MINISTÉRIO DA JUSTIÇA

COORDENAÇÃO-GERAL DE INFRAESTRUTURA, SERVIÇOS E OPERAÇÕES

NOTA TÉCNICA Nº 36/2026/CGISO/STI/SE/MJ

PROCESSO Nº 08006.000081/2026-47

INTERESSADO: STI

1. INTRODUÇÃO

1.1. Trata-se de resposta ao Pedido de Esclarecimento n.º 10 (37315234), que apresenta questionamentos acerca do Pregão Eletrônico 79/2026, que versa sobre a contratação de empresa especializada para aquisição de solução de infraestrutura de processamento para implantação de nuvem privada para atendimento das necessidades do Ministério da Justiça e Segurança Pública - MJSP, nos termos da Instrução Normativa SGD/ME n° 94, de 23 de dezembro de 2022.

1.2. O Pedido de Esclarecimento n.º 10 foi encaminhado por Daniel Burigo <daniel_burigo@lta-rh.com.br>, no dia 09 de outubro de 2026 às 16:24 GMT-3.

1.3. A Divisão de Licitações solicitou, através, do Despacho 199/2026/DILID/COLID/CGL/SAA/SE (37315252), a manifestação desta área demandante até às 09h do dia 14/10/2026, tendo em vista que será necessário inserção de comandos junto ao sistema de compras em tempo hábil.

1.4. Isto exposto passa-se à análise dos fatos.

2. RESPOSTA AO PEDIDO DE ESCLARECIMENTO N.º 10 (37315234)

2.1. O Pedido de Esclarecimento n.º 10 solicita elucidação sobre os seguintes questionamento apresentados a seguir:

> *"(...)*
>
> ***QUESTIONAMENTO 1 - item 7.14.1.1 do TR***
>
> *(...)*
>
> *O item 7.14.1.1 do Termo de Referência estabelece que o procedimento de comprovação dos requisitos técnicos "será realizado através da análise de documentos comprobatórios (datasheets e ou manuais), emitidos pelo fabricante do equipamento". Parte da documentação dos fabricantes, em especial a de sistemas operacionais de rede e a de componentes qualificados a partir de mais de um fornecedor, só é distribuída a clientes cadastrados no portal de suporte ou não detalha cada parâmetro separadamente. Diante disso, entendemos que, quando um parâmetro não constar de forma expressa em datasheet ou manual público, também serão aceitos: (a) declaração técnica do fabricante, em papel timbrado e assinada por seu representante, que identifique o modelo, o código do produto, a versão de software e o parâmetro atendido; e (b) cópia de documentação técnica oficial obtida no portal de suporte do fabricante, inclusive de acesso autenticado (guias, matrizes de compatibilidade, arquivos de MIB e modelos de dados), com indicação da origem. Os dois documentos ficam sujeitos a diligência. Está correto o nosso entendimento?*
>
> *(...)"*

2.2. **Resposta ao Questionamento 1**: Está correto o entendimento da licitante.

"(...)

QUESTIONAMENTO 2 - item 9.4.1.2 do Anexo I-A (sítios remotos)

(...)

O item 9.4.1.2 do Anexo I-A fixa para os sítios remotos, na severidade crítica, "primeiro retorno telefônico [...] em no máximo 4h (quatro horas)" e solução técnica, definitiva ou de contorno, em até 24 horas. As cinco penitenciárias federais (Brasília-DF, Catanduvas-PR, Campo Grande-MS, Porto Velho-RO e Mossoró-RN) ficam, em sua maioria, longe dos grandes centros e dos estoques de peças dos fabricantes. O próprio Termo de Referência reconhece essas condições: o item 4.5.5.3 menciona "deslocamento interestadual, controle de acesso a estabelecimentos prisionais de segurança máxima e agendamento prévio de entrada", e o item 4.10.1.2.5 condiciona o acesso dos técnicos à autorização da Secretaria Nacional de Políticas Penais. A duração dessas etapas não depende da CONTRATADA nem do fabricante. Além disso, cada unidade conta com dois servidores e dois switches (Itens 02 e 07), arquitetura redundante que tolera a falha de um componente sem interromper o serviço. Impor prazo rígido de solução nesses locais obrigaria a manter equipamentos sobressalentes em cada unidade, com aumento de preço e sem ganho proporcional de disponibilidade. Diante do exposto, entendemos que, nas penitenciárias federais, o atendimento presencial (on-site) e a solução que dele dependa serão prestados na modalidade de melhor esforço, mantidos nos prazos do edital a abertura de chamados em regime 24x7, o primeiro retorno, o diagnóstico, o suporte remoto e o envio das peças logo após o diagnóstico. Ressaltamos que este pedido se apoia em elementos que não foram examinados no Questionamento 05 do Pedido nº 08 (Nota Técnica nº 33/2026), em especial a dependência de autorização de acesso concedida pela própria Administração. Está correto o nosso entendimento?

(...)"

2.3. **Resposta ao Questionamento 2**: Não está correto o entendimento da licitante. Os níveis de serviço aplicáveis aos sítios remotos já foram diferenciados no item 9.4.1.2 do Anexo I-A e no item 4.5.5.2 do Termo de Referência. Essa diferenciação considerou as condições logísticas e de acesso descritas no item 4.5.5.3. Não será adotada a modalidade de melhor esforço. Registra-se, entretanto, que o período de espera exclusivamente decorrente da autorização de acesso aos estabelecimentos prisionais, quando concedida pela Administração, não será imputado à CONTRATADA. Para isso, a CONTRATADA deverá comprovar que solicitou o acesso tempestivamente e que não deu causa ao atraso, mediante registro no chamado e aceite da fiscalização do contrato.

"(...)

QUESTIONAMENTO 3 - item 8.1.3 do Anexo I-A (Itens 06, 07 e 08)

(...)

O item 8.1.3 do Anexo I-A exige "licenças perpétuas para o licenciamento de base do equipamento", e o item 8.1.2 exige que as licenças permaneçam "ativas e válidas durante todo o período do contrato", por no mínimo 60 meses contados da ativação. Diversos fabricantes de switches que constam do catálogo Azure Local, referenciado no item 5.1.6, comercializam o sistema operacional de rede por subscrição. Assim, entendemos que o requisito resta atendido pelo sistema operacional de rede do fabricante licenciado por subscrição de, no mínimo, 60 meses contados da ativação, que cobre todo o período contratual e de garantia, com direito de uso de todas as funcionalidades exigidas, suporte, correções e novas versões, sem custo adicional ao MJSP. Nosso entendimento está correto?

(...)"

2.4. **Resposta ao Questionamento 3**: Não está correto o entendimento da licitante. O item 8.1.3 do Anexo I-A exige licenças perpétuas para o licenciamento de base dos equipamentos dos Itens 06, 07 e 08. O objetivo é assegurar a continuidade operacional dos ativos de rede após o encerramento da vigência contratual. Licença por subscrição, ainda que vigente durante todo o contrato, não atende a essa finalidade. Mantém-se a exigência.

"(...)

QUESTIONAMENTO 4 - itens 2.1.1.7, 3.1.1.7 e 4.1.1.7 do Anexo I-A

(...)

Os itens 2.1.1.7, 3.1.1.7 e 4.1.1.7 do Anexo I-A exigem "projeto tool-less, ou seja, não necessita de ferramentas para abertura do gabinete e instalação/desinstalação de placas de expansão". Entendemos que atende ao requisito o servidor cuja tampa se abre por trava de liberação manual e cujas placas de expansão e risers são instalados e removidos por travas, sem ferramentas, inclusive quando a tampa dispõe de dispositivo opcional de travamento de segurança, fornecido destravado. Esse dispositivo protege o equipamento contra abertura indevida, o que é desejável em datacenter e em unidades prisionais, e não impede a abertura do gabinete nem a manutenção sem ferramentas. Está correto o nosso entendimento?

(...)"

2.5. **Resposta ao Questionamento 4**: Está correto o entendimento da licitante.

"(...)

QUESTIONAMENTO 5 - itens 2.1.16.1, 3.1.15.1 e 4.1.15.1 do Anexo I-A

(...)

Os itens 2.1.16.1, 3.1.15.1 e 4.1.15.1 do Anexo I-A exigem "certificação de conformidade com a norma IEC 62368-1, Energy Star, RoHS e Inmetro, ou documentação técnica equivalente que comprove o atendimento aos mesmos requisitos, emitida por organismo acreditado e reconhecido internacionalmente". Entendemos que o requisito fica atendido com a apresentação de: (a) certificado do esquema CB (IECEE) para a norma IEC 62368-1, emitido por organismo de certificação acreditado, e/ou Declaração de Conformidade do fabricante com as normas IEC 62368-1 e IEC 63000 (RoHS), referentes ao modelo regulatório do servidor; e (b) registro do modelo na base oficial do programa ENERGY STAR. Como não há programa compulsório de avaliação da conformidade do Inmetro para servidores de rack, entendemos também que esses documentos suprem a exigência relativa ao Inmetro. Está correto o nosso entendimento?

(...)"

2.6. **Resposta ao Questionamento 5**: Está correto o entendimento da licitante.

"(...)

QUESTIONAMENTO 6 - itens 2.1.13.32, 3.1.12.32 e 4.1.12.32 do Anexo I-A

(...)

Os itens 2.1.13.32, 3.1.12.32 e 4.1.12.32 do Anexo I-A exigem que "a interface de gerência do servidor deve permitir a criação de grupos de modo a permitir o gerenciamento de outros servidores a partir de um único IP sem a necessidade de softwares adicionais". Na geração atual de controladoras de gerenciamento, os fabricantes de servidores passaram a concentrar a gestão de grupos de equipamentos em consoles centralizados próprios. Entendemos, portanto, que o requisito resta atendido pelo console de gerenciamento do fabricante dos servidores, fornecido como appliance virtual sem custo adicional ao MJSP, no qual os servidores são agrupados e gerenciados a partir de um único endereço IP. Esse console faz parte do conjunto de hardware e software de gerência já exigido nos itens 2.1.13.1 e 2.1.13.2 (gerenciamento 1:1 e 1:N) e correspondentes dos Itens 02 e 03, e por isso não constitui software adicional. Nosso entendimento está correto?

(...)"

2.7. **Resposta ao Questionamento 6**: Está correto o entendimento da licitante.

"(...)

QUESTIONAMENTO 7 - itens 5.2.6 a 5.2.8, 6.2.5 e 6.2.6 do Anexo I-A

(...)

Os itens 5.2.6 a 5.2.8, 6.2.5 e 6.2.6 do Anexo I-A exigem suporte a transceivers SFP28, QSFP+ e QSFP28 nos padrões de alcance curto, longo e estendido (SR, LR e ER). Nas respostas aos Questionamentos 8 e 9 do Pedido nº 09 (Nota Técnica nº 35/2026), essa Administração esclareceu que tais itens tratam de compatibilidade e não obrigam o fornecimento de cada padrão. Assim, entendemos que o requisito é atendido pela plataforma que suporte as respectivas interfaces e os módulos homologados pelo fabricante para cada faixa de alcance. Entendemos também que, para 100 Gbps em alcance estendido, é admitido o módulo 100G ER4-lite (até 40 km com FEC), funcionalmente equivalente ao

100GBase-ER4, e que o suporte poderá ser comprovado por documentação ou declaração do fabricante (Questionamento 01). Nosso entendimento está correto?

(...)"

2.8. **Resposta ao Questionamento 7**: Está correto o entendimento da licitante.

"(...)

QUESTIONAMENTO 8 - itens 5.3.18 e 6.3.18 do Anexo I-A

(...)

Em atenção aos itens 5.3.18 e 6.3.18 do Anexo I-A, que exigem "a implementação da função de DHCP Server, capaz de suportar, pelos menos, a atribuição de endereço IPv4", entendemos que o requisito resta atendido pela função de DHCP Relay por VLAN para IPv4 e IPv6 (itens 5.3.19 e 6.3.19), associada ao DHCP Snooping, com as requisições encaminhadas ao serviço DHCP corporativo do MJSP. A atribuição automática de endereços IPv4, objetivo do requisito, continua garantida, com a vantagem de manter o endereçamento sob gestão única, sem servidores DHCP espalhados pelos switches. Além disso, entre os requisitos que a Microsoft define para switches de ambientes Azure Local, a única função de DHCP prevista é o DHCP Relay Agent. Está correto o nosso entendimento?

(...)"

2.9. **Resposta ao Questionamento 8**: Está correto o entendimento da licitante.

QUESTIONAMENTO 9 - itens 5.3.46 e 6.3.48 do Anexo I-A

(...)

Em atenção aos itens 5.3.46 e 6.3.48 do Anexo I-A, que exigem "ACLs baseadas em políticas (Policy Based ACLs), que permitem aplicar políticas de controle de acesso em grupos de objetos", entendemos que atende ao requisito a estrutura de classificadores e políticas (classifier/policy) do sistema operacional ofertado. Nela, o classificador, definido por lista de acesso ou por campos de cabeçalho, agrupa vários critérios de correspondência (endereços, prefixos, portas, protocolos e VLANs), e a política associada aplica as ações de controle de acesso ao grupo inteiro, nas interfaces, nas VLANs ou globalmente. O resultado é o mesmo das listas por grupos de objetos: o conjunto de objetos é definido uma única vez e recebe a política, qualquer que seja a nomenclatura adotada pelo fabricante. Nosso entendimento está correto?

(...)"

2.10. **Resposta ao Questionamento 9**: Está correto o entendimento da licitante.

"(...)

QUESTIONAMENTO 10 - item 5.3.45 do Anexo I-A

(...)

Em atenção ao item 5.3.45 do Anexo I-A, que exige "a configuração de, no mínimo, 2.000 (duas mil) ACLs", entendemos que o quantitativo se refere ao total de entradas de controle de acesso suportadas pelo equipamento, somadas as tabelas aplicáveis (IPv4, IPv6 e MAC, na entrada e na saída) e as políticas de classificação e de encaminhamento baseadas em listas de acesso, e não ao número de regras de uma única lista. Nos switches, essa capacidade fica distribuída em tabelas de hardware (TCAM) separadas por tipo de tráfego e por sentido, de modo que a capacidade do equipamento corresponde à soma delas. Está correto o nosso entendimento?

(...)"

2.11. **Resposta ao Questionamento 10**: Está correto o entendimento da licitante.

"(...)

QUESTIONAMENTO 11 - item 6.2.7 do Anexo I-A

(...)

O item 6.2.7 do Anexo I-A exige o fornecimento dos patch cords correspondentes à interface óptica ofertada, e a resposta ao Questionamento 9 do Pedido nº 09 (Nota Técnica nº 35/2026) incluiu no fornecimento a conectividade de uplink nas unidades remotas. Para

dimensionar esse fornecimento, solicitamos informar, para cada penitenciária federal, o fabricante do equipamento da rede local ao qual os switches do Item 07 serão conectados, o tipo e a velocidade da porta (SFP+, SFP28 ou QSFP28), o tipo de fibra e a distância aproximada do enlace. Caso essas informações não sejam disponibilizadas, entendemos que o requisito restará atendido com 2 (dois) enlaces de uplink em fibra multimodo por switch, compostos de transceptores do fabricante do switch na velocidade da porta remota, transceptores compatíveis com o equipamento remoto e patch cords no comprimento apurado na vistoria, sem ônus ao MJSP. Nosso entendimento está correto?

(...)"

2.12. **Resposta ao Questionamento 11**: Está correto o entendimento da licitante.

"(...)

QUESTIONAMENTO 12 - item 7.4.10 do Anexo I-A

(...)

Em atenção ao item 7.4.10 do Anexo I-A, que exige "mecanismos de proteção contra ataques do tipo 'ARP Poisoning'", entendemos que o requisito resta atendido pelo conjunto de mecanismos da versão ofertada: DHCP Snooping com tabela de vínculos e portas confiáveis, segurança de porta (port security) com limite de endereços MAC e fixação dos endereços aprendidos (sticky MAC), ACLs de camadas 2 e 3 e proteção do plano de controle (Control Plane Policing) com limitação de taxa. Juntos, esses mecanismos protegem a rede contra o envenenamento de ARP, pois restringem os endereços admitidos em cada porta e limitam o tráfego ARP enviado ao plano de controle. Conjunto semelhante foi acolhido na resposta ao Questionamento 17 do Pedido nº 08 (Nota Técnica nº 33/2026) para os mecanismos anti-spoofing. Está correto o nosso entendimento?

(...)"

2.13. **Resposta ao Questionamento 12**: Não está correto o entendimento da licitante. O item 7.4.10 exige mecanismo específico de proteção contra ARP Poisoning. Os mecanismos indicados restringem endereços MAC por porta e limitam a taxa de tráfego ao plano de controle, mas não validam o conteúdo dos pacotes ARP. Por isso, não impedem que um host autorizado anuncie associação falsa entre endereço IP e endereço MAC. O requisito será considerado atendido por inspeção dinâmica de ARP (*Dynamic ARP Inspection*) ou mecanismo equivalente que valide os pacotes ARP com base na tabela de vínculos do DHCP Snooping ou em associações configuradas estaticamente. A resposta ao Questionamento 17 do Pedido nº 08 tratou de requisito diferente, que admitia expressamente alternativas de filtragem anti-*spoofing*. Por isso, não se aplica por analogia ao presente caso.

"(...)

QUESTIONAMENTO 13 - item 7.2.3.3 do Anexo I-A

(...)

O item 7.2.3 do Anexo I-A exige que as portas de acesso suportem conexões a 1000 Mbps em full-duplex, a 100 Mbps em full-duplex e, no subitem 7.2.3.3, a "100 Mbps e half-duplex". Entendemos que a finalidade do subitem, que é permitir a conexão de dispositivos de 100 Mbps, é atendida por portas 10/100/1000BASE-T com autonegociação conforme a norma IEEE 802.3, que estabelecem enlaces de 100 Mbps em full-duplex com esses dispositivos, sem que a operação em half-duplex seja determinante para a aceitação. Os equipamentos que serão ligados ao switch de gerência, como as controladoras de gerenciamento dos servidores, operam em full-duplex, e o half-duplex é um modo legado, sujeito a colisões e sem aplicação em redes comutadas de datacenter. Nosso entendimento está correto?

(...)"

2.14. **Resposta ao Questionamento 13**: Está correto o entendimento da licitante.

"(...)

QUESTIONAMENTO 14 - itens 7.5.1 e 7.5.2 do Anexo I-A

(...)

Em atenção ao item 7.5.1 do Anexo I-A, que exige "agente de gerenciamento SNMP (RFC 1157)", e ao item 7.5.2, que exige "SNMP v1, v2 e v3", entendemos que o requisito resta atendido pelo agente SNMP nas versões SNMPv2c e SNMPv3, com MIB-II (RFC 1213) e

Bridge MIB, sem que o suporte ao SNMPv1 seja determinante para a aceitação. O SNMPv2c sucedeu o SNMPv1 e mantém o mesmo modelo de comunidades e o acesso às mesmas MIBs. Já o SNMPv1 não tem autenticação nem criptografia, recursos presentes no SNMPv3, e é desaconselhado pelas boas práticas de segurança. Em situação semelhante, a resposta ao Questionamento 13 do Pedido nº 08 (Nota Técnica nº 33/2026) acolheu a dispensa do Telnet por se tratar de protocolo sem cifragem. Está correto o nosso entendimento?

(...)"

2.15. **Resposta ao Questionamento 14**: Está correto o entendimento da licitante.

"(...)

QUESTIONAMENTO 15 - itens 7.4.4.1, 7.4.5.1 e 7.4.9.1 do Anexo I-A

(...)

Os itens 7.4.4.1 e 7.4.5.1 do Anexo I-A exigem o envio de "trap SNMP" em caso de violação da segurança de porta, e o item 7.4.9.1 exige, quando os limiares de broadcast, multicast e unicast da porta forem excedidos, "enviar um trap SNMP e desabilitar a porta". Entendemos que a notificação resta atendida por eventos enviados via syslog ao sistema de monitoramento, mantidas as ações locais de contenção do equipamento: bloqueio dos endereços não autorizados ou desativação da porta, no caso da segurança de porta, e contenção do tráfego excedente na própria porta, no caso dos limiares. O próprio item 7.5.13 admite "telemetria, syslog, SNMP ou funcionalidades equivalentes do fabricante" como meios de monitoramento e geração de eventos, e os sistemas de monitoramento tratam eventos de syslog da mesma forma que traps SNMP. Nosso entendimento está correto?

(...)"

2.16. **Resposta ao Questionamento 15**: Está correto o entendimento da licitante.

"(...)

QUESTIONAMENTO 16 - item 7.5.16 do Anexo I-A

(...)

Em atenção ao item 7.5.16 do Anexo I-A, que exige "o espelhamento de uma VLAN", entendemos que o requisito é atendido por sessão de espelhamento local (SPAN) ou para destino IP remoto (ERSPAN) que tenha como origem, no sentido de entrada, as portas e agregações de enlace (port-channels) membros da VLAN. Em um switch de acesso, todo o tráfego da VLAN entra por essas portas, de modo que o resultado é equivalente ao da seleção da VLAN como origem. Está correto o nosso entendimento?

(...)"

2.17. **Resposta ao Questionamento 16**: Está correto o entendimento da licitante.

3. **CONCLUSÃO**

3.1. Diante do exposto, submete-se o presente processo à Divisão de Licitações, para providências cabíveis e prosseguimento do processo de contratação.

Documento assinado eletronicamente por **Rodrigo Albernaz Bezerra**, **Integrante Requisitante**, em 13/10/2026, às 17:49, com fundamento no § 3º do art. 4º do Decreto nº 10.543, de 13 de novembro de 2020.

A autenticidade do documento pode ser conferida no site http://sei.autentica.mj.gov.br informando o código verificador **37315886** e o código CRC **EDBDE636**
O documento pode ser acompanhado pelo site http://sei.consulta.mj.gov.br/ e tem validade de prova de registro de protocolo no Ministério da Justiça e Segurança Pública.