ESTADO DO RIO GRANDE DO SUL
SECRETARIA DA FAZENDA
DEPARTAMENTO DE TIC
GABINETE

PROA: 23/1400-0008814-6
Assunto: Análise técnica habilitação – PE 9097/2024

Porto Alegre, 04 de junho de 2024.

Prezado pregoeiro,

Em relação à manifestação da empresa FAST HELP INFORMÁTICA LTDA, em resposta à análise técnica deste órgão, e em face da complementação de documentação técnica, temos o que segue:

- **Contrato ADASA:**

Conforme extraído da página 10 da manifestação da licitante (quadro abaixo), fica claro que o objeto se trata de simples fornecimento de equipamentos de firewall, com licenciamento, treinamento e serviço de instalação, portanto, não pode ser considerado como SoC/MSS.

Item	Descrição/Especificação	Quantidade
01	Firewall Tipo 2 (Equipamento)	02
02	Licenças de uso de Software (Serviço)	02
03	Treinamento Firewall (Serviço)	01
04	Instalação Firewall	01

- **Contrato UNIVERSIDADE FEDERAL DO PIAUÍ:**

Conforme extraído da página 20 da documentação, o objeto é o que segue:

1. DO OBJETO

1.1. O objeto da presente licitação é o registro de preços de **Solução de Segurança para Rede de Computadores "firewall" da UFPI,** conforme condições, quantidades e exigências estabelecidas neste Edital e seus anexos.

Além disso, conforme páginas 40 e 41 da respectiva documentação, também fica claro o fornecimento de equipamentos de firewall, com instalação e configuração, portanto, não servem para comprovar experiência no fornecimento de serviços de SoC/MSS. Esta situação fica ainda mais comprovada conforme "Anexo IV – Especificação Técnica da Solução", à página 56:

ANEXO IV

ESPECIFICAÇÃO TÉCNICA DA SOLUÇÃO

ITEM	DESCRIÇÃO COTA RESERVADA	QTD
1	Firewall tipo 1 para Reitoria	2
2	Firewall tipo 2 para Campus	2
3	Firewall tipo 3 para Campus	5
4	Software de Gerenciamento Centralizado	1
5	Treinamento Firewall	1
6	Instalação Firewall tipo 1 e tipo 2	2
7	Instalação Firewall tipo 3	5

ITEM	DESCRIÇÃO COTA RESERVADA	QTD
8	Firewall tipo 3 para Campus	1
9	Instalação Firewall tipo 3	1

- **Contrato ATACADÃO DIA-A-DIA:**

O objeto do contrato, conforme página 84, é o seguinte:

Por este instrumento particular, as **PARTES** acima nominadas e qualificadas, ambas representadas na melhor forma de suas constituições sociais, têm entre si, justo e acordado, o presente "**Contrato de Prestação de Serviço de Gerenciamento e Disponibilidade de Firewall, Endpoints e demais Ativos da Rede Corporativa**", que reger-se-á mediante as seguintes cláusulas e condições:

Analisando o texto do objeto, vê-se que se trata de gerenciamento de firewall e Endpoint, bem como disponibilidade de rede. Na página 85, temos expressamente o serviço de **NOC – Gerenciamento de Disponibilidade**:

O valor mensal para o item 1 do presente contrato é de R$ 29.270,00 (vinte e nove mil e duzentos e setenta reais), para a prestação de serviço de Gerenciamento dos Firewall´s, compreendendo a cessão dos seguintes equipamentos:

- 25 Firewall's XGS 116 Standard Protection Bundle (Stand alone);
- 06 Firewall's XGS 116 Standard Protection Bundle (03 Clusters – HA);
- 01 Firewall XGS 136 Standard Protection Bundle (Stand alone);
- 02 Firewall's XGS 3300 Xstream Protection Bundle (01 Cluster – HA);
- 02 Firewall's XGS 3100 Xstream Protection Bundle (01 Cluster – HA).

O valor mensal para o item 2 do presente contrato e de R$ 12.400,00 (doze mil e quatrocentos reais), para **o serviço de Gerenciamento de Disponibilidade - NOC.**

Mais adiante, páginas 107 e 108, a licitante anexa um "4º Termo Aditivo", onde adiciona os serviços de SIEM, SOAR e UEBA, porém chama a atenção a cronologia da documentação:

1. Conforme páginas 101 a 106, o contrato é assinado de **21 a 28/10/2022**;

2. Na página 107, o Termo aditivo faz menção a um contrato firmado em **27/12/2022**;
3. Na página 108, o citado Termo Aditivo é datado de **03/10/2022 (anterior ao contrato!)**;
4. O atestado de capacidade técnica anteriormente enviado é datado de **19/10/2022**;

Dessa forma, além de uma total incoerência entre datas dos documentos apresentados, o atestado é fornecido em **menos de 1(um) mês da assinatura do contrato** (ou do aditivo), que seja.

A licitante também apresenta um documento fiscal, à página 109, onde o valor do serviço de SoC é de aproximadamente 12% do valor da proposta ofertada para o presente certame, ficando visível a desproporção com a complexidade requerida no caso desta Secretaria.

Assim, apesar da citação dos serviços de SIEM, SOAR e UEBA, típicos de SoC, consideramos que este atestado não comprova dimensão, complexidade e experiência compatíveis com o objeto sendo licitado.

- **Contrato BNDES:**

Mais uma vez, conforme página 110, o objeto se trata de simples fornecimento de solução de Endpoint, com suporte técnico, portanto, não compatível com o objeto deste certame.

> **1. OBJETO:** Contratação de subscrição de uso, atualização e suporte técnico especializado de Symantec Endpoint Protection (SEP) para servidores, conforme as condições constantes nas especificações técnicas e na proposta apresentada pela **CONTRATADA** (ANEXOS I e II deste **CONTRATO**).

O mesmo objeto, "subscrição de uso de solução Endpoint", é referido à página 119, nas especificações técnicas do referido edital:

> **ANEXO I. ESPECIFICAÇÕES TÉCNICAS**
>
> **1. OBJETO**
>
> 1.1. Contratação de subscrição de uso, atualização e suporte técnico especializado de Symantec Endpoint Protection (SEP) para servidores, conforme as condições constantes destas Especificações Técnicas e de seus Anexos.
>
> 1.2. A renovação se refere a 400 licenças de Symantec Endpoint Protection versão 14 ou superior, para servidores Windows Server 2008 R2 64 bits e versões superiores, pelo período de 12 (doze) meses, prorrogável uma vez por igual período.

E novamente à página 129:

Objeto: Fornecimento de renovação de suporte técnico e atualização para licenças de Symantec Endpoint Protection (SEP) para servidores

- **Contrato FNDE:**

Conforme páginas 141 e 142, trata-se de fornecimento de solução de firewall, com suporte e instalação, portanto, não comporta serviços de SoC/MSS.

1. **CLÁUSULA PRIMEIRA – OBJETO**

1.1 - O objeto do presente Termo de Contrato é a aquisição de Soluções de Segurança para rede de computadores da 'FIREWALL", conforme especificações e quantitativos estabelecidos no Edital do Pregão identificado no preâmbulo e na proposta vencedora, os

1.2 - Discriminação do objeto:

ITEM	DESCRIÇÃO/ ESPECIFICAÇÃO	QUANTIDADE
1	Firewall Tipo 1 Equipamentos que compõem a solução: 01x PAN-PA-5220-SSD2-D - Firewall Palo Alto Modelo 5220 Todos os modelos ofertados acompanham as garantias, cabos e acessórios exigidos nos respectivos itens e estão de acordo com as especificações, termo de referência, edital e seus anexos	02
	01x WCSS-PAN-SVC-PREM-5220-3YR - Garantia Premium 3 anos com suporte 24x7 01x PAN-PA-5220-URL4-3YR - Licença funcionalidades Filtro URL 3 anos 01x PAN-PA-5220-TP-3YR - Licença funcionalidades Prevenção à Ameaças 3 anos	02
4	Software de Gerenciamento Centralizado Equipamentos e licenças que compõem a solução: 01x PAN-PRA-25 – Gerenciamento Centralizado Palo Alto Modelo Panorama 01x WCSS-PAN-SVC-PREM-PRA-25-3YR – Garantia Premium 3 anos com suporte 24x7 Instalação e Configuração conforme especificações contidas no Termo de Referência. Procedência: Importado dos Estados Unidos Garantia: 36 (trinta e seis) meses	01
6	Instalação Firewall - Tipo 1 e Firewall Tipo 2	02

- **Contrato MEMORA:**

O contrato em questão descreve o objeto como “Contrato de Gerenciamento de Segurança da Informação SOC/MSS”, página 211, e traz basicamente os serviços de gerenciamento de firewall e endpoint.

Na página 223, referente ao 1º Termo Aditivo, a empresa subcontrata o fornecedor "Leader Solutions" para fornecimento da solução, o que é vedado pelo atual edital.

De qualquer forma, o valor associado aos serviços, apesar de remontar ao ano de 2012, mesmo que corrigido pelo IPCA até os dias de hoje (~100% de correção) resultaria em um valor de R$3.000,00 mensais, ou seja, aproximadamente 3% (três por cento) do valor da proposta para o presente certame, portanto, totalmente incompatível em termos de dimensão e complexidade. Além disso, o respectivo atestado ou contrato não traz o tamanho da infraestrutura do contratante, não permitindo avaliar o ambiente em questão.

A descrição do objeto, página 226, deixa clara a característica de "help desk" para o serviço, e não de SoC.

BEM(NS)/EQUIPAMENTO(S):

Item	Descrição
01	Fast Defender Security Appliance – XTM 330

SERVIÇOS:

Discriminação das Soluções / Serviços	
Solução	**Características**
01 Appliance Watchguard XTM 330 UTM Firewall	- VPN (SSL VPN – IPSec VPN) - Filtro de Conteúdo Web (Categorização de Sites) - IPS – Sistema de Prevenção de Intrusão - Controle de Aplicação (Facebook, Twitter, Skype e etc) - Gateway de Anti-Malware - Software de Gerência e Monitoramento - **Suporte Técnico especializado remoto e telefônico para monitoramento do firewall (720h/mês).**
Suporte Técnico (Help Desk)	24x7x365

- **Contrato MPDFT:**

Conforme objeto constante na folha 229 da manifestação, mais uma vez, é ofertado serviço de gerenciamento de solução de firewall:

CLÁUSULA PRIMEIRA – DO OBJETO

Contratação de empresa especializada para prestação de Serviço de Segurança de Perímetro com uso de *firewall* tipo *"Next Generation Firewall – NGFW"* incluindo instalação, manutenção, monitoramento, administração da solução e treinamento, de acordo com as condições e as especificações deste instrumento e dos anexos do edital.

Além do caso do objeto ser focado em solução de firewall, também depreende-se da "cláusula quinta – do preço", do referido contrato, a desproporção da solução, resultando em aproximadamente 10% do valor da atual proposta.

Cumpre salientar que o contrato do MPDFT não traz nenhuma informação sobre o tamanho ou complexidade de sua infraestrutura, não servindo de comparativo.

- **Contrato TCE-MG:**

O contrato do TCE-MG, página 248, define seu objeto como “Serviços Gerenciados e Integrados de Segurança”, porém logo em seguida lista apenas o serviço de “Gestão de Vulnerabilidades”, o que é apenas uma pequena parcela das atividades requeridas pelo presente certame.

Item	Descrição	Qtde
4	Serviços de Gestão de Vulnerabilidades	01
9	Instalação da solução de Gestão de Vulnerabilidades	01

O quantitativo de usuários já constou no atestado anteriormente entregue, somando 1024 usuários, porém não há citação do número de hosts ou ativos gerenciados, para que possa ser comparado ao ambiente desta Secretaria.

Assim, o atestado em questão não demonstra ser comparável à complexidade, abrangência e dimensão requeridas.

- **Contrato CASA DOS PARAFUSOS:**

O atestado em questão, página 261, caracteriza os serviços típicos de SoC, abrangendo monitoramento e gerenciamento de firewall, endpoints, ativos de rede, balanceadores e gestão de incidentes, além de controle de acessos, em regime 24x7x365.

O dado que prejudica o presente atestado é sua dimensão, muito aquém do mínimo requerido nas cláusulas do edital, contemplando ambiente com apenas 200 usuários, menos de 10% do ambiente atual da SEFAZ-RS. Além disso, faz nítida confusão com o conceito de usuários, ativos e hosts, que não podem ser considerados a mesma coisa.

- **Contrato CNMP:**

Tanto o atestado apresentado (página 263) quanto o contrato (página 265) trazem como objeto o seguinte:

> O presente Contrato tem por objeto a prestação de Serviços Gerenciados de Segurança da Informação, em regime 24x7x365, para atendimento às necessidades do Conselho Nacional do Ministério Público, de acordo com as especificações técnicas contidas no Termo de Referência – TR e seus apêndices, e capacitação correlata na área de segurança da informação.

O detalhamento do objeto traz o seguinte:

Item	Descrição	Unidade de Medida	Qtde
1	Equipamentos destinados a prestação do serviço de segurança (*incluir lista de todos os equipamentos contendo marca e modelo*)	mês	60
2	Serviços gerenciados de segurança	mês	60
3	Instalação e migração	evento	1
4	Capacitação em treinamento oficial do fabricante de NGFW	aluno	3
5	Capacitação em treinamento oficial do fabricante de WAF	aluno	3

Uma melhor descrição dos serviços é dada no item 3.2 das especificações técnicas, página 328, e no item 3.2.8, página 329:

3.2. **Das especificações técnicas mínimas esperadas do serviço prestado**

3.2.1. O serviço prestado deve englobar ações relativas à instalação, manutenção, gerência de firewall, web application firewall, detecção e prevenção de intrusão, filtros de conteúdo, controle de aplicação, antivírus de rede, redes virtuais privadas, entre outras através de plataforma de hardware e software (appliance)

3.2.1.1. Em caso de detecção de tentativa de intrusão e/ou intrusão a CONTRATADA deverá adotar melhores práticas de resposta a incidentes a fim de evitar, conter, controlar e/ou mitigar os efeitos do incidente de segurança, emitindo relatório técnico e comunicando imediatamente a CONTRATADA quais direcionamentos técnicos a serem tomados.

3.2.1.2. Todas as medidas necessárias para auditoria do incidente devem ser tomadas a fim de subsidiar melhor análise da equipe técnica da CONTRATANTE que deverá ter o suporte da equipe técnica da CONTRATADA

3.2.8. A CONTRATADA deverá constantemente, sempre que necessário ou pelo menos mensalmente efetuar análise preventiva e corretiva das políticas de segurança nos equipamentos gerenciados, objetivando aderência às boas práticas recomendadas pelo fabricante, manutenção da segurança, manutenção da padronização, documentação e performance do equipamento, de modo a mitigar riscos, melhor utilizar os recursos e evitar duplicidade e sombreamento de políticas. A análise preventiva e corretiva deverá contemplar no mínimo os seguintes pontos:

3.2.8.1. Regras que estejam sendo subutilizadas ou inutilizadas. Regras sem tráfego ou sem tráfego durante um período de tempo definido;

3.2.8.2. Identificar sombreamento ou redundância de regras. Essa verificação deverá levar em conta:

3.2.8.2.1. IPs de origem e destino;
3.2.8.2.2. Portas de origem e destino;
3.2.8.2.3. Protocolos;
3.2.8.2.4. Aplicações;
3.2.8.2.5. Perfis de segurança;
3.2.8.2.6. Usuários ou grupos de usuários.

Apesar do objeto deste atestado/contrato ser similar e equivalente aos serviços sendo licitados, não foi encontrada nenhuma citação em relação ao tamanho da infraestrutura do CNMP, seja pelo número de usuários, número de hosts ou quantidade de ativos controlados, o que prejudica a análise em relação à comparabilidade com o ambiente do Secretaria da Fazenda.

- **CONCLUSÃO:**

Em linha com o que o licitante já havia apresentado na primeira remessa de atestados, é nítida sua experiência no fornecimento de soluções de segurança com suporte, garantia, licenciamento e atualizações, porém continua frágil sua comprovação de experiência no fornecimento de serviços de SoC/MSS, pelos seguintes aspectos:

- Simplificação do serviço de SoC/MSS, se atendo à gestão de firewall e endpoints;
- Atestados e contratos cujo objeto se aproxima dos serviços requeridos, não são comparáveis, seja pela falta de informação sobre os ambientes, seja pela falta de proporção dos serviços prestados;

O que se conclui é que a empresa está iniciando nos serviços de SoC propriamente ditos, mas ainda distante do tamanho e complexidade do ambiente alvo deste certame.

Estamos aqui tratando de uma Secretaria da Fazenda com mais de 2.500 usuários, em torno de 3.000 ativos entre servidores, redes e endpoints, além de um complexo ambiente de NG Firewall, sd-wan, gestão de acessos e identidades, serviços em nuvem, gestão de vulnerabilidades, SIEM, SOAR, e com serviços pulverizados por 2 datacenters e mais de 50 localidades pelo interior do Estado.

Portanto, de mesma forma que concluímos anteriormente, entendemos que a empresa FAST HELP INFORMÁTICA LTDA **não comprova** ter a expertise mínima requerida para o tamanho, amplitude e complexidade dos ambientes envolvidos.

ESTADO DO RIO GRANDE DO SUL
SECRETARIA DA FAZENDA
DEPARTAMENTO DE TIC
GABINETE

Atenciosamente,

[redacted]