrar, ainda, que parcela relevante das denominações constantes do item 3.2.2.24 apresenta correspondência direta, inclusive textual, com alarmes e assinaturas documentados no Cisco Wireless Intrusion Prevention System – wIPS/aWIPS. A documentação oficial do fabricante relaciona expressamente, entre outros, Invalid MAC OUI, Authentication Flood, Association Flood, EAPoL-Start Flood, Deauthentication Flood e Broadcast Deauthentication Flood. Da mesma forma, consta expressamente na documentação Cisco a assinatura ASLEAP Tool Detected.

Adicionalmente, algumas das ameaças relacionadas estão diretamente associadas a tecnologias ou mecanismos de segurança legados, como LEAP/ASLEAP e WEP, enquanto redes wireless atuais utilizam mecanismos mais robustos, como WPA2/WPA3, métodos EAP modernos e Protected Management Frames – PMF. Isso não significa que todos os vetores relacionados tenham perdido relevância, pois ataques de flooding, spoofing, manipulação de quadros de gerenciamento e abuso de mecanismos do protocolo 802.11 permanecem tecnicamente possíveis. O ponto é que sua detecção e mitigação podem ser implementadas atualmente por controles distintos e mais abrangentes do que uma assinatura histórica individual.

A própria literatura técnica sobre WIDS/WIPS ressalta que determinadas regras existentes em implementações anteriores podem perder relevância com a evolução das tecnologias wireless e que as políticas de detecção devem considerar os vetores de ataque efetivamente relevantes, o ambiente de RF e as capacidades técnicas da solução.

Dessa forma, eventual interpretação de que cada uma das denominações relacionadas nos incisos I a VIII deverá existir literal e individualmente na solução ofertada poderá ocasionar restrição à competitividade e vinculação tecnológica indireta, excluindo soluções modernas que proporcionem proteção funcionalmente equivalente ou mais abrangente contra os mesmos vetores de ameaça.

Diante do exposto, solicita-se esclarecer:

Está correto o entendimento de que o item 3.2.2.24 será considerado atendido por solução que implemente mecanismos WIDS/WIPS capazes de identificar ameaças e ataques à infraestrutura wireless, contemplando, no mínimo, mecanismos de detecção de ataques de negação de serviço e flooding relacionados ao protocolo 802.11 e aos processos de autenticação/associação, ataques de spoofing e falsificação de identidade, Rogue APs e dispositivos não autorizados, abuso ou falsificação de quadros de gerenciamento e demais anomalias capazes de comprometer a disponibilidade, autenticidade ou segurança da infraestrutura wireless, sendo admitidos mecanismos tecnicamente equivalentes, independentemente da nomenclatura utilizada pelo fabricante?

Entende-se, ainda, que a comprovação do atendimento deverá considerar a capacidade efetiva da solução de detectar, prevenir ou mitigar os respectivos vetores de ameaça ou seus efeitos, não sendo obrigatória a existência individual de assinaturas com denominação idêntica às relacionadas nos incisos I a VIII do item 3.2.2.24.

Está correto esse entendimento?

Caso o entendimento seja diverso, solicita-se esclarecer:

- a) qual a justificativa técnica para a exigência individual e obrigatória de cada uma das assinaturas e denominações relacionadas no item 3.2.2.24;
- b) qual norma técnica, padrão IEEE, RFC ou outra referência técnica aberta e independente de

mesmos vetores de ataque, mediante análise comportamental, detecção de flooding, spoofing, Rogue APs, PMF/IEEE 802.11w, métodos EAP atuais ou outras técnicas equivalentes, não seriam considerados aderentes;

d) qual a justificativa técnica para exigir individualmente assinaturas associadas a tecnologias legadas, como LEAP/ASLEAP e WEP, quando a solução ofertada poderá empregar mecanismos de segurança atuais que não utilizem tais tecnologias; e

e) considerando a correspondência direta de diversas denominações constantes do Termo de Referência com a taxonomia empregada na documentação oficial do Cisco WIPS/aWIPS, como será assegurada a neutralidade tecnológica e a ampla competitividade do certame, caso não sejam admitidos mecanismos WIDS/WIPS funcionalmente equivalentes. O item 3.2.2.25 estabelece que ataques de negação de serviço deverão ser mitigados pela infraestrutura através do envio de pacotes de authentication.

O item 3.2.2.25 estabelece que ataques de negação de serviço deverão ser mitigados pela infraestrutura através do envio de pacotes de authentication.

Considerando que mecanismos de contenção WIPS normalmente empregam quadros de deauthentication para interrupção ou contenção de determinadas ameaças wireless, solicita-se esclarecer se a referência a "authentication" constante do item constitui erro material, devendo ser interpretada como deauthentication.

Adicionalmente, entende-se que serão considerados aderentes mecanismos tecnicamente equivalentes de contenção ou mitigação implementados pela própria infraestrutura wireless, desde que produzam o efeito de neutralizar ou interromper a ameaça detectada, independentemente da nomenclatura ou arquitetura específica utilizada pelo fabricante.

Está correto esse entendimento?

Item 3.2.2.26 – proteção contra ARP Poisoning

O item 3.2.2.26 determina que a solução implemente mecanismos de proteção contra ataques do tipo ARP Poisoning na rede wireless.

Considerando que diferentes fabricantes podem implementar essa proteção mediante mecanismos como inspeção e validação de tráfego ARP, detecção de ARP Spoofing, AntiSpoofing, validação da relação IP/MAC ou outras técnicas de proteção de camada 2, entende-se que será considerada aderente qualquer implementação tecnicamente equivalente capaz de detectar, impedir ou mitigar a falsificação das associações entre endereços IP e MAC.

Está correto esse entendimento?

5. PORTAL WEB PARA VISITANTES – MEIOS DE VALIDAÇÃO E ENVIO DE CREDENCIAIS

O item 3.2.2.15 estabelece que a solução deverá implementar recursos de Portal Web customizável – Captive Portal – para clientes visitantes, com possibilidade de criação de conta por meio de validação "via e-mail, SMS e outros".

A própria utilização da expressão "e outros" indica a existência de diferentes modalidades possíveis de validação, não ficando claro se os meios relacionados deverão ser disponibilizados cumulativamente ou se representam alternativas admitidas pela solução.

Essa interpretação é reforçada pelo item 3.2.2.33, que estabelece expressamente que, após a criação de um usuário visitante, a solução deverá enviar as credenciais por e-mail para o usuário cadastrado.

Dessa forma, entende-se que será considerada aderente a solução que implemente a criação e validação da conta do usuário visitante por e-mail, com posterior envio das respectivas credenciais também por e-mail, conforme determinado no item 3.2.2.33, não sendo obrigatória a disponibilização simultânea de validação por SMS.

Está correto esse entendimento?

Caso negativo, e sendo efetivamente obrigatória a disponibilização de validação por SMS, solicita-se esclarecer:

- a) se o respectivo serviço de gateway ou mensageria SMS deverá integrar o objeto da contratação;
 - b) se os custos de envio de mensagens deverão estar integralmente contemplados na proposta durante os 60 meses de vigência da garantia e suporte;
 - c) qual o quantitativo estimado de mensagens SMS que deverá ser considerado pelos licitantes para formação de seus preços;
 - d) se será admitida integração da solução wireless com serviço de mensageria fornecido por terceiro;
 - e) quem será responsável pela contratação do serviço, manutenção de créditos, franquias ou pacotes de mensagens e respectivos pagamentos; e
 - f) qual será o tratamento aplicável às situações em que a plataforma wireless efetue corretamente a solicitação de envio, porém a mensagem sofra atraso ou não seja entregue em razão de indisponibilidade do gateway contratado ou das redes das operadoras de telecomunicações.
- Considerando que o envio de SMS depende de serviços externos de mensageria e da infraestrutura das operadoras de telefonia móvel, entende-se que eventuais atrasos ou falhas de entrega atribuíveis exclusivamente a tais terceiros não deverão caracterizar indisponibilidade, defeito ou descumprimento de requisito da solução wireless.

Está correto esse entendimento?

Solicitações de correção e esclarecimentos formais

Na tabela de penalidades específicas consta, na ocorrência nº 6:

"Não apresentar garantia contratual dentro do prazo estipulado neste Termo."

A respectiva penalidade estabelece multa diária de 0,5% e registra como limite máximo "20% (dois por cento)", havendo divergência entre o valor numérico e aquele expresso por extenso.

Adicionalmente, não foi identificada no Termo de Referência definição específica da mencionada garantia contratual, indicando percentual, base de cálculo, modalidade ou prazo para apresentação.

Solicita-se esclarecer se será efetivamente exigida garantia contratual do fornecedor e, em caso positivo, indicar expressamente o dispositivo do Edital ou Termo de Referência que estabelece seu percentual, base de cálculo, modalidades admitidas e prazo para apresentação.

Solicita-se, ainda, a correção da divergência existente entre "20%" e "dois por cento" na ocorrência nº 6 da tabela de penalidades.

7. CRITÉRIO DE JULGAMENTO POR LOTE E APRESENTAÇÃO DE LANCES POR ITEM

O Edital estabelece expressamente como critério de julgamento o MENOR PREÇO POR LOTE, sendo o preço máximo estimado por item utilizado como critério de aceitabilidade da proposta.

O Termo de Referência igualmente estabelece julgamento pelo menor preço por lote e prevê que, após a fase de lances, serão informados os valores unitários máximos admitidos para adequação dos preços do primeiro colocado.

Entretanto, o item 6.1.6 do Edital dispõe expressamente:

"O lance deverá ser ofertado pelo valor do item."

Solicita-se esclarecer se a etapa competitiva será realizada pelo valor global do lote, em consonância com o critério de julgamento estabelecido no Edital, ou mediante lances individualizados por item.

Caso a disputa seja efetivamente realizada pelo valor global do lote, solicita-se a adequação da redação do item 6.1.6, de forma a eliminar eventual divergência interpretativa e assegurar que todos os licitantes adotem o mesmo procedimento durante a fase competitiva.

Nestes termos, solicita-se o esclarecimento dos pontos acima, bem como, quando aplicável, a retificação dos dispositivos indicados, de modo a assegurar interpretação uniforme das condições do certame, adequada formulação das propostas, neutralidade tecnológica, ampla competitividade e igualdade de condições entre os participantes.



RESPOSTA 1: CORRETO O ENTENDIMENTO, COM RESSALVAS

Não se exige a oferta cumulativa de duas arquiteturas de gerenciamento sobrepostas ou incompatíveis. Soluções baseadas em controladora dedicada (appliance físico ou virtual em cluster de alta disponibilidade - HA) que suportem nominalmente a capacidade estipulada (800 APs e 20.000 usuários) e garantam a continuidade operacional local dos APs em caso de desconexão (local bridge) atendem aos requisitos da DPRJ. A solução ofertada deve assegurar autonomamente a gerência, redundância e resiliência sem ponto único de falha.

RESPOSTA 2: ESCLARECIDO

O Termo de Referência não estabelece a exigência compulsória de apresentação da "matriz de aderência técnica" na fase de julgamento e aceitabilidade das propostas, estando a sua entrega formal regulamentada no item 4.2.1. e subitens, exclusivamente para a etapa de recebimento e avaliação da conformidade dos produtos.

Entretanto, esclarece-se que:

Análise de conformidade e diligência: na fase de julgamento das propostas, a verificação da conformidade técnica se pauta nos documentos apresentados pela licitante. Caso haja necessidade de esclarecer informações ou sanar dúvidas sobre as especificações do produto ofertado, o pregoeiro e a equipe técnica poderão promover diligências junto à arrematante, nos termos do art. 64 da Lei nº 14.133/2021.

Documentação comprobatória aceita: para a comprovação técnica dos requisitos, seja em eventual diligência no julgamento da proposta ou no momento do recebimento do objeto, serão aceitos não apenas os folhetos comerciais (datasheets), mas também manuais oficiais, guias de administração (administration guides), guias de funcionalidades (feature guides) e declarações técnicas formais emitidas pelo fabricante.

RESPOSTA 3: CORRETO O ENTENDIMENTO, COM RESSALVAS

A presente contratação se enquadra na modalidade de aquisição definitiva de ativos permanentes de TIC, na qual os bens e licenças se incorporam definitivamente ao patrimônio da Defensoria Pública. Por essa razão, ressaltamos a distinção entre dois conceitos fundamentais:

Licenciamento perpétuo (direito vitalício de uso): Trata-se do direito inalienável e por prazo indeterminado da Administração utilizar o hardware, as licenças e o software/firmware no estado em que se encontrarem. O direito de propriedade e de uso do bem adquirido pela DPRJ é vitalício. Garantia e suporte técnico (prazo de 60 meses): Refere-se ao dever do fabricante/contratada de

fornecer novos patches de software e suporte técnico, mas não poderá, sob qualquer hipótese, acarretar o bloqueio da solução (bricking), a perda do gerenciamento dos ativos, a limitação de recursos adquiridos ou a exigência de subscrições recorrentes para manter em funcionamento um bem que foi integralmente comprado e incorporado ao patrimônio público.

RESPOSTA 4: CORRETO O ENTENDIMENTO, COM RESSALVAS

A verificação do atendimento aos itens de segurança (WIDS/WIPS, DoS e ARP) se pauta pela capacidade efetiva da solução de identificar, mitigar ou neutralizar os vetores de ataque listados, sendo aceita a taxonomia e os controles comportamentais nativos do fabricante. Confirma-se o erro material no item 3.2.2.25., devendo ser lido "envio de pacotes de deauthentication" (ou mecanismos equivalentes de contenção) para interrupção de ataques.

RESPOSTA 5: CORRETO O ENTENDIMENTO

A validação e o envio de credenciais de acesso via e-mail atendem às especificações do portal de visitantes (captive portal). O fornecimento de gateways de mensageria SMS externos ou o custeio de pacotes de telefonia móvel de terceiros não integram o escopo do objeto licitado.

RESPOSTA 6: ESCLARECIDO

Esclarece-se que o limite máximo correto e aplicável à penalidade diária de 0,5% prevista na ocorrência nº 6 é de 20% (vinte por cento), constituindo a grafia "dois por cento" mero erro material de digitação.

RESPOSTA 7: Informamos que não assiste razão ao questionamento, não havendo qualquer divergência ou necessidade de alteração nas regras do certame.

Conforme estabelecido no Edital, no Termo de Referência e no Anexo II (Proposta Detalhe), o critério de julgamento adota o MENOR PREÇO POR LOTE, composto por 2 (dois) itens, sendo o valor máximo estimado por item o critério fixo de aceitabilidade das propostas.

Esclarece-se que a dinâmica da disputa operacional no sistema Compras.gov.br ocorrerá da seguinte forma:

- Envio de Lances: A etapa competitiva é realizada mediante o lançamento dos valores unitários de cada item que compõe o lote, exatamente como indicado no subitem 6.1.6 do Edital.
- Cálculo Automático do Lote: A partir dos valores unitários informados, o próprio sistema multiplica o valor ofertado pelas respectivas quantidades e calcula automaticamente o valor total do lote.
- Julgamento: A ordenação e a classificação dos licitantes na fase competitiva consideram o valor total do lote resultante do somatório dos itens, necessitando que os itens estejam dentro do valor estimado pela administração.

Cumpramos esclarecer, que iniciada a disputa, os valores estimados unitários, por item, serão disponibilizados no chat do sistema.

Desta forma, a exigência do subitem 6.1.6 alinha-se perfeitamente ao critério global do lote, garantindo a adequada formação de preços, a igualdade de condições entre os licitantes e a plena observância às regras do sistema eletrônico.

03/09/2026 17:06	 	Q1) Referência: Item 3.2.2.4 do Termo de Referência RESPOSTA Q1) CORRETO O ENTENDIMENTO	
02/09/2026 12:48	 	Q1) Referente a instalação da solução ofertada, entendemos que a instalação dos pontos de rede, RESPOSTA Q1: CORRETO O ENTENDIMENTO	
02/09/2026 12:13	 	QUESTIONAMENTO 01 - Referente ao faturamento dos itens de HARDWARE/ SOFTWARE, RESPOSTA QUESTIONAMENTO 01 -NÃO ACATADO	
02/09/2026 12:01	 	Q1) Referente ao item "3.2.2. CONTROLADORA WIRELESS, fornecida em formato de appliance físico Resposta ao Q1): CORRETO O ENTENDIMENTO	
02/09/2026 11:32	 	Questionamento 1: Resposta Questionamento 1: NÃO ACATADO	



Acesso à
Informação