GOVERNO DO ESTADO DE RONDÔNIA
Superintendência Estadual de Compras e Licitações - SUPEL
Comissão Especial de Licitações - SUPEL-COESP

RESPOSTA

DO PEDIDO DE IMPUGNAÇÃO

PROCESSO N.º 0029.064405/2024-33

PREGÃO ELETRÔNICO N.º 90220/2025/SUPEL/RO.

OBJETO: Registro de Preços para futura e eventual contratação de outros serviços de terceiros - empresa especializada em serviços de solução tecnológica com fornecimento de plataforma de segurança e Licença de Uso, por prazo determinado abrangendo instalação, subscrição, emissão de Termo de Licenciamento, gerenciamento de chave de criptografia e treinamento, tendo vista atender a Secretaria de Estado da Educação - SEDUC/RO.

A Superintendência Estadual de Compras e Licitações – SUPEL, através de sua Pregoeira, designada por força das disposições contidas na Portaria n.° 317 de 02 de dezembro de 2025, publicada no Diário Oficial do Estado de Rondônia do dia 03/12/2025, torna público aos interessados, em especial as empresas que retiraram o instrumento convocatório, os seguintes questionamentos e respostas referente ao Pedido de Impugnação da empresa interessada na participação do certame, os documentos estão disponíveis para consulta no site www.rondonia.ro.gov.br/supel:

I. DAS PRELIMINARES

Em sede de admissibilidade, verificou-se que foram preenchidos os pressupostos de legitimidade, interesse processual, fundamentação e tempestividade (nos termos do Decreto Estadual 28.874/2024, e do item 7 do Edital, conforme comprovam os documentos colacionados ao processo administrativo SEI relacionado a este **PREGÃO ELETRÔNICO N.° 90220/2025/SUPEL**, pelo que passo formulação da resposta ao Pedido de Impugnação.

II. DA SÍNTESE DO PEDIDO DE IMPUGNAÇÃO:

QUESTIONAMENTO - EMPRESA A Id. (68809790):

(...)

SENHOR (A) PREGOEIRO (A).

Edital de Pregão Eletrônico nº 90220/2025/SUPEL/ RO

DATASYNQ CONSULTORIA E TECNOLOGIA LTDA, CNPJ: 61.138.515/0001-47, devidamente qualificada, vem, por seu representante, apresentar IMPUGNAÇÃO ao edital, nos termos a seguir expostos.

I. DO CABIMENTO

A empresa recorrente apresenta a presente impugnação tempestivamente, com esteio no art. 164 da Lei nº 14.133/2021, em face do edital publicado no dia 22/01/2026. A medida visa a correção de vícios insanáveis que comprometem a busca pela proposta mais vantajosa e o atendimento ao interesse público.

II. RAZÕES DA IMPUGNAÇÃO

O presente Pregão Eletrônico tem por objeto a contratação, por meio de Registro de Preços, de plataforma de segurança de dados, abrangendo licenças de uso, agentes especializados, gerenciamento de chaves criptográficas, serviços de implantação e treinamento, destinada à Secretaria de Estado da Educação de Rondônia, com valor estimado global de R$ 29.688.131,50.

Todavia, a análise técnica do Termo de Referência e do modelo de contratação adotado evidencia graves inconsistências de proporcionalidade, razoabilidade e competitividade, conforme se expõe a seguir.

O edital projeta uma contratação de quase R$ 30 milhões, contemplando, entre outros itens:

• 4 consoles de gerenciamento centralizado em alta disponibilidade

• 12 agentes de proteção de servidores;

• 8 agentes de proteção de dados para aplicações;

• 10 agentes de gestão de chaves criptográficas locais;

• Subscrição de classificação e descoberta de dados com franquia de 50 TB, replicada em ambiente de produção (PRM) e contingência (DR);

• Arquitetura completa de criptografia e gestão centralizada de chaves, típica de ambientes bancários, financeiros ou de defesa.

Esse conjunto técnico extrapola, de forma significativa, a necessidade operacional de uma secretaria finalística de educação, cujo foco institucional é a gestão educacional, e não a custódia de dados estratégicos de Estado, sigilos militares ou informações financeiras sensíveis de alto risco sistêmico.

Além disso, o agrupamento em lote único impede o adequado dimensionamento da verba pública, pois força a Administração a contratar todos os componentes no maior patamar possível, ainda que partes do escopo não sejam necessárias na mesma proporção ou no mesmo momento.

Se o objeto fosse dividido por itens, seria possível:

• Ajustar quantitativos por módulo conforme a real demanda;

• Priorizar investimentos onde há maior risco;

• Reduzir significativamente o custo global, preservando a efetividade da proteção.

Neste sentido, cumpre pormenorizar as ilegalidades contidas nos instrumentos licitatórios ora impugnados.

III. DA RESTRIÇÃO À COMPETITIVIDADE PELA IMPOSSIBILIDADE DE ADIÇÃO DE SOLUÇÕES CONSOLIDADAS DE MERCADO

Caso o objeto não estivesse indevidamente agrupado em lote único, seria plenamente possível à Administração Pública avaliar e contratar soluções amplamente consolidadas no mercado, por item ou módulo, cada qual especializada em sua respectiva função, tais como:

a) Proteção de dados, DLP e classificação de informações

• Forcepoint – DLP, classificação e proteção de dados sensíveis;

• Microsoft – Microsoft Purview (classificação, rotulagem e DLP);

• Broadcom (linha Symantec) – DLP e Information Security;

• Digital Guardian – proteção e monitoramento de dados sensíveis.

b) Descoberta, visibilidade e avaliação de riscos

• Tenable – visibilidade de ativos e exposição a riscos;

• Rapid7 – descoberta, avaliação de risco e governança;

• Qualys – inventário, visibilidade e compliance.

c) Criptografia e gestão de chaves

• Entrust – HSM, criptografia e gestão de chaves;

• Fortanix – gestão centralizada de chaves;

• HashiCorp – Vault para segredos e chaves;

• Utimaco – HSM e key management.

Todavia, o agrupamento compulsório de todos esses componentes em um único lote, com exigência de integração nativa e proprietária, inviabiliza a participação desses fornecedores, ainda que plenamente capacitados para atender partes relevantes da demanda.

Ademais, da forma como previsto, o instrumento configura violação ao princípio do parcelamento. O art. 40, V, “b”, da Lei nº 14.133/2021 estabelece o parcelamento como regra, visando a ampla competitividade e a economia de escala, de modo a obrigar a divisão do objeto quando técnica e economicamente viável. Neste sentido, inclusive, a Súmula 247 do TCU.

Ao aglutinar licenças, agentes, criptografia e serviços em um único lote, o edital ergue barreiras de entrada para empresas especialistas (best of-breed), restringindo o certame a poucos players globais que detêm plataformas "tudo-em-um", em detrimento de soluções mais eficientes e baratas se contratadas modularmente.

Tal prática viola o art. 9º, I, “a”, da Lei 14.133/2021, que veda condutas que restrinjam a concorrência, na medida em que o agrupamento, da forma como previsto, gera dependência tecnológica e fere a competitividade.

IV. DA AUSÊNCIA DE JUSTIFICATIVA TÉCNICA PARA A “PLATAFORMA ÚNICA POR INTEGRAÇÃO”

A alegação de que a integração exige uma plataforma única não se sustenta à luz das melhores práticas de cibersegurança. O estado da arte recomenda arquiteturas em camadas (defense in depth) e estratégia best-of breed, nas quais:

• Quanto maior a diversidade controlada de plataformas, maior a resiliência contra falhas sistêmicas, vulnerabilidades exploráveis em cadeia e dependência tecnológica;

• Soluções especializadas por função tendem a oferecer maior maturidade técnica do que plataformas genéricas “tudo-em-um”;

• A integração entre ferramentas é prática comum, realizada por APIs, conectores, padrões abertos, SIEM, SOAR e barramentos de eventos.

Grandes órgãos públicos e privados utilizam múltiplas plataformas de segurança, de fabricantes distintos, todas integradas entre si, justamente para reduzir risco, evitar lock-in e ampliar a proteção. A adoção de plataforma única não é requisito de integração, mas opção de modelo, que deve ser tecnicamente justificada, o que não ocorre no presente edital.

Portanto, a justificativa de integração em plataforma única é tecnicamente falha e juridicamente órfã, sendo vedada também a indicação de característica exclusiva, salvo se devidamente justificada, que possa gerar 4 qualquer direcionamento da contratação, a exemplo da exigência de integração nativa de fábrica.

V. COMPARAÇÃO TÉCNICA COM OUTROS ÓRGÃOS DE MAIOR CRITICIDADE INSTITUCIONAL

Chama especial atenção que órgãos com missão institucional mais sensível e maior maturidade em segurança da informação não adotaram solução única, fechada e de custo equivalente.

Como referência:

• Tribunal de Contas do Estado de Rondônia

• Tribunal de Justiça de Rondônia

Mesmo lidando com processos sigilosos, dados financeiros e informações estratégicas, optaram por contratações modulares, separando proteção de dados, criptografia, gestão de chaves, classificação de informações e serviços especializados — ampliando a concorrência e reduzindo custos, diferentemente do modelo adotado pela SEDUC/RO.

A experiência de outros órgãos de controle e cúpula (TCE/RO e TJ/RO), que optaram pelo modelo modular, serve como prova de que a viabilidade técnica do fracionamento não só é possível, como é a prática que garante a seleção da proposta mais vantajosa.

VI. DIRECIONAMENTO PARA SOLUÇÃO PROPRIETÁRIA DE FABRICANTE ESPECÍFICO

O detalhamento técnico do edital — especialmente a integração obrigatória, proprietária e indivisível em lote único — direciona a contratação para solução de fabricante específico, notadamente associada à Thales.

Tal modelagem:

• Exclui fabricantes consolidados listados acima;

• Impede soluções interoperáveis e modulares;

• Reduz drasticamente a competitividade.

VII. PEDIDOS Verifica-se que o edital:

• Prevê valor elevado (R$ 29,6 milhões) sem dimensionamento proporcional por item;

• Adota arquitetura incompatível com a realidade institucional da SEDUC/RO;

• Sustenta justificativa técnica frágil ao impor plataforma única sob o argumento de integração;

• Direciona a contratação e exclui amplo conjunto de fabricantes aptos;

• Diverge das melhores práticas e das experiências de órgãos de maior criticidade.

Diante da manifesta ilegalidade por ausência de parcelamento, direcionamento de solução e desproporcionalidade técnica, requer-se:

1. O acolhimento da presente impugnação para suspender o certame;

2. A retificação do Termo de Referência para fracionar o objeto em itens ou lotes independentes, conforme o art. 40 da Lei nº 14.133/2021, permitindo melhor dimensionamento da verba pública, ampla competitividade e a obtenção da proposta mais vantajosa para a Administração.

3. A revisão do Estudo Técnico Preliminar para adequar os quantitativos à real necessidade institucional da SEDUC/RO, sob pena de nulidade por falta de motivação.

P. Deferimento

Brasília, DF, 02 de fevereiro de 2026.

SAMMUEL AUGUSTO GOMES MACHADO

Representante Legal

(...)

MANIFESTAÇÃO da SEDUC-GCS - Análise do Pedido de Esclarecimento (68866805)

(...)

Resposta
MANIFESTACAO TECNICA

Resposta a Impugnação ao Edital de Pregão Eletrônico no 90220/2025/SUPEL/RO

Analise Tecnica das Alegações Apresentadas pela DATASYNQ CONSULTORIA E TECNOLOGIA LTDA

1. EXPOSIÇÃO PREAMBULAR

O presente parecer técnico tem por objetivo apresentar manifestação fundamentada que trata de resposta a impugnação apresentada pela empresa DATASYNQ CONSULTORIA E TECNOLOGIA LTDA ao Edital de Pregão Eletrônico no 90220/2025/SUPEL/RO, cujo objeto é a contratação de Plataforma de Segurança de Dados para a Secretaria de Estado da Educação de Rondônia.

A presente manifestação demonstra, com fundamento e alicerce legal na lei 14.133:21, nas justificativas já apresentadas no termo de referência e em seu estudo técnico preliminar, bem como com base nas definições técnicas de institutos de pesquisa independentes, que as soluções citadas pela impugnante **possuem finalidades técnicas distintas** do objeto licitado, constituindo categorias de produtos independentes com propósitos próprios, **não sendo, portanto, compatíveis nem substitutas ao que se pretende contratar, bem como que sua proposição e contestação em relação ao tema parcelamento do objeto, não encontra amparo, haja vista as justificativas que serão sobejamente ratificadas por meio do presente parecer.**

2. DEFINICAO TECNICA DE PLATAFORMA DE SEGURANCA DE DADOS

Antes de adentrarmos ao aspecto da justificativa, importante contextualizar para a impugnante o conceito de Plataforma Integrada de Segurança. Veja, o instituto de pesquisa Gartner, referência mundial em análise de tecnologia da informação, define no documento Market Guide for Data Security Platforms (Marco 2025) que: *"Data security platforms combine data security controls with business logic and fine-grained authorization, producing significant gains in efficacy and structured data security."* que uma Plataforma de Segurança de Dados (DSP) constitui **solução unificada** que integra nativamente os seguintes componentes tecnicos:

a) Descoberta e classificação automatizada de dados sensíveis em repositórios estruturados e não estruturados, permitindo identificar onde residem informações que requerem proteção.

b) Proteção de dados por meio de técnicas criptografias (criptografia, tokenização,

mascaramento dinâmico), aplicadas de forma integrada aos dados identificados.

c) Gerenciamento centralizado do ciclo de vida de chaves criptográficas(geração, armazenamento, rotação, revogação e destruição).

d) Controles de acesso granulares e gestão unificada de políticas de segurança, permitindo definir, aplicar e auditar regras de proteção a partir de console único.

Não obstante, o Forrester, outro instituto de pesquisa independente, corrobora esta definição de plataforma de segurança por meio do relatório The Forrester Wave: Data Security Platforms, Q1 2025, avaliando fornecedores com base em 23 critérios que abrangem as funcionalidades acima descritas.

Fontes: *Gartner, Market Guide for Data Security Platforms, Marco 2025; Forrester, The Forrester Wave: Data Security Platforms, Q1 2025.*

3. ANÁLISE DAS SOLUCOES CITADAS NA IMPUGNACAO

Após criteriosa análise realizada nos argumentos apresentados, verifica-se que a impugnante relaciona diversas soluções como supostamente equivalentes ao objeto licitado. Conforme demonstrado a seguir, tais soluções possuem **finalidades técnicas próprios e especificas**, constituindo categorias de produtos independentes, distintas da finalidade de uma Plataforma de Segurança de Dados e portanto, não sendo capazes de atender ao presente projeto.

3.1 Soluções de DLP (Data Loss Prevention)

As soluções de DLP (Data Loss Prevention), tais como Forcepoint DLP, Microsoft Purview DLP, Broadcom/Symantec DLP e Digital Guardian, possuem finalidade tecnica especifica e bem definida: **monitorar e controlar o fluxo de informações para verificar se os dados estão sendo utilizados de maneira adequada e em conformidade com as politicas organizacionais**.

O proposito fundamental de uma solução DLP e atuar como mecanismo de *vigilância e governança sobre o uso dos dados*. Estas ferramentas monitoram continuamente as ações dos usuários e sistemas, identificando e prevenindo situações em que dados possam estar sendo transmitidos, copiados, impressos ou acessados de forma inadequada ou em desacordo com as regras estabelecidas pela organização.

Os canais tipicamente monitorados por soluções DLP incluem: correio eletrônico (verificando anexos e conteúdo de mensagens), navegação web (controlando uploads para sites e serviços de nuvem), dispositivos removíveis (como pendrives e HDs externos), impressoras, área de transferência e aplicativos de mensagens. O DLP atua como um *"guardiao de comportamento"*, alertando ou bloqueando quando detecta acoes que violam as politicas de uso definidas.

Esta finalidade e **intrinsecamente distinta** da finalidade de uma Plataforma Integrada de Segurança de Dados. Enquanto o DLP monitora *como* os dados estão sendo utilizados e *se* estão sendo manipulados corretamente, a Plataforma de Segurança de Dados protege *o conteúdo em si* dos dados por meio de descoberta, classificação, criptografia e gestão de chaves, tornando-os ininteligíveis mesmo em caso de acesso não autorizado.

Trata-se, portanto, de soluções com propósitos próprios e independentes. Uma organização pode legitimamente necessitar de ambas as categorias de soluções para atender a diferentes requisitos de segurança, sem que uma substitua a outra. Cada categoria atende a um objetivo específico dentro da estratégia de segurança da informação.

Conclusao: As soluções de DLP citadas pela impugnante (Forcepoint, Microsoft Purview, Broadcom/Symantec e Digital Guardian) possuem finalidade tecnica propria, voltada ao monitoramento e controle do uso adequado dos dados. Esta finalidade constitui categoria de produto independente, que não guarda equivalência com o objeto licitado (proteção dos dados por meio de descoberta, classificação, criptografia e gestão de chaves) integrada a uma plataforma única de segurança.

3.2 Soluções de Gestão de Vulnerabilidades

As soluções Tenable, Rapid7 e Qualys sao classificadas pelo mercado como ferramentas de **Gestao de Vulnerabilidades (Vulnerability Management)**. Conforme a documenta Cao oficial da Tenable: *"Vulnerability management consists of technologies, tools, policies and procedures to identify, prioritize and fix security weaknesses across your organization. Its ultimate objective is to systematically reduce the overall attack surface."*

O proposito técnico destas soluções e **identificar falhas e fraquezas em sistemas, redes, aplicações e configurações**, tais como patches ausentes, configurações inseguras e vulnerabilidades conhecidas catalogadas em bases como CVE (Common Vulnerabilities and Exposures). Estas ferramentas permitem que a equipe de TI priorize e execute correções para reduzir a superfície de ataque da infraestrutura.

Trata-se de finalidade **completamente distinta** da proteção de dados sensíveis. Enquanto a Gestão

de Vulnerabilidades atua sobre a *infraestrutura de TI* (sistemas operacionais, aplicações, equipamentos de rede, servidores), a Plataforma de Segurança de Dados atua sobre os *dados de negocio* (informações pessoais de alunos, dados acadêmicos, informações administrativas da SEDUC).

Não há relação funcional entre as duas categorias de soluções. Uma ferramenta de gestão de vulnerabilidades não possui capacidade de descobrir dados sensíveis em bancos de dados, classifica-los conforme sua natureza, aplicar criptografia ou gerenciar chaves criptográficas, pois estas funcionalidades estão completamente fora de seu escopo de atuação.

Conclusao: As soluções de Gestão de Vulnerabilidades citadas pela impugnante (Tenable, Rapid7 e Qualys) possuem finalidade técnica própria, voltada a identificação de falhas em infraestrutura de TI. Esta finalidade constitui categoria de produto independente, que não guarda qualquer relação com o objeto licitado (proteção de dados sensíveis).

F o n t e : *Tenable, "Vulnerability Management Principles", 2025 (tenable.com/principles/vulnerability-management-principles).*

3.3 Solucoes de HSM (Hardware Security Module)

Os HSMs (Hardware Security Modules), tais como Entrust, Fortanix e Utimaco, são dispositivos de hardware dedicados a **custódia segura de chaves criptográficas**, oferecendo proteção física e logica para operações criptografias sensíveis.

Um HSM **representa um modulo especifico** dentro de uma arquitetura de segurança, com casos de uso próprios e bem definidos, tais como: infraestrutura de chaves publicas (PKI), assinatura digital de documentos, proteção de chaves mestras de criptografia, processamento seguro de transações financeiras e emissão de certificados digitais.

HSMs podem ser contratados separadamente quando o objetivo da contratação são estes casos de uso específicos. Organizações que necessitam exclusivamente de custodia de chaves para PKI, assinatura digital ou processamento de transações podem contratar HSMs de forma independente, pois estes casos de uso não demandam as demais funcionalidades de uma Plataforma de Segurança de Dados.

Porém, quando o objetivo e uma **Plataforma de Segurança de Dados**, objeto da presente licitação, que deve integrar nativamente descoberta, classificação, proteção e gestão de chaves em solução unificada, a mera contratação de HSMs nao atende aos requisitos, pois HSMs nao possuem as funcionalidades de descoberta de dados sensíveis, classificação automatizada ou aplicação de políticas de proteção integradas.

Conclusao: HSMs (Entrust, Fortanix, Utimaco) representam módulos com finalidade especifica (custodia de chaves), que podem ser contratados separadamente para casos de uso próprios. Quando o objetivo e uma Plataforma de Segurança de Dados integrada, HSMs isolados não atendem aos requisitos, por não possuírem as funcionalidades de descoberta e classificação que caracterizam o objeto licitado.

3.4 Soluções de Gestão de Secrets

Soluções como HashiCorp Vault sao projetadas para **gestao de secrets de infraestrutura**, tendo como finalidade principal a **autenticacao segura entre maquinas, sistemas e aplicacoes**.

Conforme a documentacao oficial da HashiCorp: *"Vault is a secrets management tool designed to securely store and tightly control access to sensitive data, such as API keys, passwords, certificates, and other critical information."* Complementarmente, a documentacao descreve os casos de uso: *"Static secrets management (key value pairs), Auto-rotating Secrets, Dynamic Secrets."*

O proposito técnico destas soluções e **permitir que aplicações e serviços se autentiquem de forma segura**, sem necessidade de armazenar credenciais em código-fonte ou arquivos de configuração. Trata-se de ferramenta voltada a comunicação segura entre componentes de infraestrutura, gerenciando credenciais como: senhas de conexão a bancos de dados, tokens de API, chaves SSH, certificados TLS e credenciais de serviços em nuvem.

Esta finalidade e **completamente distinta** da proteção de dados de negocio. Enquanto gestores de secrets protegem *credenciais utilizadas por sistemas para autenticação entre maquinas*, a Plataforma de Segurança de Dados protege *dados de negocio* (informacoes pessoais de alunos, dados acadêmicos, registros administrativos) por meio de descoberta, classificação e criptografia.

Soluções de gestão de Secrets podem ser contratadas separadamente quando o objetivo da contratacao e especificamente a autenticação segura de aplicações e serviços. Porém, quando o objetivo e uma Plataforma de Segurança de Dados, gestores de Secrets nao atendem aos requisitos, pois constituem categoria de produto com finalidade distinta.

Conclusão: Solucoes de gestao de Secrets (HashiCorp Vault) possuem finalidade técnica propria, voltada a autenticação segura entre maquinas e sistemas. Esta finalidade constitui categoria de

produto independente, que não guarda equivalencia com o objeto licitado (proteção de dados de negócio por meio de descoberta, classificação, criptografia e gestao de chaves).

Fonte: *HashiCorp Developer Portal (developer.hashicorp.com/vault/docs/what-is-vault); HCP Vault Secrets Documentation (developer.hashicorp.com/hcp/docs/vault-secrets).*

4. FUNDAMENTACAO TECNICA E SUSTENTAÇÃO LEGAL PARA SOLUCAO INTEGRADA E PARA O NÃO PARCELAMENTO DO OBJETO

Conforme exposto anteriormente, os principais institutos de pesquisa independentes do setor de tecnologia da informação recomendam a adoção de plataformas integradas de segurança, em contraposição a contratação fragmentada de ferramentas isoladas.

A fragmentação de ferramentas de segurança de dados acarreta riscos técnicos documentados: lacunas de visibilidade entre sistemas que não se comunicam; políticas conflitantes entre ferramentas distintas; dificuldade de auditoria e comprovação de conformidade; custos adicionais de integração e operação; e aumento da complexidade que pode comprometer a eficácia da proteção.

Isto posto, cumpre destacar que a decisão pelo não parcelamento do objeto em diferentes lotes, está devidamente fundamentada e alicerçada por meio do instrumento convocatório e seus anexos, mais precisamente por meio do subitem 4.2 do termo de referência, em que há justificativa clara sobre o tema.

Ademais, conforme devidamente fundamentado, não há razão que sustente seu parcelamento, haja vista os aspectos técnicos e requisitos que envolvem uma solução no campo da segurança da informação e segurança cibernética, caracterizada como uma Plataforma Integra de Segurança, também, considerando o grau de interação do conjunto de serviços técnicos descritos, natureza específica, caráter contínuo, aliada a alta criticidade e complexidade de todo o ambiente de TI de alta disponibilidade dessa administração, torna-se inviável tecnicamente o parcelamento do objeto pelas razões já expostas, bem como pelos pontos abaixo destacados:

a) é sabido que em uma eventual exposição de dados sigilosos, não será possível precisar de qual módulo se originou a falha, permitindo que as empresas transfiram a responsabilidade para terceiros, impedindo assim a penalização legal pelo fato ocorrido e a avaliação dos pontos de mitigação.

b) Potencialização de riscos inerentes a adequação à Lei Geral de Proteção de Dados (LGDP);

c) Perda de eficiência na gestão do contrato;

d) As licenças de software compõem uma plataforma integrada, existindo no mercado diversas empresas integradoras capazes de atender a globalidade do lote de maneira totalmente integrada e "indissociada";

e) A aquisição parcelada da solução trará riscos associados a transferência de responsabilidade em um evento de vazamento de dados, dificultando a tarefa de compreender qual empresa contratada ou solução não executou a contento suas responsabilidades;

f) Os serviços de treinamento, implementação e estabilização da solução são diretamente relacionados as licenças de software, razão pela qual a segmentação dos itens não encontra amparo seja do ponto de vista técnico, seja do ponto de vista de eficiência contratual, uma vez que uma empresa não irá arrematar itens de serviço referente a licenças de uma solução que ela não forneceu e não está apta a prestar os serviços indicados.

Conforme preconiza o §2º, art. 47 da Lei Federal 14.133/2021, não assiste razão para parcelar os itens, conforme segue:

§ 2º Na aplicação do princípio do parcelamento, referente às compras, deverão ser considerados:

I - a viabilidade da divisão do objeto em lotes;

II - o aproveitamento das peculiaridades do mercado local, com vistas à economicidade, sempre que possível, desde que atendidos os parâmetros de qualidade; e

III - o dever de buscar a ampliação da competição e de evitar a concentração de mercado.

§ 3º O parcelamento não será adotado quando:

I - a economia de escala, a redução de custos de gestão de contratos ou a maior vantagem na contratação recomendar a compra do item do mesmo fornecedor;

II - o objeto a ser contratado configurar sistema único e integrado e houver a possibilidade de risco ao conjunto do objeto pretendido;

III - o processo de padronização ou de escolha de marca levar a fornecedor exclusivo.

Portanto, resta devidamente comprovado e justificado que a decisão pelo não parcelamento do objeto encontra amparo técnico e jurídico.

Uma Plataforma de Segurança de Dados, conforme definição técnica dos institutos Gartner e Forrester, constitui por sua própria natureza um **sistema único e integrado**, em que as funcionalidades de descoberta, classificação, proteção e gestão de chaves operam de forma interdependente e coordenada.

5. AUSENCIA DE DIRECIONAMENTO A FABRICANTE ESPECÍFICO

Cumpre destacar que o edital em questão **não direciona a contratação a fabricante especifico**. O que se exige e que a solução ofertada atenda aos requisitos técnicos de uma Plataforma de Segurança de Dados, com gestão integrada das funcionalidades.

Conforme os relatórios Market Guide for Data Security Platforms do Gartner e The Forrester Wave: Data Security Platforms do Forrester, existem múltiplos fabricantes qualificados que oferecem soluções nesta categoria. A existência de diversos fornecedores aptos a atender aos requisitos demonstra que **não há restrição indevida a competitividade**.

O edital estabelece requisitos técnicos objetivos, baseados em definições de mercado amplamente reconhecidas, permitindo a participação de qualquer fornecedor que disponha de solução que atenda aos requisitos técnicos do objeto.

6. CONCLUSAO

Diante do exposto, conclui-se que:

I. As soluções de DLP (Forcepoint, Microsoft Purview, Broadcom/Symantec e Digital Guardian) possuem finalidade técnica própria, voltada ao monitoramento e controle do uso adequado dos dados. Esta finalidade constitui categoria de produto independente, que não guarda equivalência com o objeto licitado.

II. As soluções de Gestão de Vulnerabilidades (Tenable, Rapid7 e Qualys) possuem finalidade técnica voltada a identificação de falhas em infraestrutura de TI. Esta finalidade constitui categoria de produto independente, que não guarda qualquer relacao com o objeto licitado.

III. Os HSMs (Entrust, Fortanix e Utimaco) representam módulos com finalidade especifica (custodia de chaves), que podem ser contratados separadamente para casos de uso próprios. Quando o objetivo e uma Plataforma de Segurança de Dados, HSMs isolados não atendem aos requisitos do objeto.

IV. As soluções de Gestão de Secrets (HashiCorp Vault) possuem finalidade técnica voltada a autenticação segura entre máquinas e sistemas. Esta finalidade constitui categoria de produto independente, que não guarda equivalência com o objeto licitado.

V. Os institutos de pesquisa independentes Gartner e Forrester recomendam a consolidação de ferramentas de segurança em plataformas integradas, com 75% das organizações buscando esta estratégia e 65% visando melhoria da postura de risco.

VI. O edital não direciona a contratação a fabricante específico, estabelecendo requisitos técnicos objetivos que podem ser atendidos por múltiplos fornecedores qualificados.

VII. A Lei 14.133/2021, Art. 40, Parágrafo 3o, inciso II, fundamenta o não parcelamento quando o objeto configura sistema único e integrado, condição que se aplica a uma Plataforma de Segurança de Dados conforme definições técnicas de mercado.

Ante o exposto, considerando que as soluções citadas pela impugnante constituem categorias de produtos com finalidades próprias e independentes, distintas do objeto licitado e que há fundamentação técnica e alicerce legal para o não parcelamento do objeto, recomenda-se o INDEFERIMENTO da impugnação apresentada, mantendo-se inalterados os termos do edital e seus anexos.

7. REFERENCIAS

7.1 Institutos de Pesquisa Independentes

[1] Gartner. Market Guide for Data Security Platforms. Marco 2025.

[2] Gartner. Survey Shows 75% of Organizations Are Pursuing Security Vendor Consolidation. Setembro 2022.

[3] Gartner. Top Cybersecurity Trends for 2023. Abril 2023.

[4] Forrester. The Forrester Wave: Data Security Platforms, Q1 2025. Marco 2025.

[5] Forrester. Buyer's Guide: Data Security Platforms, 2025.

7.2 Documentacao Oficial de Fabricantes

[6] Tenable. Vulnerability Management Principles. 2025.

[7] HashiCorp. What is Vault? Developer Portal.

[8] HashiCorp. HCP Vault Secrets Documentation.

7.3 Legislacao

[9] Brasil. Lei no 14.133/2021 (Nova Lei de Licitacoes e Contratos).

(...)

III. DA CONCLUSÃO:

Tendo em vista o exposto, bem como os fatos e fundamentos jurídicos apresentados, **RECEBO as arguições referentes ao pedido de esclarecimento,** formulados pela empresa interessada, relativos ao **PREGÃO ELETRÔNICO N.° 90220/2025/LEI Nº 14.133/2021**. Com fundamento nas normas legais aplicáveis, em especial na Lei nº 14.133/2021, especialmente em seu artigo 5º, que estabelece os princípios da legalidade, impessoalidade, moralidade, publicidade, eficiência, interesse público, probidade administrativa, igualdade, planejamento, transparência, eficácia, segregação de funções, motivação, vinculação ao edital, julgamento objetivo, segurança jurídica, razoabilidade, competitividade, proporcionalidade, celeridade, economicidade e desenvolvimento nacional sustentável, bem como nas disposições do Decreto-Lei nº 4.657, de 4 de setembro de 1942 (Lei de Introdução às Normas do Direito Brasileiro).

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

Atenciosamente,

Porto Velho, data e hora do sistema.

LUCIANA PEREIRA DE SOUZA
Pregoeira da Comissão Especial de Licitações- COESP
Portaria n.° 35 de 29 de janeiro de 2026