## Pregão Eletrônico

- **Visualização de Recursos, Contrarrazões e Decisões**

**RECURSO :**

ILMA SENHORA PREGOEIROA DA FUNDAÇÃO NACIONAL DE SAÚDE - FUNASA

PREGÃO ELETRÔNICO nº 19/2020 – FUNASA

ALLTECH SOLUÇÕES EM TECNOLOGIA LTDA., empresa de direito privado, com sede no SCN Quadra 1 Bloco F Salas 1201/1220 – Ed. America Office Tower – Asa Norte, Brasília/D.F., inscrita sob o CNPJ: 21.547.011/0001-66, por seu representante legal, vem mui respeitosamente à presença de V. Sas, apresentar, RECURSO ADMINISTRATIVO contra a decisão desta Comissão julgadora, que classificou a proposta da empresa GLOBAL IP TECNOLOGIA DA INFORMACAO LTDA, pelos fundamentos de fato e de direito a seguir aduzidos.

I. DA TEMPESTIVIDADE

Conforme determinado em Edital, o prazo para interposição deste recurso vence em 22 de janeiro de 2021, Sexta-feira, o que compreende 3 (três) dias após aceite de manifestação de recurso.

II. DOS FATOS

A FUNASA, publicou o Edital no. 19/2020, tornando público o Pregão Eletrônico do tipo menor preço, tendo por objeto o Registro de Preço para contratação de licenciamento
de solução de segurança para proteção de estações de trabalho (“Endpoint”) 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.

Dentre todas as licitantes participantes do presente pregão, a empresa GLOBAL IP TECNOLOGIA DA INFORMACAO LTDA foi declarada vencedora para o fornecimento da solução com o menor valor; porém, sem que houvesse atendimento às exigências do edital, conforme será demonstrado.

III. DOS FUNDAMENTOS

A seguir, a recorrente enumera os fundamentos que, tem-se a firme convicção, ensejam a desclassificação da proponente GLOBAL IP TECNOLOGIA DA INFORMACAO LTDA, doravante simplesmente recorrida:

a) Não atendimento as especificações técnicas exigidas pelo Termo de Referência.

b) Não atendimento aos requisitos de qualificação técnica exigidos pelo Edital;

Por partes.

a) - Não atendimento as especificações técnicas exigidas pelo Termo de Referência.

Diante da vacuidade da proposta apresentada apela recorrida à Coordenação de Licitações dessa Pública Administração solicitou análise técnica e emissão de parecer detalhado quanto a documentação apresentada pela recorrida no dia 13/01/2021, em razão da complexidade de informações contidas na documentação enviada inicialmente.

A empresa GLOBAL IP TECNOLOGIA DA INFORMACAO LTDA foi declarada vencedora para o fornecimento da solução com o menor valor; porém, foi classificada sem que houvesse atendido às exigências do edital.

Conforme modelo de proposta e exigências ao longo do Edital e Termo de referência, o licitante deveria apresentar em conjunto com sua proposta, a planilha para “Verificação Ponto a Ponto – Especificação técnica” consoante com os produtos/serviços ora apresentados.

Conforme exposto, os pontos referentes às especificações técnicas abaixo transcritas do Termo de Referência, não foram atendidas pela solução ofertada. Complementa-se que não foram encontradas na documentação apresentada:

1) Funcionalidades de Console Centralizada expondo ao cliente uma administração em várias consoles e uma não integração de eventos.
2) Diversas funcionalidades requeridas de Host IPS (HIPS) não documentadas, expondo o cliente à exploração de vulnerabilidades;
3) Diversas funcionalidades requeridas de Application Control não documentadas, expondo o cliente à utilizaçao de softwares não autorizados;
4) Diversas funcionalidades requeridas de EDR não documentadas, expondo o cliente ao desconhecimento em caso de ataques bem sucedidos, prejudicando a investigação pós incidente;
5) A funcionalidade de Sandbox apresentada não é customizável como requerido pelo edital, desta forma artefatos maliciosos submetidos à sandbox podem escapar com técnicas de evasão deste tipo de ambiente;
Em suma, há diversos itens de proteção contra ameaças avançadas que não atendem o requerido em edital, desta forma fica prejudicada a proteção contra ameaças ditas avançadas;

Senão vejamos:

1) Em atenção ao item sub item 1.1, item 1 do Anexo I do Termo de Referência, onde se lê "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;", resta claro, em análise da documentação proposta como comprovatória (documento "5-Endpoint Security Administration Guide R80.30.pdf") que não há a funcionalidade de gerência centralizada e única dos produtos propostos, uma vez que o a referia documentação fala apenas em alta disponibilidade (o título consta como "Management High Availability" – "Alta disponibilidade de gerenciamento" em tradução livre) e o texto introdutório deixa claro que se fala de alta disponibilidade do banco e redundância. Desta forma, a existência de múltiplas consoles dificulta visualização de logs e eventos de segurança pelo time da FUNASA, dificultando o entendimento holístico de eventos de segurança;

2) Em atenção ao item 5 do Anexo I do Termo de Referência, onde se lê "Módulo para proteção de vulnerabilidades e Host IPS (HIPS)", não fica claro nas documentações comprobatórias o atendimento dos itens 5.1, 5.2, 5.3, 5.4, 5.5, 5.6, 5.7, 5.9, 5.10 e 5.11, constando apenas um comparativo entre versões comerciais (há de se observar a diversos tópicos propondo a demonstração bem como links para páginas de caráter comercial). Consta-se ainda a ausência de comprovação técnica propriamente dita para cada um dos sub itens listados anteriormente.

A presença da funcionalidade para proteção de vulnerabilidades é essencial, visto que a maioria dos ataques ciber criminosos utiliza-se da exploração de vulnerabilidades para a execução de artefatos maliciosos, exploração e elevação de credenciais e outras técnicas maliciosas;

3) Em atenção ao item 6 do Anexo 1 do Termo de Referência, onde consta "Módulo para Controle de Aplicações", na documentação entregue ("2-CP_R80.30_GA_EndpointSecurity_AdminGuide") não fica comprovada a possibilidade de aplicação da política de Controle de Aplicações para os alvos desejados, conforme descrito no Termo de Referência nos sub itens 6.1, 6.2 e 6.3. A não presença de comprovação do referido item gera dúvidas quanto à real possibilidade de seleção de destinos a este tipo de política de segurança;

4) Ainda sobre o item 6, sub item 6.4, do Anexo 1 do Termo de Referência, não há presença na documentação apontada a possibilidade de verificação de logs do referido módulo de proteção, impossibilitando assim a visualização dos eventos e consequente entendimento de eventos de segurança que eventualmente venham a acontecer.

A necessidade de módulo de controle de aplicações se deve ao fato de que nem sempre aplicações indesejadas são consideradas vírus/malwares/artefatos maliciosos, como por exemplo mineradores de cripto moedas, aplicações de jogos, P2P (peer-to-peer) e outras indesejadas ao ambiente corporativo, permitindo um maior controle do parque computacional;

5) Ainda em atenção ao item 6, sub item 6.7, não há na documentação a possibilidade de execução de aplicações desejadas apenas como coleta de evento sem a efetiva aplicação da regra, uma vez que a documentação resta clara em que as possibilidades são "Allowed applications" e "blocked applications" ("aplicações permitidas" e "aplicações bloqueadas" em tradução livre).

Este tipo de execução de regra é essencial quando há o desconhecimento do analista responsável dos tipos de aplicações existentes no parque (cenário comum em início de operações de novas ferramentas, por exemplo), o que reduz o impacto ao usuário final de bloqueios indevidos, mas também permite que alguns usuários possam executar determinadas aplicações com conhecimento do administrador através dos logs gerados;

6) No item 7 e seus sub itens 7.2 e 7.5 do Anexo I do Termo de Referência, fica, além de não comprovada a existência de funcionalidade de Endpoint Detection and Response (EDR), a dúvida se este módulo de fato existe na solução ofertada, uma vez que as documentações apontadas como comprobatórias se referem à soluções de "Media Encryption & Port Protection", e "Application Control" conforme se observa no canto superior direito das páginas apontadas, onde indica-se o assunto de que trata-se a seção. Como comprovação adicional, também apontamos que a própria especificação desejada nestes sub itens não consta comprovada nas páginas indicadas;

7) Ainda em se tratando do item 7 do Anexo I do Termo de Referência, mas desta vez sobre o sub item 7.3, não resta claro na documentação que o relatório forense coletará todos os dados dos artefatos analisados.

A coleta destes dados se faz necessário para que o administrador tenha em mãos todas as informações sobre o evento de segurança para que possa entender com precisão os artefatos envolvidos no incidente, e possa tomar decisões acertadas. A falta destas informações prejudica, gerando lacunas de conhecimento;

8) Em atenção ao item 8, sub itens 8.2 e 8.7.41 do Anexo I do Termo de Referência, que comporta o seguinte título "Solução De Proteção Contra Ameaças Avançadas", não fica comprovada a possibilidade de personalização/customização da sandbox, muito pelo contrário, visto que tal documento deixa claro na tabela apresentada "Emulation Specifications" ("Especificações de Emulação" em tradução livre) as possibilidade de apenas se utilizar os sitemas operacionais Microsoft Windows XP e Windows 7, além de uma pequena compatibilidade de tipos de arquivos.

Pesa ainda o fato de que a comprovação do sub item 8.7.41 faz referência apenas à "Centralized Monitoring" ("Monitoramento Centralizado" em tradução livre), não constando informações sobre sandbox, que pertence à um componente totalmente diferente.

Entendemos que uma sandbox customizável deve oferecer a possibilidade de suportar diversos sistemas operacionais a escolha do usuário, papel de parede, hora, língua, programas instalados, bem como diversos tipos de arquivos e extensões, entre outros fatores. Isto se faz necessário para que haja a mitigação de técnicas de evasão de sandbox, onde o artefato suspeito percebe que está sendo testado em um ambiente controlado e permanece inerte, gerando um falso negativo, e consequentemente, a liberação deste para o usuário, expondo assim o ambiente corporativo a um artefato potencialmente muito danoso, visto que este já foi testado por outras camadas de segurança antes de sua submissão à sandbox;

9) Ainda em atenção ao item 8 do Anexo I do Termo de Referência, apontamos que a documentação entregue não

comprova o atendimento dos itens 8.7.16, 8.7.20 e 8.7.25, não havendo descrição de análise dos protocolos e tipos de arquivos solicitados. Destacamos ainda que a documentação "7-CP_R80.40_EndpointSecurity_AdminGuide", apresentada para o item 8.7.16, em sua seção apontada na documentação comprovatória (página 121), consta como "External Endpoint Policy Servers", que conforme ela própria explica na página 119, funciona como replicador de políticas de segurança, e não como sandbox, como assim desejado na especificação do Item;

10) Ainda em referência ao item 8, mais especificamente ao sub item ao 8.7.25, não há menção alguma à detecção baseada no verdadeiro tipo de arquivo (True File Type), conforme solicitado.

Esta diferenciação do verdadeiro tipo de arquivo é importante visto que uma técnica comum por atacantes é mascarar a real extensão do artefato malicioso com outra extensão, visando enganar e burlar agentes de segurança (por exemplo, um arquivo executável com extensão .exe é maquiado para parecer um arquivo de texto com extensão .docx);

11) Em atenção ao item 8, sub item 8.7.42, não resta comprovado a identificação de comunicação maliciosas em dispositivos móveis. Tal identificação é de suma importância, visto que a existência de tais dispositivos em redes corporativas é natual na era em que vivemos, sejam eles dispositivos de propriedade da FUNASA ou do próprio individuo, visto que o advento da consumerização de Tecnologia trouxe este fenômeno consigo. A não identificação gera um vácuo na detecção de ameaças, expondo e aumentando a superfície de ataque disponível à um atacante;

12) No sub item 8.7.46 do item 8 do Anexo I do Termo de Referência, em consoância com o descrito no tópico 8 deste documento, a descrição comprovatória se refere à Centralized Monitoring" ("Monitoramento Centralizado" em tradução livre), o que não condiz com a especificação técnica solicitada, que é a detecção de tentativas de ataque do tipo brute-force, uma metodologia muito comum em ataques cibernéticos, onde é realizada uma abordagem de tentativa e erro massiva até que se encontre, em algum momento a combinação desejada;

13) Consta ainda no sub item 8.7.59. do mesmo item 8 do Anexo I do Termo de Referência, a necessidade de encaminhamento dos logs gerados à ferramentas de syslog, algo indispensável às administrações de ativos computacionais. No entanto, não resta provado na documentação "2-CP_R80.30_GA_EndpointSecurity_AdminGuide" a existência de envio à este tipo de ferramenta externa. Salientamos ainda que a documentação se refere à um produto de segurança para endpoint e não para Ameaças Avançadas conforme solicitado em especificação técnica (isto pode ser notado no rodapé da página apontada onde lê-se "Endpoint Security Administration Guide" e no canto superior direito, indicativo da seção do documento, "Using SmartEndpoint";

b) - Não atendimento aos requisitos de qualificação técnica exigidos pelo Edital;

Diante da documentação de habilitação anexada pela empresa GLOBAL IP TECNOLOGIA DA INFORMACAO LTDA, em momento prévio ao certame, verifica-se que a mesma não atende aos requisitos de qualificação técnica mínimos exigidos pelo Edital.
De acordo com o Edital, item 9.11 "Qualificação Técnica":

9.11.1. Comprovação de aptidão para a prestação dos serviços em características,
quantidades e prazos compatíveis com o objeto desta licitação, ou com o item pertinente, mediante a apresentação de atestado(s) fornecido(s) por pessoas jurídicas de direito público ou privado.
9.11.1.1. Para fins da comprovação de que trata este subitem, os atestados deverão dizer respeito a serviços executados com as seguintes características mínimas:
9.11.1.1.1. Comprovação de aptidão para a prestação dos serviços em características e prazos compatíveis com o objeto desta licitação, ou com o item pertinente, por período não inferior a um ano, mediante a apresentação de atestados fornecidos por pessoas jurídicas de direito público ou privado.
9.11.1.1.2. Somente serão aceitos atestados expedidos após a conclusão do contrato ou se decorrido, pelo menos, um ano do início de sua execução, exceto se firmado para ser executado em prazo inferior, conforme item 10.8 da IN SEGES/MPDG n. 5, de 2017;
9.11.1.1.3. Para a comprovação da experiência mínima de 1 (um) ano, é admitida a apresentação de atestados referentes a períodos sucessivos não contínuos, não havendo a obrigatoriedade do um ano ser ininterrupto, conforme item 10.6.1 do Anexo VII-A da IN SEGES/MPDG n.5/2017;
[...]
9.11.1.1.6. O atestado de capacidade técnica deve atender no mínimo 20% do quantitativo exigido para os itens do Termo de Referência.

De acordo com os itens de habilitação técnica especificados em Edital, o licitante deveria anexar atestados de capacidade técnica comprovando que forneceu solução centralizada de segurança do tipo Endpoint Protection( Item 1), bem como solução de proteção contra ameaças avançadas(Item 2) em quantidade mínima de 20% ao exigido para os itens do Termo de Referência.
Ao analisarmos os documentos anexados pela empresa Global IP, identificam-se dois atestados de capacidade técnica nomeados como "Atestado ANTT endpoint.pdf" e "Atestado banco do brasil Endpoint.pdf", respectivamente.
Em referência ao primeiro documento mencionado, verifica-se que a empresa em questão forneceu à ANTT no ano de 2012, soluções de segurança para endpoint e para e-mails (anti-spam) da fabricante SYMANTEC, em quantidade superior aos 20% exigidos. No segundo atestado apresentado, a empresa forneceu ao Banco do Brasil em 2010, licenças para proteção de endpoint da marca CHECKPOINT, com funcionalidades similares ao primeiro atestado apresentado. Tais confirmações se dão com base em consulta ao portal dos fabricantes, citados abaixo:

1) https://www.broadcom.com/products/cyber-security/endpoint
2) https://docs.broadcom.com/docs/mail-security-for-microsoft-exchange-en
3) https://www.checkpoint.com/products/media-encryption/
4) https://sc1.checkpoint.com/documents/R80.40/SmartEndpoint_OLH/EN/Content/Topics-EPSG/FDE-CPFDE-intro.htm

Ao analisarmos os atestados apresentados frente à exigência do edital, o qual trata de duas soluções distintas, segurança para endpoint(Item 1) e segurança para ameaças avançadas(Item 2), verifica-se uma lacuna na documentação enviada para qualificação técnica da empresa GLOBAL IP TECNOLOGIA DA INFORMACAO LTDA.
Ambos atestados apresentados, tratam-se especificamente de soluções RESTRITAS à segurança para endpoints. Assim, confirma-se que a empresa em questão não comprou capacidade técnica anterior e, portanto, não está apta a fornecer os produtos e serviços relacionados à solução de ameças avançadas.
Assim posto, a recorrida GLOBAL IP TECNOLOGIA DA INFORMACAO LTDA deve ser desclassificada do presente Pregão, considerando que além da solução ofertada não atender os mínimos requisitos técnicos contidos no Anexo ao Termo de Referência, a mesma não comprovou capacidade técnica para fornecer a solução para ameaças avanças nos termos do subitem 9.11 do Edital.

IV. CONCLUSÃO
Em face do exposto, pela imperiosidade dos princípios administrativos supra suscitados, requer a recorrente:

1) o provimento do presente recurso, para desclassificar a proponente GLOBAL IP TECNOLOGIA DA INFORMACAO LTDA, em face das irregularidades acima noticiadas.

Caso não seja esse o entendimento de V. Sa., requer que o presente recurso seja encaminhado a Autoridade Superior, nos termos do § 4º, do art. 109, da Lei 8.666/93, para apreciação na forma da Lei.

Nestes termos,
Pede deferimento.

Brasília-DF, 22 de janeiro de 2021.

ALLTECH SOLUÇÕES EM TECNOLOGIA LTDA
Murilo Rossetto
Diretor

Fechar