FUNDAÇÃO NACIONAL DE SAÚDE

NOTA TÉCNICA Nº 48/2020/CGMTI/DEADM/PRESI

PROCESSO Nº 25100.000191/2020-64

INTERESSADO: @interessados@

1. **ASSUNTO**

1.1. Pedido de Impugnação - Igor Homar (2458144)

2. **REFERÊNCIAS**

Nota Técnica 47 (2445447)

Pedido de Impugnação - Igor Homar (2458144)

Aviso de suspensão (2457217)

3. **SUMÁRIO EXECUTIVO**

3.1. Trata-se da análise técnica dos argumentos contidos no instrumento de impugnação ao edital de licitação do Pregão Eletrônico n. 16/2020, enviado pelo cidadão Igor Xavier Homar, e baseado no conteúdo do documento, infere-se que seja representante legal do fabricante Sophos.

3.2. A análise técnica tem como objetivo responder os apontamentos realizados pelo impugnantes, quais sejam:

3.3. a) Necessidade de revisão do parcelamento do objeto licitado, tendo em vista que a sua divisão tem severas implicações econômicas nocivas à Administração;

3.4. b) Revisão de diversos itens técnicos relativos às soluções de Endpoint protection, Anti-Spam, ameaças avançadas (ATP) e DLP que, de forma injustificada, excluem da disputa algumas das soluções líderes do quadrante mágico do Gartner Group, restringindo injustificadamente a plena competitividade almejada pelo procedimento licitatório;

3.5. c) Existência de itens técnicos injustificáveis que reclamam modificações.

4. **ANÁLISE**

4.1. Trata-se da análise técnica dos argumentos contidos no instrumento de impugnação ao edital de licitação do Pregão Eletrônico n. 16/2020, enviado pelo cidadão Igor Xavier Homar, e baseado no conteúdo do documento, infere-se que seja representante legal do fabricante Sophos.

4.2. A análise técnica tem como objetivo responder os apontamentos realizados pelo impugnantes, quais sejam:

a) Necessidade de revisão do parcelamento do objeto licitado, tendo em vista que a sua divisão tem severas implicações econômicas nocivas à Administração;

b) Revisão de diversos itens técnicos relativos às soluções de Endpoint protection, Anti-Spam, ameaças avançadas (ATP) e DLP que, de forma injustificada, excluem da disputa algumas das soluções líderes do quadrante mágico do Gartner Group, restringindo injustificadamente a plena competitividade almejada pelo procedimento licitatório;

c) Existência de itens técnicos injustificáveis que reclamam modificações.

4.3. **1. Necessidade de revisão do parcelamento do objeto licitado, tendo em vista que a sua divisão tem severas implicações econômicas nocivas à Administração**

4.4. Dentre os principais objetivos do projeto destaca-se o atendimento a demandas para soluções de proteção de usuários (endpoint) e prevenção de vazamento de dados. Esse escopo de projeto de segurança é atendido atualmente por meio dos contratos 36/2017, 50/2018 e 46/2018 (expirado e não renovado). Esses três contratos tratam das ferramentas de segurança que são a proteção de endpoint, a proteção de e-mail, a proteção contra ameaças avançadas e a proteção contra vazamento de dados.

4.5. Inicialmente, o Estudo técnico analisou incluir todas essas ferramentas em um lote único, no entanto, conforme Nota Técnica 09 (documento sei nº 2025417) anexada ao processo de contratação (25100.000191/2020-64) foi demonstrada uma análise sobre funcionalidades necessárias para manter o nível de maturidade do órgão e os fabricantes de solução de DLP capazes de fornecer tais funcionalidades. Assim, a equipe técnica entendeu que as funcionalidades de um DLP de endpoint não atenderiam as necessidades da instituição e nem conseguiriam suprir as funcionalidades já utilizadas nas ferramentas de DLP do contrato 46/2018. Uma observação importante é que a impugnante não citou o estudo contido na Nota Técnica 09 (documento sei nº 2025417) em suas afirmações, o que demonstra que não foi analisado todo o conteúdo do Estudo Técnico Preliminar para a elaboração do pedido de impugnação, já que o requerente foi plenamente atendido quando solicitou acesso completo ao processo ao qual pertencem os artefatos do Planejamento da Contratação, além de ter recebido tais documentos por e-mail. Ainda, vale lembrar que, espontaneamente, esta equipe, como forma de promoção à transparência, isonomia e controle social, demonstrando que nada temos a esconder sobre o processo em discussão, enviou tais documentos para diversos outros fabricantes de soluções previstas no Termo de Referência: Sophos, Microsoft, Symantec/Broadcom, TrendMicro, McAfee, Kaspersky, CheckPoint, Forcepoint e Fortinet.

4.6. Como já explanado, o início do estudo técnico visava contratar a ferramenta de segurança de Endpoint com a ferramenta de DLP no mesmo agente, em um lote único. Após consulta ao mercado, alguns fabricantes manifestaram a incapacidade de atendimento das exigências de EPP e DLP, enquanto alguns fabricantes como Trend e Sophos, por exemplo, manifestaram a capacidade de suas ferramentas em atender tal necessidade, ou seja, poderiam entregar essa solução em um único agente. Por outro lado, as funcionalidades de DLP oferecidas tem foco em proteção de desktop, e tem limitações das suas funcionalidades quando comparadas com as ferramentas de DLP puro, como pode ser verificado pelo item 4 da Nota Técnica 09 (documento sei nº 2025417) – LEVANTAMENTO DAS ALTERNATIVAS (DLP).

4.7. Cabe observar que para se alcançar o controle de informações pretendido pela solução de DLP, como demonstrado na Nota Técnica 09 (documento sei nº 2025417) do Estudo Técnico Preliminar, a solução a ser adquirida não se trata de solução tradicional de controle de segurança para desktop, mas sim de uma solução capaz de tratar tanto de dados estruturados como dados não estruturados, se fazendo assim a construção de segurança não somente na camada do endpoint, mas sim de diversas estratégias para melhor atendimento as normatizações e necessidades da FUNASA.

4.8. Dando maior detalhes, o projeto tem em vista não somente a proteção dos dados oriundos do desktop dos usuários foco das soluções de Endpoint Protection Platform (EPP), mas sim de dados em rede, busca de informações em ambientes como banco de dados, servidores de arquivo, ambiente de servidores e desktop se fazendo assim objetivos completamente diferentes de uma solução de segurança do tipo EPP. Outro ponto que deve ser observado nesse projeto é a necessidade de uma solução que permita a classificações de dados, outra vertente comtemplada nesse projeto e não contempladas por soluções do tipo EPP.

4.9. Tendo em vista as limitações por diversas soluções tradicionais de segurança de foco somente em antivírus e tratativas de malware, a equipe de planejamento da contratação embasou-se nos princípios da razoabilidade e competitividade para a tomada de decisão de separação dos itens em

lotes distintos. Tal decisão também é embasada nas necessidades advindas das demandas tecnológicas e das exigências contidas nas legislações vigentes, como a Lei Geral de Proteção de Dados Pessoais - LGPD, que não são alcançadas por soluções de mercado de segurança do tipo EPP. Assim, demonstra-se correta a decisão pela divisão em lotes, garantindo assim um certame aberto e mais competitivo, permitindo que essa ferramenta possa ser fornecida por fabricantes que possuem soluções especializadas em controle de dados, não limitando a competição, considerando que poucos são os fabricantes que podem entregar na mesma ferramenta as soluções de EPP e DLP descritas no Termo de Referência.

4.10. Abaixo descrevemos alguns exemplos de uso de dados no DLP:

- **Dado em repouso (Data at rest)** - São os dados em descanso que ficam armazenados nos repositórios de toda rede, seja na máquina do usuário, seja no SharePoint, seja no banco de dados (SQL, Oracle e demais), seja armazenado até mesmo em um driver em nuvem (OneDrive).
- **Dado em trânsito (data in motion)** - São os repositórios que são acessados pelos usuários, onde os dados são acessados a todo instante para serem manipulados, uma tabela no banco de dados da empresa, uma planilha de Excel em um SharePoint ou servidor de arquivo.
- **Data in Use (Dados em uso)** - São as maquinas endpoint, e o fato de se chamar endpoint não quer dizer que é um projeto somente de endpoint. São os dados usados na memória do computador.

4.11. Conforme o item 4.10 da Nota Técnica 09 (documento sei nº 2025417) que analisa os principais fabricantes de solução de DLP - Guardião Digital, Forcepoint, McAfee e Symantec - é identificado que esses players possuem diversas funcionalidades e módulos que o DLP de endpoint não possui. Logo, pode-se concluir que a ferramenta de DLP fornecida pela Sophos e pela Trend não atendem às necessidades técnicas da Funasa.

4.12. Por outro lado, não entendemos adequados os argumentos técnicos para se manterem os requisitos que as funcionalidades desses 3 (três) módulos (dados em uso, repouso e em trânsito) sejam executadas por apenas um agente único. Para esclarecimento sobre esse item, a equipe técnica entendeu que caso fossem exigidas todas essas ferramentas de segurança em um único lote, provavelmente, apenas dois fabricantes de soluções seriam capazes de atender a especificação, fato que comprometeria fortemente a competitividade do certame.

4.13. A impugnante informa que consegue fornecer a solução de Endpoint + DLP em um único agente, porém, não deixa claro se a mesma consegue atender todas as necessidades técnicas exigidas para a ferramenta de DLP descritas no Termo de Referência.

4.14. Desse modo, o pedido da impugnação por si só já não tem sentido, pois sugere que seja ignorado o princípio da ampla competição, limitado a possibilidade de participação às empresas que possuem um único agente e excluindo outros fabricantes que forneçam soluções mais robustas de DLP, já que, como mencionado, o projeto de proteção de dados é mais abrangente que uma solução de proteção de endpoint que venha a proteger apenas estações de trabalho.

4.15. Quanto às tecnologias testadas no ambiente da FUNASA, a impugnante oculta informações do Estudo Técnico Preliminar e evidencia somente parte do seu conteúdo, com o intuito de ocultar os fatos, pois a mesma analisou o ETP e evidenciou somente o item 5.5, no qual faz uma análise da solução Trend, contudo, não se aprofundou na leitura do documento e ignorou o item 5.2 que demonstra uma análise das ferramentas Symantec utilizadas no ambiente da Funasa, não tendo também se atentado ao item 5.3 que faz um estudo das ferramentas de segurança da Microsoft. Logo, vemos aqui um novo equívoco cometido pela impugnante, resultado de uma análise superficial e parcial dos estudos preliminares, que resultou em diversas afirmações infundadas sobre a equipe técnica de planejamento da contratação, sendo a mais incômoda, aquela que sugere direcionamento para uma solução específica.

4.16. Logo em seguida o impugnante discorre análise sobre o estudo Técnico Preliminar e sobre a necessidade de Revisão do Parcelamento do Objeto, considerando o cálculo apresentado no Estudo Técnico Preliminar para o Custo de propriedade.

4.17. O requerente afirma em sua peça que o Termo de Referência como descrito tem o potencial de causar grave prejuízo ao Erário pelas seguintes razões:

a) pelo incremento no custo total de propriedade relativo ao projeto

b) pelo incremento nos gastos com recursos humanos para gestão do sistema; e

c) pela possibilidade de que se imponha à Administração a realização de compras de produtos e licenças de forma repetida e sobreposta

4.18. No que tange à sobreposição de objetos, como já demonstrado acima e detalhado na Nota Técnica 09 (documento sei nº 2025417) do Estudo Técnico Preliminar, documento conhecido pelo impugnante, o Termo de Referência não traz elementos sobrepostos, ainda que tenha ocorrido um pequeno erro nas tabelas do item 14 do Estudo Técnico Preliminar, que tinha como objetivo não descrever o produto, mas de demonstrar o valor estimado para cada item a ser adquirido, juntamente com suas bases de estimativas. Tal erro, provocado pela necessidade de replicar as tabelas através das funções de “CTRL+C, CTRL+V, porém, não se propagou ao Termo de Referência, que manteve a descrição correta do objeto, vide item 2.2.1 e 10.1 do Termo de Referência CGMTI (2401738):

2. **DESCRIÇÃO DA SOLUÇÃO DE TIC**

2.1. **Bens e serviços que compõem a solução**

2.2. Os quantitativos e respectivos códigos dos itens são os discriminados nas tabelas abaixo:

2.2.1. **Lote 01** - Licenciamento de solução integrada de segurança para proteção de estações de trabalho (''*Endpoint*''), gateway de e-mails (antispam) e redes, com serviços de suporte técnico e atualização, serviço de migração e serviço de treinamento para atender às necessidades da Funasa, pelo período de 36 (trinta e seis) meses.

LOTE 01				
ITEM	DESCRIÇÃO	UNIDADE	QUANTIDADE	CATMAT/CATSER
1	Licenciamento de solução centralizada de segurança do tipo Endpoint, contendo (Antivírus/Antimalware), web reputation, firewall, IPS, controle de dispositivos, controle de aplicação, EDR e Gerência centralizada, incluindo, garantia e atualização por 36 (trinta e seis) meses.	Unitário	3.560	24333
2	Licenciamento de solução de proteção gateway de e-mails (Antispam), incluindo garantia e atualização por 36 (trinta e seis) meses.	Unitário	5.000	24333
3	Licenciamento de solução de proteção contra ameaças avançadas, incluindo garantia e atualização por 36 (trinta e seis) meses	Unitário	01	24333
4	Serviço de treinamento da solução	Turma	04	3840
5	Suporte técnico especializado	Meses	36	27332
6	Serviço de Implantação e configuração das soluções - Item 1, 2, 3 e 4.	Unidade	04	27332

10. **VALOR ESTIMADO DA CONTRATAÇÃO (REFERENCIAL)**

10.1. Diante do exposto e com base na presente pesquisa de mercado, elaborada de acordo com a Instrução Normativa nº 03 de 20 de abril de 2017, considerando a configuração de uma solução de segurança que atenda a necessidades da Funasa por 36 meses, conclui-se que a valor da contratação está estimado em R$ **4.288.590,76** (quatro milhões, duzentos e oitenta e oito mil quinhentos e noventa reais e setenta e seis centavos), estão discriminados por itens nas tabelas a seguir:

Lote 01

ITEM	DESCRIÇÃO	QUANTIDADE	VALOR UNITÁRIO	VALOR TOTAL
1	Solução centralizada de segurança do tipo Endpoint, contendo (Antivírus/Antimalware), web reputation, firewall, IPS, controle de dispositivos, controle de aplicação, EDR e Gerência centralizada, incluindo, garantia e atualização por 36 (trinta e seis) meses.	3.560	R$ 234,51	R$ 834.855,06
2	Solução de proteção gateway de e-mails (Antispam), incluindo garantia e atualização por 36 (trinta e seis) meses.	5.000	R$ 118,50	R$ 592.500,00
3	Solução de proteção contra ameaças avançadas, incluindo garantia e atualização por 36 (trinta e seis) meses	1	R$ 558.745,83	R$ 558.745,83
4	Serviço de treinamento da solução	4	R$ 10.440,83	R$ 41.763,33
5	Suporte técnico especializado	36	R$8.308,81	R$ 299.117,16
6	Serviço de Implantação e configuração das soluções - Item 1, 2, 3 e 4.	4	R$ 24.980,21	R$ 99.920,83
Valor Total Lote 1				R$ 2.426.902,75

4.19. Apesar de haver um erro de digitação no Estudo Técnico Preliminar, a equipe técnica de Planejamento da Contratação não entende que o mesmo tenha trazido prejuízos ao estudo, já que não ocorreu em capítulo cujo objetivo seria definir o objeto de aquisição, o que se comprova pela correta descrição do produto no Termo de Referência e seus anexos.

4.20. Por esse motivo, não se entende necessário, por esse item, revogar o certame para republicação da documentação com essa correção no ETP.

4.21. Em relação à afirmação sobre o incremento no custo total de propriedade relativo ao projeto, pelo mesmo demonstrado acima, no Estudo Técnico Preliminar e na Nota Técnica 09 (documento sei nº 2025417), que é parte integrante do ETP, verificamos não haver fundamento no afirmado pelo impugnante quando considera que o valor de R$ 3.198.990,83 se refere ao item 1 já era composto pelo DLP. Como já demonstrado, o Item 1, de acordo com o Termo de Referência, não inclui o item de DLP com as funcionalidades descritas no seu corpo e em seus anexos. Por outro lado, está correta a afirmação quando o impugnante explica que o Termo de Referência não incluiu o item para proteção de servidores virtuais, datacenter e nuvem, com o valor estimado em R$ 778.168,67. Tal item foi excluído durante o planejamento da contratação conforme a justificativa descrita na Nota Técnica 40 (2378288)

4.22. O que o impugnante esqueceu de mencionar é que a tabela expressa no Termo de Referência não inclui esse item, e o valor levado ao Termo de Referência para o Lote 1 foi de R$ 2.426.902,75, ou seja, não incluindo o valor estimado para o item para proteção de servidores virtuais e datacenter para 36 meses. É correto afirmar sim, que o Lote 1, após exclusão do referido item, deveria ter o valor correto de R$ 2.420.821,33, porém mais uma vez, houve um pequeno erro de cálculo, que resultou em um aumento no valor estimativo do produto final em R$ 6.081,42, ou seja, 0,25%, o que não se torna relevante no caso por ser um valor estimado antes da ocorrência da disputa pelo menor preço.

4.23. Por fim, no que se refere à afirmação quanto ao incremento nos gastos com recursos humanos para a gestão do sistema, essa é uma afirmação não muito pertinente, considerando que o contrato para sustentação de infraestrutura atualmente vigente na Funasa considera os custos mensais por item de configuração sustentado e não por quantitativo de pessoal alocado para a gestão da ferramenta. Ademais, apesar de termos como ideal todas as funcionalidades em apenas uma interface de gerenciamento, a exigência desse requisito no Termo de Referência culminaria em uma restrição de competitividade entre os potenciais fornecedores, com resultados nem considerados no Estudo Técnico Preliminar.

4.24. Quanto à gestão de riscos, é fácil inferir que o incremento potencial no preço final da licitação seria impactado fortemente por tal exigência restritiva como a sugerida pelo impugnante. Por outro lado, considerando o custo do risco, calculado através do Valor Monetário Esperado - VME (VME = ΣProbabilidade x Impacto), adotando como premissa a Probabilidade = 100%, ou seja, assumindo que aumentará o número de consoles de gerências de 3 (número atual de console de gerenciamento) para 4 (número potencial dependendo das soluções vencedoras do certame), temos como resultado o VME = R$ 431,00 mensais, ou seja, VME = R$ 15.516,00 por 36 meses (Nota Técnica 49 - SEI 2455548), correspondente a 0,63% do valor previsto para o Lote 1. Sabemos que fazer gestão é fazer escolhas e assumir riscos, e nesse caso, o risco tem como contrapartida a expectativa de ampla competitividade e consequentemente redução dos custos de aquisição para o período, e basta que a redução na disputa do pregão seja maior que 0,63% para comprovar a correta escolha dos gestores que compõem a equipe de planejamento da contratação.

4.25. Assim, frente ao conflito entre restrição à competitividade e praticidade na operação das ferramentas conseguidas através das exigências técnicas excessivas, esta equipe técnica de planejamento da contratação primará sempre pelo atendimento ao interesse público e pelos princípios que regem a licitação.

5. AVALIAÇÃO DA ESPECIFICAÇÃO DE ACORDO COM A ANÁLISE DE RISCOS - NOTA TÉCNICA 49 (2455548)

5.1. No que tange à existência de itens técnicos injustificáveis que reclamam modificações e à alegação em que foram realizadas várias tentativas para tornar a tecnologia Sophos aderente com as especificações técnicas mínimas que possibilitassem a competitividade, como já demonstrado anteriormente, foi excluído o item para proteção de servidores a pedido da impugnante, além de outros ajustes, como realizado em atendimento aos diversos pedidos advindos de fornecedores. Por outro lado, foram enviadas pelo impugnante algumas solicitações de alterações nas especificações que restringem a competição sem qualquer justificativa, e por isso não foram atendidas. Por fim, algumas solicitações não foram atendidas por não atenderem à necessidade do órgão, sugerindo alterações que distorceriam o requisito inicial. Vejamos:

5.2. Análise 1

Texto da Impugnação:

> 1. SOLUÇÃO DE GERENCIAMENTO:
>
> 1.21. Permitir configuração de varredura em tempo real, permitindo selecionar o que será escaneado, como pastas, memória, rootkits e arquivos suspeitos, dentre outros;
>
> Foi solicitada a alteração deste item para:
>
> Permitir a de varredura em tempo real, verificando pastas, memória, rootkits e arquivos suspeitos, dentre outros;
>
> Resultado: Não atendido e não modificado!

Análise da equipe técnica de Planejamento da Contratação:

> Analisando a literalidade da solicitação, esta não se mostra razoável considerando a necessidade do órgão em analisar dispositivos ou áreas isoladamente, como pendrives, cartões de memória, pastas, etc. A solicitação da alteração, se atendida, buscaria uma solução que faz varredura na máquina constantemente, impedindo uma varredura em um periférico de forma isolada, podendo impactar diretamente no desempenho das máquinas protegidas.
>
> Evidenciamos que a Funasa mantém em seu parque alguns computadores mais antigos com menor capacidade de processamento. Assim, o requisito sendo mantido não significa direcionamento, já que é uma funcionalidade comum entre as soluções disponíveis no mercado.

5.3. Análise 2

Texto da Impugnação:

> 1. SOLUÇÃO DE GERENCIAMENTO:
>
> 1.34. Geração de relatórios que contenham informações como: Os TOPs vírus mais detectados, as TOPs máquinas que mais sofreram infecções, quantitativos de ameaças identificadas, os usuários que mais sofreram infecções em um determinado período;
>
> Foi solicitada a alteração deste item para:
>
> A contratada deve gerar relatórios que contenham informações como: Os TOPs vírus mais detectados, as TOPs máquinas que mais sofreram infecções, quantitativos de ameaças identificadas, os usuários que mais sofreram infecções em um determinado período;
>
> Resultado: Não atendido e não modificado!

Análise da equipe técnica de Planejamento da Contratação:

> O pedido de modificação não se mostra razoável considerando que não faz sentido que a contratada detenha o monopólio da geração de relatórios. A necessidade do órgão, que é comum em diversos outros usuários de ferramentas como esta, é que seja possível acessar a ferramenta e suas funcionalidades a qualquer tempo, como a geração de relatórios, de forma a garantir a prestação de serviço pelas equipes especializadas.
>
> Por outro lado, o pedido foi incompreendido pela equipe, considerando que se a contratada é capaz de gerar os relatórios através da ferramenta, não há motivos para que esta não seja acessada pela equipe técnica da Funasa para a mesma finalidade.

5.4. Análise 3

Texto da Impugnação:

> 4. MÓDULO DE PROTEÇÃO PARA DISPOSITIVOS MOBILE:
>
> 4.5. Deve monitorar os aplicativos do dispositivo e permitir bloquear o acesso a softwares por categorias;
>
> Foi solicitada a alteração deste item para:
>
> Deve informar os aplicativos do dispositivo e permitir o gerenciamento da store dos dispositivos Android e IOS;
>
> Resultado: Não atendido e não modificado!

Análise da equipe técnica de Planejamento da Contratação:

A sugestão não atende à necessidade do órgão, já que o que se espera é que as restrições possam ser realizadas por categorias, como por exemplo: jogos, redes sociais, aplicações bancárias, etc.

A solicitação de alteração demonstrada na redação enviada pelo requerente, obrigaria que essa classificação seja realizada pela equipe de TI do órgão, não podendo para a decisão de acolher a sugestão ou não, descartar a ampla variedade de categorias de aplicativos que podem ser instalados pelo usuário, na ordem de milhões de aplicativos disponíveis nas lojas de aplicativos.

O pedido então não se mostra razoável considerando que não faz sentido que a equipe de TI do órgão tenha de manter uma base de aplicações restritas ao órgão, não desconsiderando a grande quantidade de aplicativos disponibilizados diariamente.

5.5. Análise 4

Texto da Impugnação:

4. MÓDULO DE PROTEÇÃO PARA DISPOSITIVOS MOBILE:

4.6. Bloqueie por categoria ou aplicação;

Foi solicitada a alteração deste item para:

Bloqueie por categoria ou aplicação, Ou permitir que os aplicativos sejam instalados através da console de gerenciamento.

Resultado: Não atendido e não modificado!

Análise da equipe técnica de Planejamento da Contratação:

Da mesma forma que a sugestão anterior, a sugestão, analisada pela sua literalidade, é de difícil compreensão pela equipe técnica. Isso porque o que se espera é que a restrição possa ser realizada por categorias, como por exemplo: jogos, redes sociais, aplicações bancárias, etc. Assim, não atende a necessidade do órgão que o usuário do dispositivo móvel tenha que abrir chamado para a equipe de suporte à infraestrutura para que os aplicativos sejam instalados apenas pelas equipes técnicas. Por outro lado, isso poderia ser aceito desde que a carga adicional de trabalho para instalação dos aplicativos apenas pela console de gerenciamento seja absorvida pela contratada pelo serviço de suporte. Assim, alteraremos o texto para:

Bloqueie por categoria ou aplicação, ou permita que os aplicativos sejam instalados através da console de gerenciamento, desde que, nesse caso, sejam atendidos pela contratada através do suporte técnico.

5.6. Análise 5

Texto da Impugnação:

4. MÓDULO DE PROTEÇÃO PARA DISPOSITIVOS MOBILE:

4.15. Capacidade de configurar White e Black Lists de aplicativos.

Foi solicitada a alteração deste item para:

Capacidade de configurar White e Black Lists de Websites;

Resultado: Não atendido e não modificado!

Análise da equipe técnica de Planejamento da Contratação:

A sugestão enviada é até difícil de ser avaliada, considerando que não são sinônimos os termos “aplicativos” e “Websites”. Ainda, o item trata exclusivamente de PROTEÇÃO PARA DISPOSITIVOS MOBILE, e, portanto, a alteração desqualificaria completamente o requisito.

Assim, a sugestão do jeito que colocada não atende à necessidade do órgão, já que o que se espera é a proteção dos aplicativos móveis contra a instalação e utilização de aplicativos considerados restritos. Por outro lado, é possível aceitar a ferramenta que permita o bloqueio de websites que se comuniquem com aplicativos, impedindo assim o seu funcionamento.

Exemplo: Bloquear o website do Facebook e por consequência impedir o aplicativo do facebook de funcionar no dispositivo.

Dessa forma, a reescrita do requisito seria:

Capacidade de configurar White e Black Lists de aplicativos ou Websites que impeçam o funcionamento de um aplicativo.

Exemplo: Bloquear o website do Facebook e por consequência impedir o aplicativo do facebook de funcionar no dispositivo.

5.7. Análise 6

Texto da Impugnação:

6. MÓDULO PARA CONTROLE DE APLICAÇÕES

6.3. As políticas de controle de aplicações devem permitir a combinação lógica dos critérios para identificação do(s) alvo(s) de cada política;

Foi solicitada a alteração deste item para:

As políticas de controle de aplicações devem permitir a combinação lógica dos critérios para identificação do(s) alvo(s) de cada política, como Usuário e Grupos de Usuários, ou Computador e Grupos de Computadores;

Resultado: Não atendido e não modificado!

Análise da equipe técnica de Planejamento da Contratação:

A sugestão enviada não foi acatada por não colaborar com a ampliação da competição, considerando que o requisito do Termo de Referência amplia a interpretação da necessidade descrita, enquanto a sugestão enviada pode ser a cópia de um trecho de algum datasheet específico, e por isso pode servir como base restritiva no momento do julgamento da proposta e dos atestados de capacidade técnica.

5.8. Análise 7

Texto da Impugnação:

8. SOLUÇÃO DE PROTEÇÃO GATEWAY DE E-MAILS (ANTISPAM)

8.2. SPAM / Phishing

8.2.4. Possuir configurações de sensibilidade na detecção de SPAMs, no mínimo em 3 níveis;

Foi solicitada a alteração deste item para:

Possuir configurações de ações diferenciadas para suspeita de spam, confirmado e bulk;

Resultado: Não atendido e não modificado!

Análise da equipe técnica de Planejamento da Contratação:

A sugestão enviada não foi acatada por não colaborar com a ampliação da competição, considerando que o requisito do Termo de Referência amplia a interpretação da necessidade descrita, enquanto a sugestão enviada pode ser a cópia de um trecho de algum datasheet específico, e por isso pode servir como base restritiva no momento do julgamento da proposta e dos atestados de capacidade técnica.

A princípio, entende-se que a sugestão se enquadra em 3 níveis de sensibilidade de detecção, porém os requisitos do edital não restringem tais níveis baseados na sua denominação.

5.9. Análise 8

Texto da Impugnação:

8. SOLUÇÃO DE PROTEÇÃO GATEWAY DE E-MAILS (ANTISPAM)

8.4. FILTROS

8.4.5. Permitir criar exceções para os filtros, definidos por rotas, grupos de usuários ou usuários específicos;

Foi solicitada a alteração deste item para:

Permitir criar exceções para os filtros, definidos por origem (hosts/IP), remetentes e destinatários;

Resultado: Não atendido e não modificado!

Análise da equipe técnica de Planejamento da Contratação:

A equipe técnica não vislumbrou necessidade de alteração do texto inicial considerando que a diferença entre os dois requisitos é apenas na forma de escrita, não contendo diferença significativa de significado, e ambos poderiam ser aceitos.

5.10. Análise 9

Texto da Impugnação:

8. SOLUÇÃO DE PROTEÇÃO GATEWAY DE E-MAILS (ANTISPAM)

8.4.9. Permitir a verificação em arquivos compactados nos formatos mais utilizados em no mínimo 5 níveis de compactação;

Foi solicitada a alteração deste item para:

Permitir a verificação em arquivos compactados nos formatos mais utilizados;

Resultado: Não atendido e não modificado!

Análise da equipe técnica de Planejamento da Contratação:

A sugestão enviada não foi acatada por ferir requisitos básicos de segurança, já que, da maneira como proposta, a solução não seria capaz de verificar ameaças contidas em arquivos compactados em 2 níveis ou mais.

É possível verificar que o requisito não é restritivo, considerando ser atendido por diversos fabricantes, a exemplo:

https://hscbrasil.com.br/materiais/hsc_mli_manual%20v5_x.pdf?15266a&15266a página 157.

Symantec, McAfee e Trend informaram que atendem a esta configuração - (documento SEI n. 2337950 e documento sei n. 2338116).

5.11. Análise 10

Texto da Impugnação:

8. SOLUÇÃO DE PROTEÇÃO GATEWAY DE E-MAILS (ANTISPAM)

8.4.13. Possui regra específica para anexos protegidos por senha

Foi solicitada a alteração deste item para:

Possui funcionalidade de detectar arquivos criptografados.

Resultado: Não atendido e não modificado!

Análise da equipe técnica de Planejamento da Contratação:

A sugestão enviada é difícil de ser avaliada, considerando que não são sinônimos os termos “protegidos por senha” ou “criptografados”. Esse requisito tem sido reforçado pelas necessidades trazidas pela LGPD, e por isso, se tornou comum o tráfego de arquivos PDF protegidos por senha, que devem ter tratamento diferenciado daqueles arquivos criptografados.

Symantec, McAfee e Trend informaram que atendem a esta configuração - (documento SEI n. 2337950 e documento sei n. 2338116).

Por outro lado, se a solução comprovar que ao detectar arquivos criptografados também o faz para arquivos protegidos por senha, a solução será aceita.

5.12. Análise 11

Texto da Impugnação:

8. SOLUÇÃO DE PROTEÇÃO GATEWAY DE E-MAILS (ANTISPAM)

8.4.22. Permitir personalizar os filtros de registros baseado em:

8.4.22.1. Tempo;

8.4.22.2. Total de mensagens;

8.4.22.3. Porcentagem de mensagens;

8.4.22.4. Ação a ser tomada;

Foi solicitada a alteração deste item para:

Permitir personalizar os filtros de registros baseado em:

Tempo;

Total de mensagens por RBL

Total de mensagens verificadas por DKIM

Ação a ser tomada;

Resultado: Não atendido e não modificado!

Análise da equipe técnica de Planejamento da Contratação:

A sugestão enviada não foi acatada por não colaborar com a ampliação da competição, considerando que o requisito do Termo de Referência amplia a interpretação da necessidade descrita, enquanto a sugestão enviada pode ser a cópia de um trecho de algum

data sheet específico, e por isso pode servir como base restritiva no momento do julgamento da proposta e dos atestados de capacidade técnica.

É possível verificar que o requisito não é restritivo, podendo ser atendido pela requerente da forma como descrita na sugestão.

5.13. Análise 12

Texto da Impugnação:

8. SOLUÇÃO DE PROTEÇÃO GATEWAY DE E-MAILS (ANTISPAM)

8.4.23. Prevenir contra ataques de SPAM, permitindo rejeitar a conexão quando exceder configuração personalizada para esse ataque;

Foi solicitada a alteração deste item para:

Prevenir contra ataques de SPAM, permitindo rejeitar a mensagem quando exceder configuração personalizada para esse ataque;

Resultado: Não atendido e não modificado!

Análise da equipe técnica de Planejamento da Contratação:

A equipe técnica entende que os dois requisitos podem ser considerados equivalentes, podendo ser aceitas qualquer uma delas presentes em datasheets de soluções.

Porém, a equipe de planejamento da contratação não é contrária à republicação desse item, tornando o requisito ampliativo, da seguinte forma:

Prevenir contra ataques de SPAM, permitindo rejeitar a conexão ou mensagem quando exceder configuração personalizada para esse ataque;

5.14. Análise 13

Texto da Impugnação:

8. SOLUÇÃO DE PROTEÇÃO GATEWAY DE E-MAILS (ANTISPAM)

8.5. AÇÕES

8.5.1. Possuir recurso que permita adiar a entrega de determinadas mensagens para um horário específico;

Foi solicitada a alteração deste item para:

Possuir recurso que permita armazenar mensagens para entrega em caso de indisponibilidade;

Resultado: Não atendido e não modificado!

Análise da equipe técnica de Planejamento da Contratação:

A equipe técnica entende que ambos os requisitos não são equivalentes, porém, a equipe de planejamento da contratação não é contrária à retirada desse item tornando-o mais ampliativo.

Cabe reforçar que a Mcaffe sugeriu, como a Sophos, um texto que nada se relaciona com o objetivo inicial do requisito, vejamos:

“Sugestão Mcaffe: Possuir recurso que permita efetuar rate limiting nas mensagens que entram no ambiente.”

Dessa forma, com o intuito de flexibilizar a especificação, a equipe técnica abre mão de um requisito esperando como contrapartida a ampliação da competitividade.

5.15. Análise 14

Texto da Impugnação:

8. SOLUÇÃO DE PROTEÇÃO GATEWAY DE E-MAILS (ANTISPAM)

8.5.2. Permitir enviar notificações de ocorrências customizadas ao administrador, remetente, destinatário;

Foi solicitada a alteração deste item para:

Permitir enviar notificações de ocorrências ao remetente;

Resultado: Não atendido e não modificado!

Análise da equipe técnica de Planejamento da Contratação:

A sugestão enviada não foi acatada por não atender requisitos quanto à comunicação ao destinatário sobre falso positivo de spam, já que, da maneira como proposta, a solução não seria capaz de comunicar ao destinatário sobre a classificação de uma mensagem contendo spam, que caso fosse um falso positivo, o usuário poderia solicitar novo envio ou solicitar outras ações de tratamento pela equipe de TI do órgão.

É possível verificar que o requisito não é restritivo, considerando ser atendido por diversos fabricantes, a exemplo de https://help.symantec.com/cs/SMG_10_6_6/SMG/v19896840_v125807409/About-policy-violation-notifications?locale=EN_US e

https://support.kaspersky.com/KS4Exchange/9.2/en-EN/84818.htm.

Symantec, McAfee e Trend informaram que atendem a esta configuração - (documento SEI n. 2337950 e documento sei n. 2338116).

5.16. Análise 15

Texto da Impugnação:

8. SOLUÇÃO DE PROTEÇÃO GATEWAY DE E-MAILS (ANTISPAM)

8.5.6. Permitir apagar anexos indesejados, mas entregar a mensagem ao destinatário informando da ação;

Foi solicitada a alteração deste item para:

Permitir drop de anexos indesejados;

Resultado: Não atendido e não modificado!

Análise da equipe técnica de Planejamento da Contratação:

O objetivo do item é a entrega da mensagem, podendo o administrador definir que tipos de anexo são indesejados ou, quando maliciosos, a ferramenta possua capacidade de tratamento automatizado.

É possível verificar que o requisito não é restritivo, considerando ser atendido por diversos fabricantes, a exemplo de

https://www.hscbrasil.com.br/materiais/manual_mli_v5_0_30-2.pdf?6e6543&6e6543 e https://help.symantec.com/cs/SMSMSE_7_9/SMSMSE/SMSID0ESJAI_v126015838/About-content-and-file-filtering?locale=EN_US.

Symantec, McAfee e Trend informaram que atendem a esta configuração - (documento SEI n. 2337950 e documento sei n. 2338116).

5.17. Análise 16

Texto da Impugnação:

8. SOLUÇÃO DE PROTEÇÃO GATEWAY DE E-MAILS (ANTISPAM)

8.5.9. Permitir a escolha do local onde se irá colocar a notificação customizada para o começo ou fim da mensagem original;

Foi solicitada a alteração deste item para:

Permitir a escolha da notificação como por exemplo Proteção contra malware e Proteção de Dados;

Resultado: Não atendido e não modificado!

Análise da equipe técnica de Planejamento da Contratação:

A equipe técnica não vislumbrou necessidade de alteração do texto inicial considerando que a diferença entre os dois requisitos é apenas na forma de escrita, não contendo diferença significativa de significado, e ambos poderiam ser aceitos.

Por outro lado, a equipe de planejamento da contratação não é contrária à retirada desse item tornando-o mais ampliativo, mesmo entendendo que não se trata de um item restritivo ou que evidencie qualquer tipo de direcionamento, já é atendido por diversos fabricantes, como podemos ver nos documentos abaixo relacionados:

McAfee, Symantec e Trend informaram que atendem a esta configuração - (documento SEI n. 2337950 e documento sei n. 2338116).

https://hscbrasil.com.br/materiais/hsc_mli_manual%20v5_x.pdf?15266a&15266a página 223.

5.18. Análise 17

Texto da Impugnação:

8. SOLUÇÃO DE PROTEÇÃO GATEWAY DE E-MAILS (ANTISPAM)

8.5.10. Permitir inserir variáveis nas notificações, onde informem:

Foi solicitada a alteração deste item para:

Permitir filtrar com o uso variáveis nas áreas de quarentena ou logs, onde informem;

Resultado: Não atendido e não modificado!

Análise da equipe técnica de Planejamento da Contratação:

A equipe técnica entende que ambos os requisitos não são equivalentes, porém, a equipe de planejamento da contratação não é contrária à retirada desse item tornando-o mais ampliativo, mesmo entendendo que não se trata de um item restritivo ou que evidencie qualquer tipo de direcionamento, já é atendido por diversos fabricantes, como podemos ver nos documentos abaixo relacionados:

Atendido por Kaspersky: https://support.kaspersky.com/KS4Sharepoint/9.3/en-US/58433.htm ;

Atendido por Symantec: https://help.symantec.com/cs/SMG_10_7_0/SMG/v72426555_v132085995/Content-filtering-notification-variables?locale=EN_US

McAfee e Trend informaram que atendem a esta configuração - (documento SEI n. 2337950 e documento sei n. 2338116).

Dessa forma, com o intuito de flexibilizar a especificação, a equipe técnica abre mão de um requisito tendo como contrapartida a ampliação da competitividade.

5.19. Análise 18

Texto da Impugnação:

8. SOLUÇÃO DE PROTEÇÃO GATEWAY DE E-MAILS (ANTISPAM)

8.5.21. Nome da quarentena para onde a mensagem foi enviada;

Foi solicitada a alteração deste item para:

Enviar para quarentena;

Resultado: Não atendido e não modificado!

Análise da equipe técnica de Planejamento da Contratação:

A equipe técnica não vislumbrou necessidade de alteração do texto inicial considerando que a diferença entre os dois textos é apenas na forma de escrita, não contendo diferença significativa de significado, e ambos poderiam ser aceitos. Por outro lado, a equipe de planejamento da contratação não é contrária à alteração desse, de acordo com a solicitação, já que o impugnante entende que assim tornaria o item tornando-o mais ampliativo. Deve ficar claro que não se trata de um item restritivo ou que evidencie qualquer tipo de direcionamento, já é atendido por diversos fabricantes.

5.20. Análise 19

Texto da Impugnação:

8. SOLUÇÃO DE PROTEÇÃO GATEWAY DE E-MAILS (ANTISPAM)

8.5.22. Permitir configurar ações para mensagens fora do padrão (mensagens malformadas);

Foi solicitada a alteração deste item para:

Permitir filtrar ações para mensagens fora do padrão;

Resultado: Não atendido e não modificado!

Análise da equipe técnica de Planejamento da Contratação:

A equipe técnica não vislumbrou necessidade de alteração do texto inicial considerando que a diferença entre os dois requisitos é apenas na forma de escrita, não contendo diferença significativa de significado, e ambos poderiam ser aceitos.

5.21. Análise 20

Texto da Impugnação:

8. SOLUÇÃO DE PROTEÇÃO GATEWAY DE E-MAILS (ANTISPAM)

8.5.23. Permitir ação personalizada para mensagens com anexos protegidos por senha;

Foi solicitada a alteração deste item para:

Permitir filtrar mensagens não escaneadas;

Resultado: Não atendido e não modificado!

Análise da equipe técnica de Planejamento da Contratação:

A sugestão enviada é difícil de ser avaliada, considerando que não são sinônimos os termos "protegidos por senha" e" mensagens não escaneadas". Esse requisito tem sido reforçado pelas necessidades trazidas pela LGPD, e por isso, se tornou comum o tráfego de arquivos PDF protegidos por senha, que devem ter tratamento diferenciado. Outro ponto que dificultou o entendimento foi que a sugestão de modificação do item foi para algo totalmente diferente do que foi pedido na redação. Seria mais eficiente se a impugnante informasse o motivo que não consegue atender o item, desse modo, a equipe técnica poderia flexibilizar o item para a participação do reclamante.

É importante mencionar que não se trata de um item restritivo ou que evidencie qualquer tipo de direcionamento, já é atendido por diversos fabricantes, como podemos ver nos documentos abaixo relacionados:

Atendido por Symantec: https://help.symantec.com/cs/SMG_10_7_0/SMG/v72426555_v132085995/Content-filtering-notification-variables?locale=EN_US

McAfee e Trend informaram que atendem a esta configuração - (documento SEI n. 2337950 e documento sei n. 2338116).

5.22. Análise 21

Texto da Impugnação:

8. SOLUÇÃO DE PROTEÇÃO GATEWAY DE E-MAILS (ANTISPAM)

8.5.25. Permitir encaminhar as mensagens em cópia oculta para destinatário não inserido originalmente na mensagem;

Foi solicitada a remoção deste item.

Resultado: Não atendido e não removido!

Análise da equipe técnica de Planejamento da Contratação:

A equipe técnica entende que essa funcionalidade é muito básica e é bastante utilizada pelos usuários da instituição, atualmente, através das ferramentas de correio eletrônico. Por outro lado, a equipe de planejamento da contratação não é contrária à retirada desse item tornando-o mais ampliativo, mesmo entendendo que não se trata de um item restritivo ou que evidencie qualquer tipo de direcionamento, já é atendido por diversos fabricantes, como podemos ver nos documentos abaixo relacionados:

McAfee, Symantec e Trend informaram que atendem a esta configuração - (documento SEI n. 2337950 e documento sei n. 2338116).

5.23. Análise 22

Texto da Impugnação:

8. SOLUÇÃO DE PROTEÇÃO GATEWAY DE E-MAILS (ANTISPAM)

8.5.26. Permitir arquivar as mensagens sem que o remetente ou destinatário saibam para fins de auditoria;

Foi solicitada a remoção deste item.

Resultado: Não atendido e não removido!

Análise da equipe técnica de Planejamento da Contratação:

A equipe técnica entende que essa funcionalidade é muito básica e é bastante utilizada. Por outro lado, a equipe de planejamento da contratação não é contrária à retirada desse item tornando-o mais ampliativo, mesmo entendendo que não se trata de um item restritivo ou que evidencie qualquer tipo de direcionamento, já é atendido por diversos fabricantes, como podemos ver nos documentos abaixo relacionados:

McAfee, Symantec e Trend informaram que atendem a esta configuração - (documento SEI n. 2337950 e documento sei n. 2338116).

5.24. Análise 23

Texto da Impugnação:

8.7. ADMINISTRAÇÃO

8.7.6. Possuir recurso que faça uma monitoração do sistema, alertando o administrador caso haja falta de espaço em disco, se o serviço estiver indisponível e se a fila de mensagens chegarem a um número estabelecido como máximo pelo administrador;

Foi solicitada a alteração deste item para:

Possuir recurso que faça uma monitoração do sistema, alertando o administrador caso haja falta de espaço em disco.

Resultado: Não atendido e não modificado!

Análise da equipe técnica de Planejamento da Contratação:

A equipe técnica entende que essa funcionalidade é muito básica e é bastante utilizada, e oferecida em maior amplitude por diversos fabricantes.

Ainda, entendemos que não se trata de um item restritivo ou que evidencie qualquer tipo de direcionamento, já é atendido por diversos fabricantes, como podemos ver nos documentos abaixo relacionados:

McAfee, Symantec e Trend informaram que atendem a esta configuração - (documento SEI n. 2337950 e documento sei n. 2338116).

https://www.hscbrasil.com.br/materiais/manual_mli_v5_0_30-2.pdf?6e6543&6e6543 página 87.

Assim, a equipe técnica de planejamento da contratação manterá o texto, que é o mais simples possível frente aos diversos datasheets estudados, considerando que a funcionalidade de alertar o administrador em caso de indisponibilidade do serviço ou quando a fila de

mensagens atingir um número a sua capacidade máxima, é indispensável para que o administrador possa garantir a disponibilidade do serviço e realizar o troubleshooting (solução de problemas).

5.25. Análise 24

Texto da Impugnação:

8.7. ADMINISTRAÇÃO

8.7.8. Definição de timeout de conexão SMTP;

Foi solicitada a remoção deste item.

Resultado: Não atendido e não removido!

Análise da equipe técnica de Planejamento da Contratação:

A equipe técnica entende que essa funcionalidade é muito básica e é bastante utilizada, e oferecida em maior amplitude por diversos fabricantes.

Ainda, entendemos que não se trata de um item restritivo ou que evidencie qualquer tipo de direcionamento, já é atendido por diversos fabricantes, como podemos ver nos documentos abaixo relacionados:

É atendido por: https://support.kaspersky.com/KSMG/1.0/en-EN/90599.htm

É atendido por: https://help.symantec.com/cs/SMG_10_6_6/SMG/v27734759_v125807409/SMTP-Advanced-Settings--DeliverySMTP_delivery?locale=EN_US

É atendido por: https://www.hscbrasil.com.br/materiais/manual_mli_v5_0_30-2.pdf?6e6543&6e6543 página 151.

McAfee, Symantec e Trend informaram que atendem a esta configuração - (documento SEI n. 2337950 e documento sei n. 2338116).

5.26. Análise 25

Texto da Impugnação:

8.7. ADMINISTRAÇÃO

8.7.12. Possuir mecanismo de alerta específico para ataques do tipo Command & Control (C&C).

Foi solicitada a remoção deste item.

Resultado: Não atendido e não removido!

Análise da equipe técnica de Planejamento da Contratação:

O objetivo deste item é alertar a equipe de segurança quando existe a ameaça de ataques do tipo Command & Control (C&C). Por não ser um tipo de ataque novo no mundo da segurança da informação, o item foi exigido no Termo de Referência.

Por outro lado, a equipe de planejamento da contratação não é contrária à retirada desse item tornando-o mais ampliativo, mesmo entendendo que não se trata de um item restritivo ou que evidencie qualquer tipo de direcionamento, já é atendido por diversos fabricantes, como podemos ver nos documentos abaixo relacionados:

Symantec e Trend informaram que atendem a esta configuração - (documento SEI n. 2337950 e documento sei n. 2338116).

É atendido por: https://hscbrasil.com.br/materiais/hsc_mli_manual%20v5_x.pdf?15266a&15266a página 135.

5.27. Análise 26

Texto da Impugnação:

10. SOLUÇÃO DE PROTEÇÃO CONTRA AMEAÇAS AVANÇADAS

10.2. Sandbox customizada do tipo On-Premise com hardware físico homologado pelo fabricante ou em máquina virtual local;

Este item técnico não estava presente nas últimas versões de TR compartilhadas anteriormente pela equipe técnica da FUNASA. A exigência de: Sandbox customizada e On-Premise é muito restritiva e exclui a participação de fabricantes que utilizam infraestrutura de nuvem para análise de artefatos maliciosos e desconhecidos. Desta forma solicitamos que o texto seja modificado para flexibilizar o modelo de uso de Sandbox e proporcionar a participação de fabricantes que utilizam esta funcionalidade em nuvem.

Além disso a possibilidade de utilização da nuvem JÁ É POSSIBILITADA no processo vide:

*Imagem extraída do documento: Anexo do Termo de Referência SEI_FUNASA - 2405994 - especificação técnica.pdf

Como pode-se observar não há motivo para exigência de instalação local, seja física ou virtual do ambiente de Sandbox.

Tal exigência confirma o indevido favorecimento para a tecnologia da Trend Micro em caráter de exclusividade.

Análise da equipe técnica de Planejamento da Contratação:

A impugnante acusa a equipe de favorecer a um único fabricante de solução de segurança, porém não se utiliza de fatos concretos. Hoje, a Funasa utiliza a solução EDR (Sandbox + ATP) da Symantec de forma on-primisse. A equipe técnica deseja manter essa característica da solução, e por esse motivo, foi possibilitado que o licitante tenha a opção de compor com outras ferramentas caso não possua este serviço on-primisse.

Cabe mencionar que essa exigência não se trata de um item restritivo ou que evidencie qualquer tipo de direcionamento, já é atendido por diversos fabricantes, como podemos ver nos documentos abaixo relacionados:

Atendido por: https://help.symantec.com/cs/SymantecEDR_4.1/EDR/v123002272_v130949130/Configuring-Symantec-EDR-to-use-cloud-sandboxing-or-on-premises-sandboxing?locale=EN_US

Atendido por : https://www.checkpoint.com/downloads/products/sandblast-appliances-datasheet.pdf

Atendido por: https://www.bitdefender.com.br/business/enterprise-products/sandbox-analyzer.html.

Atendido por: https://www.mcafee.com/enterprise/pt-br/assets/data-sheets/ds-advanced-threat-defense.pdf

Atendido por:

https://e.huawei.com/br/related-page/products/enterprise-network/security/apt/firehunter6300/brochure/security_firehunter6300_en

Atendido por:

https://www.fortinet.com/content/dam/fortinet/assets/data-sheets/FortiSandbox.pdf

Atendido por:

https://www.fireeye.com/content/dam/fireeye-www/products/pdfs/pf/forensics/ds-malware-analysis.pdf

Atendido por:

https://www.cylance.com/content/dam/cylance/pdfs/data_sheets/CylanceSmartAntivirusDataSheet.pdf

Atendido por:

https://www.forcepoint.com/sites/default/files/resources/files/brochure_forcepoint_advanced_malware_detection_appliance_en.pdf

Atendido por:

https://www.crowdstrike.com.br/produtos-de-seguranca-de-endpoints/falcon-sandbox-malware-analysis/

Por outro lado, a equipe de planejamento da contratação com o intuito de ampliar o item tornando-o mais ampliativo irá alterar a redação para:

Item 10.2. Sandbox customizada do tipo On-Premise com hardware físico homologado pelo fabricante ou em máquina virtual local ou disponibilizada em serviço de nuvem. Caso o serviço seja disponibilizado na nuvem, a infraestrutura de nuvem da solução deverá ser operada em território brasileiro. Conforme a norma do Gabinete de Segurança Institucional (GSI) NC14/IN01/DSIC/GSIPR.

5.28. Análise 27

Texto da Impugnação:

10. SOLUÇÃO DE PROTEÇÃO CONTRA AMEAÇAS AVANÇADAS

10.7.31. Deve possuir capacidade de envio de artefatos para analisador virtual dedicado, externo, sendo que este deverá suportar no mínimo os sistemas operacionais Windows 7 e Windows 2012;

Foi solicitada a alteração deste item para:

Deve possuir capacidade de envio de artefatos para analisador virtual dedicado ou externo, sendo que este deverá suportar analise em Windows;

Resultado: Não atendido e não modificado!

Análise da equipe técnica de Planejamento da Contratação:

A sugestão enviada não foi acatada por não colaborar com a ampliação da competição, considerando que o requisito do Termo de Referência define uma faixa de versões na qual a solução de segurança deve funcionar (Windows 7 ou superior e Windows server 2012 ou superior).

O texto como sugerido pelo impugnante restringe amplamente a competição, considerando que ao alterar o texto para "deverá suportar analise em Windows", entende-se que deve ser suportada a análise em QUALQUER versão Windows, inclusive Windows 3.1, Windows 3.11 ou Windows NT.

Não sabemos exatamente se a solução representada pelo impugnante é capaz de cumprir tais requisitos, porém, caso ofereça tal funcionalidade, a sugestão poderia servir como uma armadilha para o oferecimento de recursos contra a análise das propostas dos concorrentes. Por outro lado, não interessaria para a Funasa tamanha amplitude de versões de Windows, já que a Funasa utiliza máquinas com Windows nas versões discriminadas, e superiores.

5.29. Análise 28

Texto da Impugnação:

10. SOLUÇÃO DE PROTEÇÃO CONTRA AMEAÇAS AVANÇADAS

10.7.37.6. Recomendações de Segurança;

Foi solicitada a remoção deste item!

Resultado: Não atendido e não removido!

Análise da equipe técnica de Planejamento da Contratação:

Analisando o item por completo, temos:

Deve possuir capacidade de geração de relatórios dos seguintes tipos e contendo as seguintes características:

Recomendações de Segurança;

A equipe técnica entende que essa funcionalidade é muito básica e é bastante utilizada. Por outro lado, a equipe de planejamento da contratação não é contrária à retirada desse item tornando-o mais ampliativo, já que é apenas uma boa prática e não compromete a segurança do parque tecnológico. Ainda, é preciso ficar claro que não se trata de um item restritivo ou que evidencie qualquer tipo de direcionamento, sendo atendido por diversos fabricantes, como podemos ver nos documentos abaixo relacionados:

McAfee, Symantec e Trend informaram que atendem a esta configuração - (documento SEI n. 2337950 e documento sei n. 2338116).

6. DOCUMENTOS RELACIONADOS

Nota Técnica 47 (2445447)

Pedido de Impugnação - Igor Homar (2458144)

Aviso de suspensão (2457217)

7. CONCLUSÃO

7.1. Conforme o exporto nos parágrafos anteriores, entendemos que as alterações das especificações técnicas da solução proporcionará a ampliação da competitividade do processo licitatório atendendo adequadamente as necessidades da Funasa e proporcionando maior economicidade na aquisição do produto. Vale ressaltar que estas mudanças não altera o preço estimado da contratação, não sendo necessária nova cotação de preços.

7.2. Segue o resumo das alterações efetuados no TR:

1. Item 4.6 teve redação alterada para: *4.6. Bloqueie por categoria ou aplicação, ou permita que os aplicativos sejam instalados através da console de gerenciamento, desde que, nesse caso, sejam atendidos pela contratada através do suporte técnico.*

2. Item 4.15 teve redação alterada para: 4.15. *Capacidade de configurar White e Black Lists de aplicativos ou Websites que impeçam o funcionamento de um aplicativo.*

Exemplo: Bloquear o website do Facebook e por consequência impedir o aplicativo do facebook de funcionar no dispositivo.

3. Item 8.4.23 Teve redação alterado para: *Prevenir contra ataques de SPAM, permitindo rejeitar a conexão ou mensagem quando exceder configuração personalizada para esse ataque;*

4. Item 8.5.1 *Removido.*

5. Item 8.5.9 *Removido.*

6. Item 8.5.10 *Removido.*

7. Item 8.5.21 teve redação alterada para: Enviar para quarentena.

8. Item 8.5.22 *Removido.*

9. Item 8.5.25 *Removido.*

10. Item 8.5.26 *Removido.*

11. Item 8.7.12 *Removido.*

12. Item 10.2 teve redação alterada para: *Sandbox customizada do tipo On-Premise com hardware físico homologado pelo fabricante ou em máquina virtual local ou disponibilizada em serviço de nuvem. Caso o serviço seja disponibilizado na nuvem, a infraestrutura de nuvem da solução deverá ser operada em território brasileiro. Conforme a norma do Gabinete de Segurança Institucional (GSI) NC14/IN01/DSIC/GSIPR.*

Documento assinado eletronicamente por **Darlan Henrique da Silva Venturelli**, **Integrante Requisitante**, em 26/10/2020, às 00:47, conforme horário oficial de Brasília, com fundamento no art. 6º, § 1º, do Decreto nº 8.539, de 8 de outubro de 2015.

Documento assinado eletronicamente por **Marcelo Dias de Sá**, **Integrante Técnico**, em 26/10/2020, às 09:09, conforme horário oficial de Brasília, com fundamento no art. 6º, § 1º, do Decreto nº 8.539, de 8 de outubro de 2015.

Documento assinado eletronicamente por **Túlio César de Araújo Porto**, **Integrante Técnico**, em 26/10/2020, às 10:15, conforme horário oficial de Brasília, com fundamento no art. 6º, § 1º, do Decreto nº 8.539, de 8 de outubro de 2015.

A autenticidade deste documento pode ser conferida no site https://sei.funasa.gov.br/consulta, informando o código verificador **2450824** e o código CRC **5982408C**.