Amanda da Solidade Silva

De: Igor homar <igorhomar86@gmail.com>
Enviado em: terça-feira, 20 de outubro de 2020 17:49
Para: Comissão Permanente de Licitação
Assunto: Impugnação de Edital - Pregão Eletrônico n. 16/2020 - Processo n. 25100.000.191/2020-64
Anexos: Impugnação FUNASA.pdf

Prezada Comissão de Licitações.

Sirvo-me do presente para apresentar a competente impugnação ao procedimento licitatório constante do:

Pregão Eletrônico n. 16/2020

Processo n. 25100.000.191/2020-64

Oportunidade em que colaciono a peça acostada em anexo, para que surtam os devidos fins de direito.

Ciente da compreensão de todos, pugnamos pelo deferimento da presente impugnação, oportunidade em que encerramos nossas ponderações com os votos da mais elevada estima e consideração

Att.

Igor Xavier Homar
OAB/GO nº 30.111
Telefone: (11) 94455-4343

ILUSTRÍSSIMO SENHOR PREGOEIRO DA FUNDAÇÃO NACIONAL DE SAÚDE

Pregão Eletrônico n. 16/2020
Processo n. 25100.000.191/2020-64

Igor Xavier Homar, brasileiro, casado, advogado, inscrito na Ordem dos Advogados do Brasil, Subseção de Goiás, sob o nº 30.111, portador do CPF/MF nº 019.419.151-67, com endereço profissional estabelecido à Rua Surubim, nº 577, CJ. 182/183, Brooklin, São Paulo-SP, vem respeitosamente à presença de V. Senhoria apresentar **IMPUGNAÇÃO** ao edital de licitação, o que faz na forma do item 24 do instrumento de convocação do aludido certame, pelos fatos e fundamentos a seguir aduzidos:

1. DA TEMPESTIVIDADE:

Inicialmente, imperioso se faz considerar que a presente peça se mostra tempestiva. O prazo para apresentar impugnação, conforme disposto no subitem 24.1 do instrumento de convocação da licitação, é de 3 (três) dias úteis anteriores à sessão de licitação, programada para 23/10/2020, sexta-feira. Dessa forma, o prazo, contado na forma do art. 110 da Lei n. 8.666/93, encerra-se em 20/10/2020.

2. DA IMPUGNAÇÃO:

A presente impugnação versará basicamente sobre os seguintes pontos:

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.

É o que se passa a expor.

2.1 Da necessidade de revisão do parcelamento do objeto – Custo de propriedade e premissas do Estudo Técnico Preliminar:

O primeiro tópico de impugnação refere-se à deficiência na forma de composição do objeto em disputa, o que, sob o pretexto de ampliar a competitividade, 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.

De acordo com o termo de referência, o objeto em disputa está separado em dois lotes. O lote 01 trata das soluções de EPP (*endpoint protection*), Antispam e EDR (proteção de ameaças avançadas), conforme redação dos itens 1 a 3, com os respectivos serviços de treinamento, suporte e implantação (itens 4 a 6).

A seu turno, de forma segregada, o lote 02 trata da solução de DLP (item 1), também com os serviços correspondentes (itens 2 a 4).

A separação do DLP da solução de EPP, a princípio, poderia ser considerada como uma vantagem competitiva, eis que, parcelando o objeto, permitiria que um número maior de empresas se apresentasse para a disputa. Ocorre que, no caso em tela, analisando as especificidades das soluções a serem adquiridas e do parque da FUNASA, percebe-se que,

em verdade, os efeitos são contrários ao que pretende a lei, já que, se se mantiver a disposição do edital, haverá claro prejuízo ao Erário.

Antes de examinar os fatos subjacentes, é bom que se examine o substrato normativo que está na base da interpretação. A Lei Federal n. 8.666/93 tem um princípio geral de parcelamento do objeto **quando for possível que assim se dê**, justamente com o objetivo de reduzir as exigências de habilitação e de ampliar o universo de competidores. Veja-se a lei:

> *Art. 23. (...)*
> *§ 1º As obras, serviços e compras efetuadas pela Administração serão divididas em tantas parcelas quantas se **comprovarem técnica e ECONOMIACAMENTE viáveis**, procedendo-se à licitação com vistas ao melhor aproveitamento dos recursos disponíveis no mercado e à ampliação da competitividade sem perda da economia de escala.*
> *(grifo nosso)*

Isso é o que consta da Súmula n. 247 do TCU, cuja redação trazemos à colação:

> ***SÚMULA TCU 247:** É obrigatória a admissão da adjudicação por item e não por preço global, nos editais das licitações para a contratação de obras, serviços, compras e alienações, cujo objeto seja divisível, **desde que não haja prejuízo para o conjunto ou complexo ou PERDA DA ECONOMIA DE ESCALA**, tendo em vista o objetivo de propiciar a ampla participação de licitantes que, embora não dispondo de capacidade para a execução, fornecimento ou aquisição da totalidade do objeto, possam fazê-lo com relação a itens ou unidades autônomas, devendo as exigências de habilitação adequar-se a essa divisibilidade.*
> *(grifo nosso)*

Passemos aos fatos.

No Estudo Técnico Preliminar (ETP), encontram-se as seguintes menções:

> *1. INTRODUÇÃO*
> *1.1. A presente análise tem por objetivo demonstrar a viabilidade técnica e econômica da solução centralizada de segurança do tipo endpoint protection (Antivírus/Antimalware) no âmbito da Fundação Nacional de Saúde - Funasa.*
> *1.2. Destaca-se que os contratos 36/2017, 50/2017 e 46/2018 foram firmados com vigência de 12 (doze) meses podendo ser prorrogados até 60 (sessenta) meses .*
> *1.3. Assim, o Estudo Técnico Preliminar tem por objetivo realizar uma análise detalhada sobre a viabilidade, ou não, da demanda gerada no documento 1907641de Monitoramento do Acórdão 2207/2018 – TCU – Plenário, prolatado no âmbito do TC 015.932/2018-4.*
> *2. DESCRIÇÃO DA SOLUÇÃO DE TECNOLOGIA DA INFORMAÇÃO*
> *2.1. Constitui objeto deste Estudo Técnico Preliminar a **solução centralizada de segurança do tipo endpoint protection - EPP**, no âmbito da Funasa,*

incluindo serviços de implementação, suporte técnico on-site, repasse de conhecimento hands-on.

2.2. O serviço deve ser provido por meio da implantação de tecnologia que possua capacidade de gerenciar de forma centralizada os clientes instalados nas estações de trabalho, utilizando-se de licença de sofware com função de Antivírus, Anti-Spyware, Firewall, Proteção Contra Intrusos (HIPS), Controle de Dispositivos, Controle de Aplicações, ***entre outras****. As licenças que serão ativadas nos servidores de gerência deverão ser flutuantes entre, no mínimo, dois nós em cluster e caso isso não seja possível, cada um dos componentes deve ser licenciado para que as funcionalidades permaneçam ativas no caso de indisponibilidade de um dos nós.*

3. JUSTIFICATIVA DA ARQUITETURA DA SOLUCÃO

3.1. A infraestutura de tecnologia da informação da Funasa conta com uma estrutura de firewall e proxy que constituem um aparato tradicional de segurança, destinados ao controle das comunicações entre redes e ao permissionamento de acesso a recursos, serviços e dados. Tais dispositivos, contudo, não garantem proteção contra infecção por malware, captura de informações privadas ou sigilosas, acesso indevido a serviços de rede por usuário não autorizado, dentre outras vulnerabilidades.

3.2. Para tratar especificamente de vírus, wormse spywares, a Rede da Funasa conta com uma solução de antivírus em camadas que constitui a barreira de proteção contra esses tipos específicos de malware. São os principais elementos dessa solução:

3.2.1. ***Gateway antivírus em formato "appliances" instalados na borda da rede****, responsáveis pela detecção de vírus nas mensagens de correio eletrônico recebidas da Internet antes que essas mensagens atinjam os servidores de correio eletrônico e as caixas postais dos usuários. Trata-se de uma primeira camada de defesa, que promove a desinfecção de mensagens contaminadas com vírus.*

3.2.2. ***Antivírus de servidor de correio eletrônico, instalado nos servidores Microsoft Exchange responsáveis pela entrega das mensagens às caixas postais dos usuários. Constitui uma segunda camada de proteção, uma vez que pode haver mensagens infectadas oriundas do ambiente interno da rede, que não passam pela detecção do antivírus de borda.***

3.2.3. Antivírus local, instalado em cada um dos cerca de 3.961 computadores da Rede Funasa, já incluídos notebooks de propriedade da Casa e 200 servidores virtuais.

3.2.4. A solução atual não possui uma Console de gerenciamento centralizada para a plataforma antivírus,a solução de DLP e solução de ataques avançados, logo, cada solução possui uma interface de monitoramento própria mesmo sendo do mesmo fabricante.

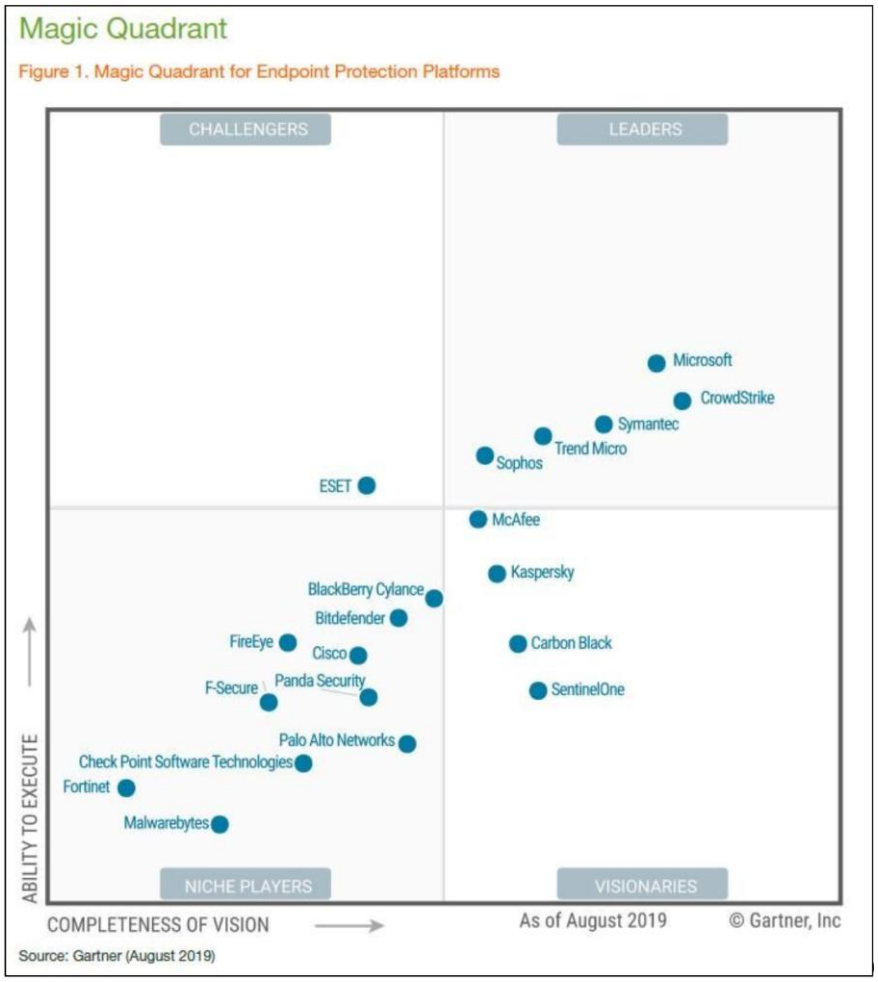
(...)

3.4. Trata-se de uma abordagem voltada às ameaças que privilegiam o ataque direto a esses computadores: ***contaminação por malware, intrusão em estação de trabalho, acesso indevido ou não autorizado a recursos de rede, perda ou vazamento de informações privadas ou confidenciais, vazamento de informações por perda de dispositivo móvel (notebook), uso não autorizado nas estações de trabalho de dispositivos de comunicação ou de armazenamento de dados que representam risco ao ambiente, dentre outras****. Mais que isso,* ***as soluções de segurança de Endpoint apresentam uma console integrada para todas essas ferramentas****, o que permite a criação e aplicação de políticas de segurança de Endpoint em nível corporativo envolvendo todas essas disciplinas citadas.*

3.5. ***O estudo proposto neste Projeto almeja avaliar uma solução que integre e consolide, sob o menor número possível de consoles de gerenciamento, as seguintes disciplinas de segurança de Endpoint:***

3.5.1. Antimalware (...).

3.5.2. Firewall pessoal (...).
3.5.3. Sistema Local de Prevenção de Intrusão (Host-based Intrusion Prevention System– HIPS) (...).
3.5.4. Controle de Acesso à Rede (Network Access Control– NAC) (...).
3.5.5. Prevenção de Perda de Dados Corporativos (Data Loss Prevention - DLP) (...)
3.5.6. Criptografia de unidades de armazenamento (discos rígidos) (...)
3.5.7. ***Seguindo as boas práticas de gerenciamento de segurança, todos os componentes devem ser de um mesmo fabricante e geridos sob console(s) de gerenciamentos desse mesmo fabricante****.* ***Não se deve aceitar soluções que congregam componentes de diversos fabricantes distintos, posto que isso atenta contra a integração e estabilidade da solução como um todo****.*
(...)
5. LEVANTAMENTO DAS ALTERNATIVAS (CENÁRIOS POSSÍVEIS)
5.1. ***O mercado de soluções de segurança com gerência centralizada para controle de ameaças em estações de trabalho apresenta diversos fabricantes*** *e soluções conforme pode ser visto em levantamento anual realizado pelo Gartner (Figura 1), acerca de soluções centralizadas de antivírus.*



5.1.1. Definição: "Uma Plataforma de Proteção de Endpoint (sigla em inglês EPP) é uma solução implantada em dispositivos endpoint para blindar endpoints, para evitar malwares e ataques mal-intencionados, e para fornecer a investigação e recursos de correção necessários para responder

dinamicamente a incidentes de segurança quando eles evadem controles de proteção.
5.1.2. O Gartner Quadrante Mágico de Plataformas de Proteção de Endpoints avalia soluções com ênfase na ***proteção, detecção de ataques avançados, ataques fileless e capacidade de resposta, favorecendo soluções fornecidas na nuvem que fornecem uma fusão de produtos e serviços****.*
5.1.3. O Gartner menciona também que soluções tradicionais de EPP são entregues através de um agente cliente gerenciado por um servidor de gerenciamento local, no entanto, soluções mais modernas usam a arquitetura nativa da nuvem e desloca o gerenciamento e parte da carga de trabalho de análise e detecção para a nuvem.
5.1.3.1. O Gartner estima que até 2025, as soluções EPP entregues em nuvem crescerão de 20% para 95% em novos negócios.
5.1.3.2. ***As soluções de DLP – Data Loss Prevention e criptografia, também são classificadas como parte de soluções de EPP****, mas segundo o Gartner são consideradas pelos compradores em um ciclo de compra diferente.*
(...)
6.3.2. Foi analisado que os fabricantes Trend Micro, Sophos e Mcafee oferecem a solução de DLP, EDR e Criptografia de disco no mesmo agente, ou seja, na aquisição de uma licença de EPP está incluso o licenciamento das funções de DLP e EDR. Hoje a Funasa possui um contrato para cada função.
6.3.3. Estudando o pregão do Banco Nacional de Desenvolvimento Econômico e Social (BNDES) que foi homologado no dia 22/02/2020, identificamos que o BNDES adquiriu a solução ***Symantec Protection Suite*** *V. 14 pelo valor global de R$ 526.704,00 por 24 meses, no escopo do termo de referencia e da proposta vencedora, encontramos o valor de R$ 90.75 por licença para estação de trabalho.*
(grifo nosso)

O que se extrai do ETP é que aguns dos objetivos buscados pela FUNASA são os seguintes:

a) observar as prescrições do Acórdão 2207/2018-Plenário do TCU, conforme item 1.3 (o que também toca na necessidade de adquirir solução contemplando o menor custo de propriedade possível);
b) adquirir ferramentas que contemplem uma ampla gama de ameaças tecnológicas (item 2.2);
c) proteger os servidores do Microsoft Exchange (subitem 3.2.2);
d) a possibilidade de redução da complexidade do gerenciamento das diversas tecnologias de proteção envolvidas, reduzindo o número de consoles empregadas para diminuir o custo humano de gerenciamento e as ferramentas de gerência instaladas (o item 3.5 fala em “menor número possível de consoles de gerenciamento”).

Entretanto, todas as premissas acima do ETP acabaram negadas pela formatação final do projeto. A primeira delas (econômica) está prejudicada pela aquisição separada das ferramentas de EPP e de DLP, a despeito de o próprio ETP ter afirmado que os líderes de mercado já trazem DLP embarcado em suas plataformas de EPP.

E por que isso é relevante? Porque a compra do DLP unificada com a solução de EPP traz **economia à Administração, reduzindo o TCO (*total cost of ownership*) ou custo total de propriedade (CTP)**.

Inclusive, um dos fundamentos principais do Acórdão 2207/2018-Plenário do TCU é justamente que a FUNASA busque avaliar **alternativas que permitam a redução do custo total de propriedade em seus projetos de TI**. A respeito, confira-se trecho do voto do Ministro Relator:

> *Em outro giro, não se pode perder de vista que a legislação exige, além da existência e demonstração da necessidade de cada contratação, que sua autorização seja precedida de uma avaliação, **em termos de custo (custo total de propriedade - CTP), das alternativas de mercado capazes de anteder à referida necessidade**. Não obstante, na única avença em que há indícios de necessidade da Funasa, tal obrigação foi desrespeitada, em potencial prejuízo aos cofres públicos.*
>
> *Ante o exposto, acolho parcialmente a lista de indícios de irregularidades cometidas pela equipe de planejamento da contratação (peça 102, p. 144), em relação ao seguinte:*
> *(...)*
> *3) ausência de avaliação do custo total de propriedade e do alinhamento da solução tecnológica com o objetivo da contratação (art. 12, III, da IN 4/2014 e art. 12, IV, 'b', da IN 4/2014)*
> *(...)*
> *Com as devidas vênias, deixo de acatar tal conclusão. Se, por um lado, são frágeis as justificativas para o não parcelamento constantes dos autos, consoante alertado pela Procuradoria da Funasa, a meu ver não se pode afirmar desde já que não haveria "óbice para a contratação de uma empresa para o fornecimento das licenças e outra para a operação assistida, o que aumentaria a competitividade do certame" (peça 102, p. 144) .*
> ***Entendo que o assunto afigura-se de elevada complexidade e requer estudo mais aprofundado, em especial quanto às práticas de mercado ou aos contornos técnicos do eventual parcelamento do objeto. Para se ter ideia da profundidade do tema, ressalto recente realização da auditoria sobre a contratação de licenças de software e práticas adotadas por grandes fornecedores de TI, TC030.236/2016-9, sob relatoria do e. Ministro Aroldo Cedraz.** Portanto, deixo de acolher, desde já, a conclusão de que a mencionada ausência de justificativas levou a prejuízos à Funasa.*
> *(Acórdão 2207/2018-Plenário, Rel. Min. Augusto Sherman, julgado em 19/09/2018, grifo nosso).*

Conforme há de se considerar, a separação da aquisição em EPP e DLP como lotes separados deixa de considerar que, como dito, as funcionalidades de DLP já estão embarcadas nas soluções líderes de mercado de EPP. Ou seja, com a aquisição de uma solução de EPP, o DLP já pode ser comprado, não havendo necessidade de compra separada e possivelmente sobreposta, o que **encarecerá a aquisição**.

Inclusive, na tabela do subitem 14.2.4 do ETP, descreve-se a solução de DLP como integrante do EPP, apontando-se um custo estimado de contratação de **R$ 3.198.990,83** para os 36 meses. Veja-se a transcrição:

ITEM	DESCRIÇÃO	Quantidade	Valor Estimado Unitário Otimista	Valor Estimado Total Otimista (Eo)	Valor Estimado Unitário Realista	Valor Estimado Total Realista ou Média (Em)	Valor Estimado Unitário Pessimista	Valor Estimado Total Pessimista (Ep)	Estimativa 3 Pontos (Eo+4*Em+Ep)
1	Solução centralizada de segurança do tipo Endpoint Protection Platform -EPP contendo (Antivírus/Antimalware), web reputation, firewall, IPS, controle de dispositivos, controle de aplicação, prevenção de vazamento de dados, EDR e Gerência centralizada, incluindo, garantia e atualização por 36 (trinta e seis) meses.	3.534	R$ 150,00	R$530.100,00	R$ 202,90	R$717.048,60	R$ 445,46	R$1.574.255,64	R$ 828.758,34
2	Solução de proteção gateway de e-mails (Antispam), incluindo garantia e atualização por 36 (trinta e seis) meses.	5.000	R$ 64,00	R$320.000,00	R$ 133,18	R$665.900,00	R$ 114,30	R$ 571.500,00	R$ 592.516,67
3	Solução de segurança para proteção de servidores virtuais, data center e nuvem, incluindo garantia e atualização por 36 (trinta e seis) meses	200	R$ 2.990,74	R$598.148,00	R$ 3.993,58	R$798.716,00	R$ 4.380,00	R$ 876.000,00	R$ 778.168,67
4	Solução de proteção contra ameaças avançadas, incluindo garantia e atualização por 36 (trinta e seis) meses	1	R$131.875,00	R$131.875,00	R$527.000,00	R$527.000,00	R$1.112.600,00	R$1.112.600,00	R$ 558.745,83
5	Serviço de treinamento da solução	4	R$ 9.800,00	R$ 39.200,00	R$ 10.555,00	R$100.417,52	R$ 10.625,00	R$ 42.500,00	R$ 80.561,68
6	Suporte técnico especializado	36	R$ 3.921,11	R$141.159,96	R$ 9.186,35	R$330.708,60	R$ 9.186,35	R$ 330.708,60	R$ 299.117,16
7	Serviço de Implementação e configuração das soluções - Item 1, 2, 3 e 4.	4	R$ 24.708,75	R$ 98.835,00	R$ 27.027,50	R$108.110,00	R$ 17.062,50	R$ 68.250,00	R$ 99.920,83
Valor Estimado Total para a solução de segurança para Endpoint (36 meses)									R$3.198.990,83
Valor Estimado Total para a solução de segurança para Endpoint (12 meses)									R$1.066.330,28

Por qual motivo está sendo feita a opção de se desprezar o cenário acima, cujo custo estimado é de **R$ 3.198.990,93**, em favor de uma divisão do objeto que aponta para um custo de **R$ 4.288.590,76** ? Qual é a avaliação de custo total de propriedade que admitiria esse incremento de valor estimado, desprezando o que o próprio ETP aponta ao

afirmar que "**os fabricantes Trend Micro, Sophos e Mcafee oferecem a solução de DLP, EDR e Criptografia de disco no mesmo agente"**?

Além do mais, não se pode deixar de destacar que essa forma de separação do objeto, não satisfeita com o incremento de mais de **R$ 1 milhão no custo** de aquisição total, deixa de atender a outra das premissas do ETP, que é a aquisição de proteção para as caixas postais do Microsoft Exchange Server, necessidade apontada pela própria FUNASA. Veja-se transcrição de trecho relevante do ETP:

3.2.2. Antivírus de servidor de correio eletrônico, instalado nos servidores *Microsoft Exchange* responsáveis pela entrega das mensagens às caixas postais dos usuários. Constitui uma segunda camada de proteção, uma vez que pode haver mensagens infectadas oriundas do ambiente interno da rede, que não passam pela detecção do antivírus de borda.

Ora, na tabela do subitem 14.2.4 do ETP, que, reiteramos, não se sabe por que foi abandonada, o custo total de **R$ 3.198.990,93** já incluía solução em item separado para proteção de servidores virtuais, datacenter e nuvem, com o estimado em **R$ 778.168,67**. Isso foi removido da versão publicada do edital, o que denuncia que não só houve incremento de custo estimado, mas redução da extensão das proteções a serem adquiridas.

Assim, o valor com a remoção do referido item de servidores deveria ter sido reduzido para R$ 2.420.822,26. Ocorreu, no entanto, o contrário, tendo sido verificado um aumento para R$ 4.288.590,76.

Pelo que se observa, nos salta aos olhos a constatação de que ao prosseguir com o certame nos moldes publicados, a FUNASA pretende gastar mais e comprar menos, o que não merece prosperar e contraria a efetiva utilidade do procedimento licitatório.

A se acrescentar ao alegado, há, ainda, o problema de gerência, constituindo a terceira violação a premissa do ETP. Como formatado o processo de aquisição, as ferramentas serão as seguintes:

- Uma console para o item 1 do lote 1;
- Uma console para o item 2 do lote 1 (podendo essa ser de fabricante distinto dos itens 1 e 3);
- Uma console para o item 3 do lote 1;
- Uma console para o item 1 do lote 2.

Mas isso contraria, como já indicado, trechos do ETP. Veja-se o que ampara a aquisição:

3.2.4. A solução atual não possui uma Console de gerenciamento centralizada para a plataforma antivírus,a solução de DLP e solução de ataques avançados, logo, cada solução possui uma interface de monitoramento própria mesmo sendo do mesmo fabricante.

3.4. Trata-se de uma abordagem voltada às ameaças que privilegiam o ataque direto a esses computadores: contaminação por malware, intrusão em estação de trabalho, acesso indevido ou não autorizado a recursos de rede, perda ou vazamento de informações privadas ou confidenciais, vazamento de informações por perda de dispositivo móvel (*notebook*), uso não autorizado nas estações de trabalho de dispositivos de comunicação ou de armazenamento de dados que representam risco ao ambiente, dentre outras. Mais que isso, as soluções de segurança de *Endpoint* apresentam uma console integrada para todas essas ferramentas, o que permite a criação e aplicação de políticas de segurança de *Endpoint* em nível corporativo envolvendo todas essas disciplinas citadas.

3.5. O estudo proposto neste Projeto almeja avaliar **uma solução que integre e consolide, sob o menor número possível de consoles de gerenciamento,** as seguintes disciplinas de segurança de *Endpoint*:

Ou seja, na atual configuração do edital, ter-se-á um cenário pior do que já havia na FUNASA, com a necessidade de se operarem **quatro consoles de gerenciamento distintas ao invés das três consoles anteriores**.

Esse parcelamento, portanto, como demonstrado, atenta a um só tempo contra a técnica e contra a economicidade do processo.

E a justificativa usada para que se parcele a aquisição (tabela 11 do ETP), data máxima vênia, também se mostra equivocada. Ao citar o processo do PE 05/2016-AGU, a FUNASA se equivoca porque despreza o fato de que, naquela licitação, **a separação se deu entre o EPP e o *Anti-Spam***. O DLP não foi comprado de forma apartada e nem se deixou de proteger os servidores.

Essa forma de segregação (EPP com EDR, DLP e outros num lote e Anti-Spam em outro) pode ser realizada sem problemas, até porque contempla fabricantes que apenas trabalham com soluções de Anti-Spam. Mas o parcelamento previsto neste edital, como demonstrado, além de antieconômico, viola a boa técnica e desfaz as bases em que se ampara o Estudo Técnico Preliminar da própria FUNASA, atentando contra as prescrições trazidas pelo Acórdão 2207/2018-Plenário do TCU.

2.2 Do direcionamento

É importante salientar que mediante análise do ETP é constatado que somente empresas representantes da tecnologia TREND MICRO enviaram cotações à época de pesquisa de mercado, até mesmo porque nenhum outro fabricante atenderia as especificações técnicas como demonstraremos a seguir.

- All tech Soluções: https://alltechsolucoes.com.br/
- SafetyWare: https://www.safetyware.com.br/
- IT Protect: https://www.trendmicro.com/pt_br/about/newsroom/press-releases/2018/cio-meeting.html
- Zillion: https://zillion.com.br/

Aludida restrição injustificada da competitividade, reforça o direcionamento na medida em que o registro constante no ETP (SEI_FUNASA - 2378042 - Estudo Técnico Preliminar da Contratação.pdf) sobre a única tecnologia testada no ambiente da FUNASA, quando no estudo de mercado, nos orienta *"ipsis verbis"*:

5.5. **Cenário 3 - Aquisição de uma nova Solução Antivírus**

Cenário 3 - Aquisição de Solução de Antivírus	
Entidade/Fornecedor:	Trend Micro
Descrição:	Solução de segurança para proteção de endpoint e data center
Análise da Solução:	1. Foi avaliada a solução da Trend Micro: • Smart Protection for Endpoints, antivírus que oferece proteção para diversos ambientes (computadores, Mac, Linux, iOS e Android); • TM Interscan Messaging Virtual Appliance - Solução de Antispam; • Deep Security - Solução de segurança contra ameaça avançada para data center; 2. Podemos destacar os seguintes pontos observados durante a PoC realizada pela Equipe de Segurança da Informação da, conforme documento SEI nº 1909638: 2.1. Implementação fácil, pois as opções e recursos da solução são intuitivos para quem já possui experiência no gerenciamento de Endpoint Protection Platform (EPP); 2.2. A interface da console de gerenciamento e do agente mostrou-se clara no quesito usabilidade, o que facilitou a configuração e criação de regras e tarefas; 2.3. Não houve problema para realizar a instalação dos agentes nas estações de trabalho; 2.4. A console de gerenciamento de eventos permitiu a identificação, visibilidade e controle (podendo até efetuar bloqueios) sobre todos os softwares instalados nas estações de trabalho; 2.5. Durante a varredura, a solução foi capaz de identificar se os arquivos e/ou pastas já tinham sido modificados desde a última verificação; 2.6. A ferramenta, ainda, permite definir o período em que os arquivos serão novamente verificados; 2.7 Para atender alguns requisitos, como, por exemplo, o bloqueio por tipos de arquivos em dispositivos USB, seria necessário implementar outra solução de segurança para executar essa atividade. 2.8 A solução de segurança Trend Micro representa uma solução de segurança que atende os requisitos mínimos de segurança. 2.9 A aquisição desta solução de antivírus implica em custos adicionais necessários de implementação e repasse de conhecimento para os profissionais que ficariam responsáveis pela administração da solução.

Imagem extraída do documento: SEI_FUNASA - 2378042 - Estudo Técnico Preliminar da Contratação.pdf

Foram várias tentativas de tornar a tecnologia SOPHOS (e as demais) aderente com as especificaçoes técnicas mínimas que possibilitassem competitividade. No entanto não houve alteração nas sugestões solicitadas conforme detalharemos a seguir:

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 alteraçao 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!

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!

4. MÓDULO DE PROTEÇÃO PARA DISPOSITIVOS MOBILE:

4.5. Deve monitor os aplica□vos 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!

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!

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!

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!

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!

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), remtentes e destinatários;

Resultado: Não atendido e não modificado!

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!

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!

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!

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!

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!

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!

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!

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!

8.5.10. Permitir inserir variáveis nas notificações, onde informem:

Foi solicitada a alteração deste item para:

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

Resultado: Não atendido e não modificado!

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!

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

Foi solicitada a alteração deste item para:

Permitir filtrar ações para mensagens fora do padrão;

Resultado: Não atendido e não modificado!

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!

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!

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!

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!

8.7.8. Definição de timeout de conexão SMTP;

Foi solicitada a remoção deste item.

Resultado: Não atendido e não removido!

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!

10. SOLUÇÃO DE PROTEÇÃO CONTRA AMEAÇAS AVANÇADAS

10.2. Sandbox customizada do tipo On-Premise com hardware fisico 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 utilizaçao da nuvem JÁ É POSSIBILITADA no processo vide:

REQUISITOS TECNOLÓGICOS

I - As soluções que compõe o item 01 devem ser do mesmo fabricante.

II - A solução do item 02 poderá ser de um fabricante diferente do item 01 e 03.

III - A solução do item 03 deverá ser on primise (local). As análises podem ser complementadas utilizando recursos na nuvem da solução, onde será permitido apenas o envio de metadados dos artefatos sob análise, sem submissão do artefato em si ou seu conteúdo à nuvem.

1. **Solução de gerenciamento**

1.1. A solução de gerenciamento deverá ser feita através de uma central única, baseada em web e em nuvem, que deverá conter todas a fermentas para a monitoração e controle da proteção dos dispositivos;

1.2. A solução de gerenciamento centralizado deve permitir a integração com a solução de segurança para proteção de endpoint;

1.3. Possuir plataforma de gerenciamento em servidor nos seguintes sistemas operacionais:

1.3.1. Plataforma Microsoft: Windows Server 2012, 2016 (64bits) e superior ou;

1.3.2. Plataforma Linux (32 e 64 bits) Centos;

Imagem extraída do documento: Anexo do Termo de Referência SEI_FUNASA - 2405994 - especificaç¦o 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.

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;

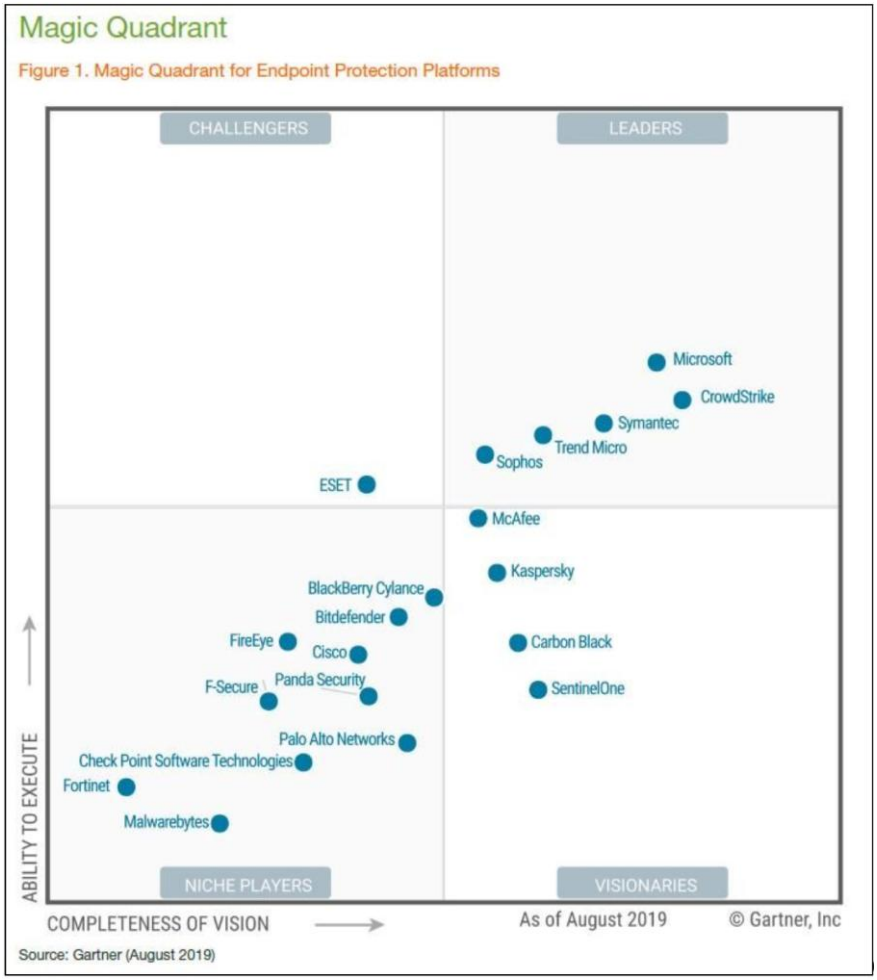
Resultado: Não atendido e não modificado!

10.7.37.6. Recomendações de Segurança;

Foi solicitada a remoção deste item!

Resultado: Não atendido e não removido!

Essas exigências todas, pela forma como previstas, excluem da competição empresas líderes de mercado de acordo com o Quadrante Mágico do Gartner Grup, que, para as soluções de EPP, conforme constante do ETP do edital, são as seguintes:



Mas há outro problema: a segregação do DLP em lote apartado, além de ser antieconômica (incrementando custo de gestão e impondo a compra sobreposta de função que já está embarcada nas tecnologias de EPP), impede a participação de importantes fabricantes do mercado.

O TCU preconiza justamente que as licitações sejam norteadas pela fixação de exigências tecnológicas que permitam que **um amplo conjunto de soluções atendam à demanda**. Veja-se o precedente:

Enunciado

> *No planejamento de suas aquisições de equipamentos, A ADMINISTRAÇÃO DEVE IDENTIFICAR UM CONJUNTO REPRESENTATIVO DOS DIVERSOS MODELOS EXISTENTES NO MERCADO QUE ATENDAM COMPLETAMENTE SUAS NECESSIDADES ANTES DE ELABORAR AS ESPECIFICAÇÕES TÉCNICAS E A COTAÇÃO DE PREÇOS, de modo a caracterizar a realização de ampla pesquisa de mercado e evitar o direcionamento do certame para modelo específico pela inserção no edital de características atípicas.*
> *(TCU, Acórdão 2829/2015-Plenário, Rel. Min. Bruno Dantas, julgado em 04/11/2015, destaque nosso).*

Dessa maneira, em se tratando de itens restritivos e que limitarão a competição frustrando o objetivo de obtenção da melhor proposta para a Administração, entende-se que a melhor solução é a suspensão desta licitação, reforma do termo de referência e republicação deste edital reposicionando a demanda de DLP e eliminando as características restritivas dos itens de Endpoint protection, Anti-Spam, Ameaças Avançadas (ATP) e DLP apontados acima, sob pena de indevido prejuízo ao erário.

3.CONCLUSÃO

Diante do exposto, pugna-se pela suspensão da presente licitação, oportunidade em que pugnamos pela modificação dos itens do edital supra impugnados, especialmente no que tange à definição do parcelamento do objeto e a reformulação das especificações técnicas dos itens de Endpoint protection, Anti-Spam, Ameaças Avançadas (ATP) e DLP, atentando-se ao previsto no art. 21, § 4º, da Lei n. 8.666/93, garantindo o atendimento integral e competitividade por diversos fabricantes/tecnologias de mercado de maneira isonômica.

Vale salientar que, mediante a continuidade do processo nos moldes em que se encontra, iremos acionar os órgãos de auditoria e controle a fim de evitar prejuízo para a Adminstração Pública, decorrente de direcionamento e sobrepreço praticados.

Nesses Termos,
Pede Deferimento.

Brasília, 20 de outubro de 2020.

Igor Xavier Homar
OAB/GO Nº 30.111