Prezados Senhores,

Em atenção ao Pedido de Esclarecimento referente ao Pregão Eletrônico Nº 009/2025, esta Fundação SEADE manifesta-se nos seguintes termos:

Esclarecimento 01: item 5.1 que trata do preenchimento da proposta no sistema eletrônico, em seu subitem 5.1.2. diz que a proposta do licitante deverá vir acompanhada de documentação técnica. No entanto, tendo em vista que a fase de habilitação sucederá as fases de apresentação de propostas e que o portal Compras.Gov não disponibiliza campo para anexar documentos antes da disputa, entende a proponente que os documentos técnicos deverão ser apresentados somente pela empresa arrematante após a fase de lances. Está correto nosso entendimento?

ESCLARECIMENTO: Sim

Esclarecimento 02: conforme CLÁUSULA DÉCIMA PRIMEIRA – GARANTIA DE EXECUÇÃO da minuta do contrato, a contratada deverá prestar garantia de execução do contrato nos moldes do art. 96 da Lei nº 14.133, de 2021.No entanto, não é informado qual será a porcentagem exigida. Sendo assim, questionamos: qual porcentagem a proponente deverá considerar?

ESCLARECIMENTO: Esclarecemos que por um erro material não constou o percentual de 5% (cinco por cento) relativo Cláusula Décima Primeira, a saber:

1. CLÁUSULA DÉCIMA PRIMEIRA – GARANTIA DE EXECUÇÃO (art. 92, XII)
A contratação conta com garantia de execução prestada pelo Contratado, nos moldes do art. 96 da Lei nº 14.133, de 2021, na modalidade XXXXXX, no valor de R$_____, correspondente a 5% (cinco por cento) do valor inicial do contrato, observando-se para a definição e aplicação desse percentual, quando o caso, o disposto no parágrafo único do artigo 98 do referido diploma legal.

Esclarecimento 03: O edital determina que, no momento da habilitação, para qualificação técnica da empresa licitante, deverá ser apresentado atestado com *"regularmente emitido(s) pelo conselho profissional competente, quando for o caso".* Entendemos que se trata de texto padrão inserido no edital, sendo descartada a apresentação do atestado da licitante registrado na entidade profissional competente (CREA). Nosso entendimento está correto?
Caso não seja este o entendimento da comissão, solicitamos a gentileza de justificar a exigência supracitada.

ESCLARECIMENTO: Sim

Esclarecimento 04: com relação aos prazos de entrega exige-se que**:**
"5.1.3.1. A entrega dos equipamentos/materiais para a implantação deverá ocorrer num prazo máximo de, até 30 (trinta) dias, a contar da data da assinatura do instrumento de contrato.
5.1.3.2. A prestação de serviços de instalação, configuração, parametrização, e etc., incluindo a migração de servidores virtualizados e treinamentos deverão estar plenamente concluídos e funcionando num prazo máximo de 30 dias corridos após a assinatura do contrato."

Ponderando que a logística do fornecimento de produtos importados de informática envolve fabricantes, distribuidores, revenda e cliente final, os licitantes que prezam pela qualidade no fornecimento e em honrar seus contratos, são afastados do certame pelo curto prazo de fornecimento. Entende a proponente que para ampliar o universo de participantes e possibilitar a administração em adquirir o objeto licitado numa condição mais vantajosa, o prazo de entrega dos equipamentos e prestação dos serviços poderá ser de até 90 (noventa) dias, contados da assinatura do contrato, sendo assim mais razoável. Nosso entendimento está correto?

ESCLARECIMENTO: Em referência ao Pedido de Dilação de Prazo de entrega, esta Fundação SEADE manifesta-se nos seguintes termos sobre a alegação de exíguo prazo para fornecimento dos serviços após assinatura do contrato:

1. **Da Essencialidade do Prazo para Continuidade dos Serviços Públicos:** A Administração reitera que o prazo estabelecido para a efetivação da prestação dos serviços, após a celebração do contrato, constitui requisito **fundamental e estratégico** para a garantia da continuidade dos serviços de segurança da informação da Fundação SEADE. Conforme explicitado no Estudo Técnico Preliminar (ETP), a presente contratação visa a modernização e a substituição do contrato atual, que possui término previsto para **agosto de 2025**. A inobservância desse cronograma acarreta risco iminente de descontinuidade da proteção do ambiente de Tecnologia da Informação da Fundação, comprometendo diretamente a integridade, disponibilidade e confidencialidade dos dados e sistemas que sustentam as atividades finalísticas desta Instituição.
2. **Da Razoabilidade e da Análise de Mercado na Definição do Prazo:** O foi estabelecido com base em criteriosa análise das **ofertas de mercado de soluções do tipo "Firewall como Serviço (FwaaS)" e congêneres**. A escolha pela Solução 3 ("Firewall como Serviço") foi precisamente fundamentada em sua característica de **rápida implementação**, conforme destacado no ETP: "Diante das análises e vantagens apresentadas, a contratação da Solução 3, "Firewall como Serviço (FwaaS)", se mostra como a opção mais vantajosa e estratégica para a Fundação Seade. Ela garante a segurança, a continuidade e a eficiência dos serviços da instituição, ao mesmo tempo em que otimiza custos e libera a equipe interna para atividades de maior valor estratégico."

   Empresas aptas a fornecer soluções nesse modelo, que implicam tipicamente em infraestrutura gerenciada e entregue como serviço, precisam possuir a capacidade e a expertise para cumprir com o cronograma demandado pela natureza do objeto. A adequação de processos internos da Contratada para atendimento aos prazos editalícios é uma condição inerente à sua capacidade de execução, não podendo o interesse individual em postergar prazos se sobrepor ao interesse público na continuidade e segurança dos serviços.

3. **Conformidade com Princípios Licitatórios:** A exigência do prazo se alinha aos princípios da **eficiência, da celeridade e da economicidade** (considerando os custos da descontinuidade ou atraso), bem como ao princípio da **vinculação ao instrumento convocatório**. A Administração, ao definir seus requisitos, considera suas necessidades essenciais e a capacidade de atendimento do mercado apto a fornecer a solução pretendida.

Diante do exposto, e considerando a fundamental necessidade de continuidade dos serviços e a análise de mercado que corrobora a exequibilidade do prazo para empresas preparadas para a prestação dos

serviços de "Firewall como Serviço", a Administração **mantém inalterado o prazo estabelecido** para a efetivação da prestação dos serviços após a celebração do contrato.

Esclarecimento 05: Com relação aos profissionais certificados nas tecnologias, que serão designados para a prestação dos serviços do item 7 (NOC) e 8 (SOC), entendemos que serão aceitos profissionais da contratada, com comprovação através de CTPS e/ou Contrato de prestação de serviços (PJ). Nosso entendimento está correto?

Esclarecimento 06: Com relação ao ITEM 5 - Solução de XDR (400 (quatrocentas) licenças), Requisito do Agente (coletor), o cenário atual de Cibersegurança tem enfrentado uma crescente sofisticação nas ameaças cibernéticas, incluindo ataques com dupla criptografia por ransomware, malwares sem arquivo e técnicas de OFUSCAÇÃO baseadas em inteligência artificial. Diante desse contexto, é essencial que as soluções de anti-malware sejam mais robustas e tecnologicamente avançadas para garantir uma proteção eficaz. Entretanto, os requisitos mínimos atualmente definidos (120 MB de RAM, 2% de CPU e 20 MB de disco) não são suficientes para suportar funcionalidades modernas, como análise comportamental, machine learning e análise dinâmica de ameaças. Sugerimos a revisão desses parâmetros para, no mínimo, 1024 MB de RAM, 5% de CPU e 2048 MB de espaço em disco, permitindo que a solução atue de forma mais eficiente, sem comprometer o desempenho do ambiente. Com base nisso, entendemos que os requisitos atuais acabam limitando a operação estável e eficaz da solução de segurança. Está correto o nosso entendimento?

ESCLARECIMENTO: Devido a dinâmica operacional das soluções XDR modernas. Temos o seguinte:

- Comportamento de Agentes XDR Modernos: Reconhecemos que as soluções XDR atuais utilizam mecanismos avançados como análise comportamental, machine learning e inspeção contínua. Essas tecnologias são fundamentais para a identificação de ameaças sofisticadas, mas, por sua natureza, demandam um uso de recursos que varia dinamicamente. É, de fato, esperado que durante eventos de escaneamento, mitigação ou resposta a incidentes, o consumo de CPU, RAM e disco possa superar os limites (dentro do razoável) estabelecidos para um estado ocioso.
- Variação Conforme o Contexto do Endpoint: Além disso, a heterogeneidade da infraestrutura computacional nos ambientes corporativos é um fator crucial. O desempenho do agente é, sem dúvida, influenciado pelas características técnicas da máquina onde será instalado (arquitetura do processador, RAM disponível, utilização de disco, etc.). Dessa forma, pode não ser preciso garantir um consumo fixo e padronizado de CPU, RAM e disco em todos os cenários possíveis de operação.

Portanto, reafirmamos que os limites estabelecidos para o consumo de recursos (120 MB de memória RAM, menos de 2% de uso da CPU e menos de 20 MB de espaço em disco) referem-se ao estado ocioso estimado do agente.

É aceitável que haja variação no consumo, dentro de parâmetros razoáveis, conforme o contexto do endpoint, especialmente durante atividades intensivas como escaneamento, detecção ativa ou resposta a incidentes. O que buscamos é um desempenho otimizado em condições normais de operação, sem que isso impeça a capacidade da solução de atuar de forma eficaz em momentos críticos, sendo, portanto, neste contexto, são aceitos os valores sugeridos.

Esclarecimento 07: Com relação ao ITEM 5 - Solução de XDR (400 (quatrocentas) licenças), Requisito - Controle de Vulnerabilidade e Comunicação, na linha do item que estabelece que “a solução proposta deve ter capacidade para realizar um patch virtual, por meio da restrição de acessos de comunicação nas aplicações vulneráveis”, gostaríamos de esclarecer um ponto. O termo "Virtual Patch", assim como a abordagem baseada em HIPS (Host Intrusion Prevention System) está tradicionalmente associado a soluções legadas de segurança, fundamentadas principalmente em assinaturas ou regras pré-definidas. A proteção oferecida pela solução que propomos não se baseia em assinaturas ou métodos convencionais de correção virtual, que identificam comportamentos anômalos, como tentativas de injeção de memória, execução de processos suspeitos ou outras atividades potencialmente maliciosas. Dessa forma, entendemos que o objetivo do item pode ser atendido por meio dessa abordagem mais atual de proteção baseada em comportamento. Está correto o nosso entendimento?

ESCLARECIMENTO: O item apontado remete que o agente no endpoint receba as últimas atualizações ou assinaturas para que possa estar com as últimas versões de segurança. A solução proposta deve garantir que os endpoints recebam updates com as últimas vacinas.

Esclarecimento 08: Com relação ao ITEM 5 - Solução de XDR (400 (quatrocentas) licenças), Requisito - Console de Administração, na linha do item que estabelece que “a solução proposta deve exigir que uma senha seja desabilitada por um aplicativo de terceiros”, compreendemos que o agente instalado no dispositivo deve possuir proteção por senha, conforme definido na política de segurança da solução. Adicionalmente, entendemos que essa senha deve poder ser desativada por meio de um aplicativo de terceiros, possivelmente por meio de integração via API ou mecanismo equivalente. Está correto o nosso entendimento?

Esclarecimento: O entendimento é que essa funcionalidade indica que, deve ser necessário senha para que um aplicativo terceiro desabilite o agente.

Item 1 – Firewall

Esclarecimento 09: É exigido para o ITEM 1 – Firewall em seus subitens 7, 11 e 12 as seguintes especificações respectivamente:

- Suportar Throughput de, no mínimo, 20 Gbps com a funcionalidade de firewall **(UTM/NGFW, IPS, Controle de Aplicação, Filtro de URL e Antivírus)** habilitada para tráfego IPv4 e IPv6, independentemente do tamanho do pacote;
- Suportar no mínimo 3,4 Gbps de throughput de IPS;
- Suportar Throughput de, no mínimo, 1 Gbps com as seguintes funcionalidades habilitadas simultaneamente para todas as assinaturas que a plataforma de segurança possuir devidamente ativadas e atuantes: Controle de aplicação, IPS, Antivírus e Antispyware. Caso o fabricante divulgue múltiplos números de desempenho para qualquer uma destas funcionalidades, somente o de menor valor será aceito;

Ocorre que essas especificações se sobrescrevem no sentido de exigirem números diferentes de desempenho para basicamente o mesmo cenário, pois se é exigido que o firewall suporte 20 Gbps com as funcionalidades de UTM/NGFW, IPS, Controle de Aplicação, Filtro de URL e Antivírus, somente considerando somente a funcionalidade de IPS, como exige o item 11, é um cenário que exige menos do hardware e deveria, portanto, ser mais performático. O mesmo acontece para o item 12. Entendemos que nesse caso deve-se considerar como capacidade mínima exigida a maior capacidade especificada, ou seja, o subitem 7. Está correto nosso entendimento?

ESCLARECIMENTO: A referência do item 7 do 3. ESPECIFICAÇÕES DAS CARACTERÍSTICAS MÍNIMAS OBRIGATÓRIAS (pg 86) deve ser atendida, é sobre Throughput de Firewall, IPv4 e IPv6, UDP 1518 / 512 / 64 byte.

Esclarecimento 10: É exigido para o ITEM 1 – Firewall em seu subitem 9, que a solução suporte 200.000 (mil) novas conexões por segundo. Ocorre que a solução da Cisco que atende ao tamanho e desempenhos exigidos e, portanto, estará em nível de paridade de competitividade com seus concorrentes suporta 170.000 (mil) novas conexões por segundo. Em tempo, estimar essa quantidade de conexões deve levar em consideração a quantidade de usuários, dispositivos e o perfil de uso dos mesmos, ou até mesmo dados históricos da solução em produção atualmente, estimando, em pior caso, que cada usuário/dispositivo faça 20 novas conexões por segundo, o total de 170 mil novas conexões por segunda atenderia um ambiente de 8.500 usuários/dispositivos. Entendemos que o suporte a 170.000 (mil) licenças é suficiente para atendimento ao ambiente da SEADE e será considerado como suficiente para atender à exigência. Nosso entendimento está correto?

ESCLARECIMENTO: A solução proposta deve atender a quantidade estipulada de conexões.

Esclarecimento 11: É exigido no tópico de características gerais do ITEM 1 – firewall, que seja suportado PIM-DM para roteamento multicast. Ocorre que a solução da Cisco não suporta PIM-DM, somente PIM-SM. O PIM-DM só seria utilizado em caso de ambientes com sistema legado que só suporte esse protocolo, já que o PIM-SM é o protocolo mais atual e evita broadcast necessário na rede. Entendemos que o suporte somente ao PIM-SM será suficiente para atendimento desse item. Está correto nosso entendimento?

ESCLARECIMENTO: A solução deve comportar ao menos o PIM-DM. Qualquer outro suportado, adicionalmente, será considerado um ganho e diferencial. Entendemos que o PIM-SM, além de ser uma proposta mais atual, atende e supera o solicitado.

Esclarecimento 12: É exigido no subitem 25 do Item 1 – Firewall, que a solução deve ser capaz implementar balanceamento de link por peso. Nesta opção deve ser possível definir o percentual de tráfego que será escoado por cada um dos links. Deve suportar o balanceamento de, no mínimo, três links. Ocorre que a solução da Cisco permite o balanceamento desses três links, mas não permite a definição do percentual a ser escoado por cada um deles. Entendemos que, com o objetivo de respeitar o princípio da competitividade, será permitido atender o item dessa forma, possibilitando a participação do fabricante Cisco. Está correto nosso entendimento?

ESCLARECIMENTO: A solução deve, de alguma forma, ser capaz de efetuar o balanceamento por peso, prioridade ou banda.

Esclarecimento 13: É exigido no subitem 26, do tópico prevenção de ameaças, que a solução deve “Permitir o bloqueio de vírus e spywares em, pelo menos, os seguintes protocolos: HTTP, FTP, CIFS, SMTP e POP3;” O protocolo CIFS é um protocolo já descontinuado e raramente utilizado e, portanto, não o suportamos. Suportamos o protocolo sucessor do CIFS, o SMB em suas versões mais recentes. Entendemos que tal item estará atendido dessa forma. Está correto nosso entendimento?

ESCLARECIMENTO: Sim, poderá ser considerado o SMB

Esclarecimento 14: O subitem 36 de mesmo tópico especifica que a solução deve “Fornecer proteção contra-ataques de dia zero por meio de estreita integração com os componentes Sandbox (on-premise e nuvem);” Entendemos que a capacidade de armazenar a base de reputação de arquivos localmente e a capacidade de passar um arquivo pelo crivo do Sandbox na nuvem é suficiente para atendimento a essa especificação. Via regra essa é a forma de implementação de todos os fabricantes, já que ter algo on-premisses para Sandbox aumenta o footprint, custo e tempo de deploy da solução. Está correto nosso entendimento?

ESCLARECIMENTO: Sim, correto o entendimento

Esclarecimento 15: É exigido no tópico QoS e Traffic Shaping, em seus subitens, a capacidade de QoS, como marcação e modificação de valores dos campos DSCP e Diffserv, além de políticas de QoS. Acontece que a solução da Cisco, um dos líderes desse mercado e presente no quadrante mágico do Gartner, não suporta QoS somente traffic shaping. Entendemos que, respeitando o princípio da competitividade, em que o processo de seleção deva ser o mais aberto possível desde que mantendo a qualidade exigida pelo órgão e ambiente, entendemos que suportando Traffic Shaping é suficiente e atende a necessidade da Contratante. Está correto no entendimento?

ESCLARECIMENTO: De algum modo a solução deve entregar minimamente as 2 opções

Esclarecimento 16: O tópico que trata das especificações de VPN, exige em seu subitem 4, suportar autenticação MD5, e em seu subitem 6 suportar os algoritmos Diffie-Hellman dos grupos 1, 2, 5 e 14. Acontece que tanto a autenticação usando MD5 quanto os algoritmos Diffie-Hellman dos grupos 1 e 2 já foram descontinuados e já é recomendado a sua não utilização, por já serem passíveis de violação. A solução da Cisco, prezando sempre pela segurança, já não suporta tais protocolos/algoritmos. Por ser um risco ao ambiente, entendemos não ser obrigado o suporte a tais protocolos e algoritmos. Está correto nosso entendimento?

ESCLARECIMENTO: Neste contexto, podemos considerar o apontamento como não obrigatório

Esclarecimento 17: No item 02 que especifica o Access Point, é exigido em seu subitem 7 que o rádio deve “Ter potência máxima de ao menos 23 dBm.” Entendemos que o atendimento a esse item pode ser considerado a soma da potência do rádio com o ganho da Antena, ou seja, o EIRP. Está correto nosso entendimento?

ESCLARECIMENTO: Será considerado o valor de potência do rádio apontada no datasheet do fabricante.

Esclarecimento 18: É exigido no subitem 11 do Item 02 que o ponto de acesso possa operar em modos Mesh, Tunnel e Local-Bridge. Entendemos que o suporte as funcionalidades de mesh e local-bridge sejam suficientes para atendimento ao edital desde que todos os outros recursos sejam atendidos pelo equipamento/solução proposto, está correto nosso entendimento?

ESCLARECIMENTO: A solução proposta deve oferecer possibilidade de operar nos 3 modos descritos, mesmo que na implantação seja definido apenas um deles.

Esclarecimento 19: O Item 3 que trata da especificação da Solução de Armazenamento de logs e relatórios para a solução do firewall exige que “4. Deve permitir a gravação de no mínimo 190GB de logs por dia e possuir no mínimo 2 (dois) TBytes de capacidade de armazenamento interno;” A solução da Cisco que atende aos requisitos e mais se aproxima dessa capacidade suporta 1.8 (um ponto oito) TBytes. Entendemos que tal diferença não causará impacto nenhum à solução e, portanto, solicitamos que seja permitido o atendimento a esse item com 1.8 TBytes de capacidade de armazenamento interno. Podemos entender assim?

ESCLARECIMENTO: Sim, pode ser utilizado da forma apontada em 1,8TB