

ESTUDO TÉCNICO PRELIMINAR

Processo Administrativo nº 2023/2008

**Aquisição de solução para proteção do
perímetro de rede do TJAL**

Maceió, maio de 2023

Diretoria Adjunta de Tecnologia da Informação - DIATI

Histórico de Revisões

Data	Versão	Descrição	Autor
07/05/2022	1.0	Versão inicial	Equipe de planejamento
20/06/2022	1.1	Inclusão das propostas comerciais	Equipe de planejamento
11/05/2023	1.2	Inclusão de mais informações na área de análise de soluções	Equipe de planejamento

SUMÁRIO

1. ANÁLISE DE VIABILIDADE DA CONTRATAÇÃO.....	5
1.1. CONTEXTUALIZAÇÃO.....	5
1.2. DEFINIÇÃO E ESPECIFICAÇÃO DAS NECESSIDADES E REQUISITOS.....	6
1.2.1. Identificação das necessidades de negócio.....	6
1.2.6. Identificação dos requisitos tecnológicos.....	6
1.2.7. Requisitos de garantia e manutenção.....	7
1.2.8. Requisitos de experiência profissional.....	7
1.2.9. Requisitos de capacitação.....	8
1.2.10. Requisitos de segurança.....	8
1.3. ANÁLISE DE SOLUÇÕES.....	9
1.3.1. SOLUÇÕES DISPONÍVEIS NO MERCADO DE TIC.....	9
1.3.2. CONTRATAÇÕES PÚBLICAS SIMILARES.....	11
1.3.3. OUTRAS SOLUÇÕES DISPONÍVEIS.....	12
1.3.4. PORTAL DO SOFTWARE PÚBLICO BRASILEIRO.....	12
1.3.5. ALTERNATIVA DE SOFTWARE LIVRE NO MERCADO DE TIC.....	12
1.3.6. MODELO NACIONAL DE INTEROPERABILIDADE - MNI.....	12
1.3.7. INFRAESTRUTURA DE CHAVES PÚBLICAS BRASILEIRA – ICP-BRASIL.....	13
1.3.8. MODELO DE REQUISITOS MOREQ-JUS.....	13
1.4. ANÁLISE DOS CUSTOS TOTAIS DA DEMANDA.....	13
1.5. ESCOLHA E JUSTIFICATIVA DA SOLUÇÃO DE TIC A SER CONTRATADA.....	13
1.5.1. MOTIVAÇÃO DA ESCOLHA.....	13
1.5.2. DESCRIÇÃO DA SOLUÇÃO.....	13
1.5.3. ALINHAMENTO DA SOLUÇÃO.....	13
1.5.4. BENEFÍCIOS ESPERADOS.....	14

1.5.5. RELAÇÃO ENTRE A DEMANDA PREVISTA E A QUANTIDADE DE BENS/SERVIÇOS A SEREM CONTRATADOS.....	14
2. SUSTENTAÇÃO DO CONTRATO.....	18
2.2. ADEQUAÇÃO DO AMBIENTE.....	18
2.4. RECURSOS MATERIAIS E HUMANOS NECESSÁRIOS À CONTINUIDADE DE NEGÓCIO.....	18
2.8. DESCONTINUIDADE DO FORNECIMENTO.....	18
2.13. TRANSIÇÃO CONTRATUAL E ENCERRAMENTO DO CONTRATO.....	19
2.16. ESTRATÉGIA DE INDEPENDÊNCIA TECNOLÓGICA.....	19
3. ESTRATÉGIA PARA CONTRATAÇÃO.....	20
4. ANÁLISE DE RISCOS.....	21
4.1. RISCOS DO PROCESSO DE CONTRATAÇÃO.....	21
4.2. RISCOS DE NEGÓCIO.....	21
4.3. RISCOS DA EXECUÇÃO DO OBJETO.....	22
4.4. RISCOS ADMINISTRATIVOS.....	23
4.5. MATRIZ DE AVALIAÇÃO QUALITATIVA DOS RISCOS IDENTIFICADOS.....	23
5. APROVAÇÃO E ASSINATURA.....	24
6. ANEXO TR1 – PROPOSTAS DE PREÇOS.....	25

INTRODUÇÃO

O Estudo Técnico Preliminar tem por objetivo identificar e analisar os cenários para o atendimento da demanda que consta no Documento de Oficialização da Demanda, bem como demonstrar a viabilidade técnica e econômica das soluções identificadas, fornecendo as informações necessárias para subsidiar o respectivo processo de contratação.

Referência: Art. 11 da IN SGD/ME nº 1/2019 e Resolução CNJ nº 182/2013

1. ANÁLISE DE VIABILIDADE DA CONTRATAÇÃO

1.1. CONTEXTUALIZAÇÃO

- 1.1.1. A prestação jurisdicional na Justiça Alagoana depende diretamente dos serviços de TIC que sustentam os sistemas informatizados da Corte. Para sustentar o funcionamento dos sistemas são necessários vários tipos de redes de comunicação, entre elas a Internet, as redes locais dentro das dependências do TJAL (redes LAN) e as redes privadas que conectam o TJAL a funcionários e parceiros. Toda a segurança dos dados que circulam entre todas as redes de dados do Tribunal, nos seus diferentes níveis de interligações, é promovida por um conjunto de soluções de segurança da informação, dentre eles o Firewall, tornando este equipamento imprescindível para o negócio do Tribunal.
- 1.1.2. Visando a garantir melhores condições de segurança da informação, com vistas à integridade dos processos eletrônicos judiciais e administrativos e demais serviços à disposição dos jurisdicionados, faz-se necessário a implantação de soluções que atuem no controle e segurança das informações, nas camadas de rede mais avançadas, em nível de aplicação (camada 7), além do controle de aplicações mais específicas e direcionadas, servidas mediante os protocolos HTTP e HTTPS, relacionados aos portais Web, de modo a minimizar os riscos de exploração de possíveis ameaças e que permitam, por meio de alarmes e controles, uma rápida resposta do Tribunal em caso de incidentes de segurança.
- 1.1.3. Atualmente o Tribunal de Justiça de Alagoas (TJAL) mantém em seu datacenter 2 (dois) equipamentos de Firewall do tipo Next Generation Firewall (NGFW), modelo Fortigate 500E, que funcionam como um único cluster. Estes equipamentos funcionam em regime de comodato por meio do contrato de prestação de serviço nº 10/2018 e são utilizados para prover restrição de tráfego malicioso entre a Internet e a rede local, além funcionar como um gateway para serviços relevantes do Tribunal, como a Rede Privada Virtual (VPN – Virtual Private Network), por exemplo.
- 1.1.4. Após alguns estudos, observaram-se as seguintes oportunidades de melhoria em relação a este contrato:
 - 1.1.4.1. O serviço de fornecimento dos firewalls, imerso no contrato 10/2018, é agregado a um serviço de fornecimento de link de internet, ambos providos por uma única empresa. Desmembrando estes objetos potencializará a competição entre empresas interessadas, cada qual especializada no fornecimento de um objeto específico, aumentando as chances de se obter uma melhor relação custo-benefício para a Administração;
 - 1.1.4.2. Buscou-se adquirir os firewalls ao invés de repetir o modelo de contratação atual. Este modelo de contratação, provida como serviço, atualmente carece de maturidade no âmbito da Administração Pública. Em outras palavras, o provimento dos equipamentos – em comodato – conjugado à terceirização da operacionalização destes ainda é infimamente presente em contratos públicos. Desta forma, não é trivial obter parâmetros de preço e desempenho que minimizem os riscos de uma eventual perpetuação deste tipo de serviço. Ademais, a aquisição dos firewalls, atrelado ao treinamento especializado, dará mais autonomia ao *staff* da CONTRATANTE para administrar e operar o produto;
 - 1.1.4.3. O modelo Fortigate 500E, atualmente em operação, está apresentando indícios de subdimensionamento, para determinadas funções, em relação à atual demanda da Corte Alagoana. Na fase de estudos preliminares, uma ampla análise de mercado foi realizada com o objetivo de

parear, com a maior precisão possível, as necessidades institucionais e tecnológicas do TJAL com o que o mercado poderia oferecer na área de Segurança da Informação, mais precisamente na área de Firewall de Próxima Geração. Portanto, esta pretensão traduz os anseios da Corte Alagoana de se obter uma solução de Firewall mais robusta, visando o aprimoramento da Segurança da Informação no curto, médio e longo prazo.

- 1.1.5. Para o contexto apresentado, portanto, desponta-se como imprescindível a aquisição de solução de Firewall de Próxima Geração (NGFW – *Next Generation Firewall*) atualizada aos atuais padrões de mercado, com recursos de alta disponibilidade para sustentar o funcionamento institucional da Justiça.

1.2. DEFINIÇÃO E ESPECIFICAÇÃO DAS NECESSIDADES E REQUISITOS

1.2.1. Identificação das necessidades de negócio

1.2.2. **Necessidade 1: assegurar a disponibilidade e a segurança da informação;**

- 1.2.2.1. promover ações de controle e proteção das informações disponíveis;
- 1.2.2.2. repelir ações que comprometam a disponibilidade da informação;
- 1.2.2.3. monitorar o perímetro de rede e solicitações encaminhadas aos portais e aplicações à serviço da população, a fim de garantir a proteção das informações disponíveis no ambiente do TJAL.

1.2.3. **Necessidade 2: preservar a confidencialidade, a integridade e a disponibilidade da informação;**

- 1.2.3.1. promover os meios necessários para que a informação esteja acessível e utilizável;
- 1.2.3.2. promover os meios necessários para que a informação não seja modificada ou destruída, de maneira não autorizada ou acidental;
- 1.2.3.3. promover os meios necessários para que a informação esteja acessível e utilizável;

1.2.4. **Necessidade 3: potencializar o cumprimento da Política de Segurança da Informação;**

- 1.2.4.1. promover funções capazes para viabilizar a disponibilidade, a integridade, a confidencialidade e a autenticidade das informações.

1.2.5. **Necessidade 4: Aprimorar a proteção aos serviços disponibilizados à população;**

- 1.2.5.1. Promover proteção superior aos serviços disponibilizados de forma online;
- 1.2.5.2. Promover a melhoria da imagem do Poder Judiciário de Alagoas como provedor de serviços;

1.2.6. Identificação dos requisitos tecnológicos

1.2.6.1. **Requisitos gerais de Arquitetura Tecnológica**

- 1.2.6.1.1. Deve ser fornecido em formato de appliance físico.
- 1.2.6.1.2. Deve ser novo, sem uso, entregue em perfeito estado de funcionamento, sem marcas, amassados, arranhões ou outros problemas físicos, acondicionados em suas embalagens originais.
- 1.2.6.1.3. Nenhum dos equipamentos fornecidos pode estar em modo End of Life, End of Sale e End of Support.
- 1.2.6.1.4. Deve ser apropriado para o uso em ambiente tropical com umidade relativa na faixa de 10 a 90% (sem condensação) e temperatura ambiente na faixa de 0 a 40°C.

- 1.2.6.1.5. Deve possuir fonte com alimentação nominal de 100~120VAC e 210~230VAC e frequência de 50 ou 60 Hz ou auto-ranging. Deve vir acompanhado de cabo de alimentação com, no mínimo, 1,80m (6 pés), com plug tripolar 2P+T no padrão ABNT NBR 14136.
- 1.2.6.1.6. Deve possuir, no mínimo, 1 (uma) interface Ethernet para gerenciamento.
- 1.2.6.1.7. Deve ser fornecido em sua capacidade máxima de processamento, memória e armazenamento interno.
- 1.2.6.1.8. Deve ser fornecido com todas as suas portas de comunicação, interfaces e afins habilitadas, operacionais e prontas para operação, inclusive com seus respectivos transceivers instalados, sem custos adicionais.
- 1.2.6.1.9. Deve possuir certificação de conformidade sustentável de acordo com os padrões EPA (Environmental Protection Agency) ou similares, tais como EnergyStar, RoHS (Restriction on Hazardous Substances) ou WEEE (Waste Electrical and Electronic Equipment).
- 1.2.6.1.10. Deve suportar afiação em bastidor (rack) padrão EIA-310 com largura de 19' (dezenove polegadas) e altura de até duas unidades de rack (2U), acompanhado de todos os acessórios necessários (cabos, suportes, gavetas, braços, trilhos etc).
- 1.2.6.1.11. Deve possuir 2 (duas) fontes de alimentação independentes, redundantes e *hotswappable*.

1.2.6.2. Requisitos de Implantação

- 1.2.6.2.1. Todas as atividades necessárias à implantação e configuração da solução deverão ser obrigatoriamente de responsabilidade da CONTRATADA. Tais atividades estão relacionadas com todas as funcionalidades, licenciamentos, serviços, hardware e qualquer outro item que compõe a solução, podendo ser mencionados os seguintes exemplos: instalação física e montagem em rack, instalação de todos os cabos e conectores necessários, energização, definição de topologia, configurações básicas da interface de gerência, instalação e atualização de firmware, além de qualquer outra que se faça necessária para o pleno funcionamento da solução.
- 1.2.6.2.2. A etapa de conclusão da instalação e configuração dos equipamentos deverá contemplar, no mínimo:
 - a) Testes de Aceite e Funcionamento, simulando todos os cenários possíveis de failover e failback;
 - b) Operação Assistida de Funcionamento da Solução, que consiste da disponibilização de um técnico residente certificado pelo fabricante do equipamento, no endereço do CONTRATANTE, devidamente identificado, para sanar quaisquer dúvidas e problemas que ocorrerem na operação da solução, durante prazo mínimo de 3 dias;
 - c) Fornecimento da documentação de todo o projeto (AS-BUILT)
- 1.2.6.2.3. O serviço de instalação e configuração deverá ser realizado por técnico certificado oficialmente pelo fabricante da solução ofertada ou pelo próprio fabricante;

1.2.7. Requisitos de garantia e manutenção

- 1.2.7.1. Deverá ser oferecida garantia de 60 (sessenta) meses;
- 1.2.7.2. Para a solução de segurança adquirida e licenciada, deverá ser prestado atendimento técnico telefônico/e-mail (on-line) e presencial (on-site), em escala de 24 (vinte e quatro) horas por dia, 7 (sete) dias por semana, 365 (trezentos e sessenta e cinco) dias por ano, ininterruptamente, cumprindo os prazos estabelecidos no Termo de Referência.

1.2.8. Requisitos de experiência profissional

- 1.2.8.1. A execução dos serviços técnicos especializados deverá ser realizada por profissional certificado pelo fabricante da solução, sendo indispensável apresentação de documentação original do fabricante que comprove a validade da certificação quando solicitada pela CONTRATANTE a qualquer momento.
- 1.2.8.2. Os serviços técnicos deverão sempre ser executados por profissionais que detenham os conhecimentos requeridos para a execução dos serviços detalhados em Ordem de Serviços ou Chamados Técnicos.

1.2.9. Requisitos de capacitação

- 1.2.9.1. É recomendado que se realize capacitação do corpo técnico para melhor gerenciamento e administração e nesse caso podem ser elencados os seguintes requisitos:
 - 1.2.9.1.1. A capacitação deverá ser realizada nas dependências do TJAL, ou curso oficial, a depender dos custos envolvidos e do conteúdo programático de cada um, com abordagem teórica e prática para equipe de até 8 (oito) técnicos designados pelo CONTRATANTE.
 - 1.2.9.1.2. A CONTRATADA é responsável por prover os recursos e o ambiente computacional para realização da capacitação, que pode ser um ambiente acessado remotamente.
 - 1.2.9.1.3. Deverá ser realizado em dias úteis, em horário comercial.
 - 1.2.9.1.4. Deverá ter carga horária total e cronograma propostos pela CONTRATADA de modo que comporte todo o conteúdo programático proposto.
- 1.2.9.1.5. O conteúdo programático e a respectiva ementa deverão contemplar os recursos e configurações existentes na solução adquirida, devendo abordar, no mínimo os tópicos:
 - 1.2.9.1.5.1. arquitetura de funcionamento da Solução de Segurança, configuração básica para funcionamento e a configuração de gerenciamento;
 - 1.2.9.1.5.2. Deverá ser fornecido material didático, que poderá ser em formato digital, incluindo o material de apoio utilizado nas aulas, como, por exemplo, slides.
 - 1.2.9.1.5.3. Após o término da capacitação a CONTRATADA deverá fornecer certificados de participação aos alunos.

1.2.10. Requisitos de segurança

- 1.2.10.1. A CONTRATADA obrigase a tratar como "segredos comerciais e confidenciais", quaisquer informações, dados, processos, fórmulas, códigos, fluxogramas, diagramas lógicos, dispositivos e modelos relativos aos serviços ora contratados, utilizando-os apenas para as finalidades previstas neste ajuste, não podendo revelá-los ou facilitar a sua revelação a terceiros;
- 1.2.10.2. A CONTRATADA deverá cumprir e atender aos padrões de segurança e controle para acesso e uso das instalações da CONTRATANTE, zelando por sua integridade, preservando o sigilo e a confidencialidade de todos os dados e informações pertinentes aos serviços prestados, de acordo com a legislação vigente que dispõe sobre a categoria dos documentos públicos sigilosos e o acesso a eles;
- 1.2.10.3. Os profissionais disponibilizados pela Contratada para a prestação dos serviços deverão estar identificados com crachá de identificação da mesma, estando sujeitos às normas internas de segurança do Contratante, inclusive àqueles referentes à identificação, trajés, trânsito e permanência em suas dependências.
- 1.2.10.4. A CONTRATADA não deverá acessar ou manipular qualquer informação confiada sem prévia autorização da CONTRATANTE;
- 1.2.10.5. A CONTRATADA deverá firmar um Termo de Confidencialidade, por ocasião da assinatura do Contrato.

1.3. ANÁLISE DE SOLUÇÕES

1.3.1. SOLUÇÕES DISPONÍVEIS NO MERCADO DE TIC

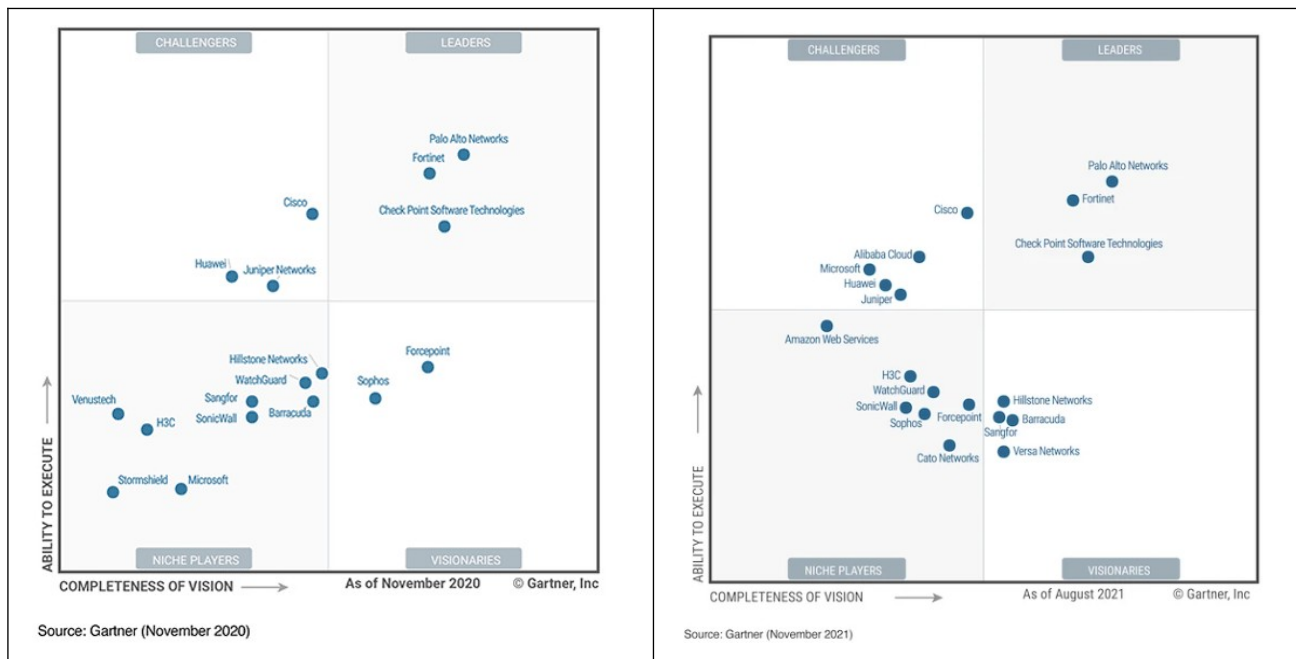
- 1.3.1.1. A análise comparativa de soluções de TIC, capazes de atender a necessidade do TJAL, visa a elencar as alternativas de atendimento considerando, além do aspecto econômico, os aspectos de eficiência e eficácia em termos de benefícios para o alcance dos objetivos da contratação.
- 1.3.1.2. Considerando os objetos deste estudo, visualizam-se 02 (duas) possíveis alternativas presentes no mercado, para cada tipo de solução. As soluções de TIC identificadas são:

Cenário	Nome da solução (ou cenário)	Descrição resumida
1A	Aquisição de Firewall de última geração (Next Generation Firewall - NGFW)	Aquisição de nova solução de firewall. Esta solução é baseada na aquisição de novos equipamentos, incluindo licenciamento, manutenção, garantia e capacitação. Em relação ao atual Firewall, esta opção apresenta atualização de hardware, com entrega melhor de desempenho.
1B	Contratação de nova solução de NGFW como serviço	Contratação do equipamento como serviço incluindo o licenciamento e suporte técnico. Esta solução é baseada no aluguel do equipamento em detrimento à aquisição. É o atual formato de contratação vigente no TJAL, junto com um serviço de acesso à internet, ambos provisionados em um único contrato, 19/2018.

1.3.1.3. Cenário 1A: Aquisição de Firewall de última geração (Next Generation Firewall - NGFW):

- 1.3.1.3.1. Sendo uma solução comum de mercado, existem diversos fabricantes que podem oferecer soluções de segurança de perímetro, com diferentes graus de qualidade e diversos preços a serem pagos. Sendo inviável avaliar todas as opções disponíveis, recorreu-se ao Gartner, empresa referência na área de consultoria em soluções de Tecnologia da Informação, para delimitar as melhores opções a serem consideradas no projeto, desde o dimensionamento de appliances até a solicitação de propostas orçamentárias.
- 1.3.1.3.2. O Gartner possui um “quadrante”, publicado anualmente, onde são utilizados diversos critérios para avaliar a qualidade das soluções. Como o Tribunal preza pela qualidade das soluções adquiridas para compor sua infraestrutura tecnológica, as soluções consideradas foram as que se enquadram no quadrante “Leaders”, considerando os 2 últimos anos. Os fabricantes localizados neste quadrante foram avaliados com os melhores resultados em suas soluções oferecidas.

Ano de referência: 2020	Ano de referência: 2021
--------------------------------	--------------------------------



1.3.1.4. Cenário 1B: Contratação de nova solução de NGFW como serviço:

- 1.3.1.4.1. Uma solução pouco praticada no setor público, sobretudo no âmbito do Poder Judiciário.
- 1.3.1.4.2. Esta a contratação está consubstanciada em uma empresa que presta um serviço de SOC, ou Security Operation Center, monitorando e dando suporte a um equipamento NGFW instalado no cliente, cedido em comodato.
- 1.3.1.4.3. No entanto, a grande maioria das contratações que envolvem equipamentos de NGFW, no âmbito do Poder Judiciário, optam pela aquisição do produto. Nesta situação, há casos em que existe um serviço atrelado ao produto, à parte, como serviços de consultoria acionados sob demanda.
- 1.3.1.4.4. Em pesquisas realizadas com empresas deste nicho, este cenário se mostrou substancialmente mais oneroso do que o cenário anterior.

1.3.1.5. Quadro-resumo de análise dos cenários:

Características analisadas	Solução 1.a	Solução 1.b
Uso de equipamentos novos	Sim	Sim
Atualização de hardware com melhor entrega de desempenho	Sim	Sim
Valor econômico mais vantajoso	Sim	Não
Equipamentos não estarão em fim de vida útil	Sim	Sim
Adequação da capacidade de desempenho em relação ao ambiente atual	Sim	Sim
Após o prazo final da garantia, o equipamento permanecerá operacional	Sim	Não

apenas e não receberá mais atualizações		O ativo será devolvido
Necessidade de política de descarte de equipamentos de TI	Sim	Não
Necessidade de janela de migração entre a solução atual e a nova	Sim	Sim
Risco de interrupção do fornecimento da solução por questões ligadas à CONTRATANTE (orçamentário, administrativo) ou à CONTRATADA (inadimplência do serviço, falência, etc)	Não há Equipamentos adquiridos e recursos humanos treinados proverão a sustentação da solução durante todo o ciclo de vida.	Há
Adotação na esfera pública	Massivo	Escasso
Autonomia e retenção do conhecimento	Maior	Menor
Preço	Maior	Menor

Tabela 1

1.3.2. CONTRATAÇÕES PÚBLICAS SIMILARES

1.3.2.1. A equipe de planejamento tomou como base contratações do mesmo tipo, presentes em soluções apresentadas em editais publicados por outros órgãos da Administração Pública, ocorridas nos 2 últimos anos, obtidas através do portal de compras governamentais (<https://www.comprasgovernamentais.gov.br>) e pesquisas feitas pela internet, com destaque para:

Órgão	Pregão	Descrição
Tribunal de Justiça do Estado da Paraíba	019/2020	Aquisição de solução de Segurança da Informação com gerenciamento centralizado, incluindo equipamentos, softwares, licenciamentos, treinamento, consultoria, garantia e suporte técnico para o Poder Judiciário do Estado da Paraíba;
Tribunal Superior do Trabalho	031/2020	Aquisição de solução de segurança para redes de dados do tipo <i>Next Generation Firewall</i> de alta disponibilidade, compreendendo: sistema de detecção e prevenção de intrusão do TIPO IPS/IDS, gerenciamento centralizado e integrado, controle de ameaças, filtro de URL, controle de aplicação, suporte e garantia do fabricante, assinaturas de proteção e suporte técnico em repositório mundial do fabricante, suporte técnico do fabricante local e/ou remoto, incluindo serviços de instalação e treinamento.
EBSERH	22/2020	Aquisição de solução de firewall, composta por equipamentos, licenças de aplicações, software de gerenciamento, instalação e capacitação, para atender as necessidades da Administração Central da Empresa Brasileira de Serviços Hospitalares e suas filiais.

Instituto Federal do Triângulo Mineiro	23/2020	Aquisição, pelo sistema de registro de preços, de solução de proteção de rede com características de Next Generation Firewall (NGFW) ou Unified Threat Management (UTM) para segurança de informação perimetral que inclui filtro de pacote, controle de aplicação, administração de largura de banda (QoS), VPN IPSec e SSL, prevenção contra invasão (IPS), prevenção contra ameaças de Malware/vírus, Filtro de Conteúdo URL com categorização automática, bem como controle de transmissão de dados e acesso à internet compondo uma plataforma de segurança integrada e robusta com identificação de usuários e controle granular de permissões de acesso;
Universidade Federal do Cariri	38/2020	Registro de preço para contratação de empresa especializada para fornecimento de licenças para expansão do sistema de gerenciamento de rede e de solução de proteção de dados (Firewall).
AMGESP/AL – Agência de Modernização da Gestão de Processos	10.194/2020	Fornecimento de equipamentos de segurança da informação e de redes, incluindo firewall, conjugado com licenças de uso de software, garantia mínima de 36(trinta e seis) meses, incluindo serviços de instalação, serviços customizados de integração e migração, suporte técnico, atualização de software e transferência de conhecimento.
Tribunal Regional Federal da 5ª Região	19/2022	Ata de Registro de Preços, a contratação de empresa especializada para aquisição de Solução de NGFW com licenças e garantias para 48 (quarenta e oito) meses, para o Tribunal Regional Federal da 5ª Região (Órgão Gerenciador), e Justiça Federal de 1ª Instância em Pernambuco, Justiça Federal de 1ª Instância nas Alagoas, Justiça Federal de 1ª Instância na Paraíba, Justiça Federal de 1ª Instância no Rio Grande do Norte, Justiça Federal de 1ª Instância no Ceará e Justiça Federal de 1ª Instância em Sergipe (Órgãos Participantes)

1.3.3. OUTRAS SOLUÇÕES DISPONÍVEIS

- 1.3.3.1. Em virtude da natureza da demanda, não se vislumbra outras soluções disponíveis no mercado além das apresentadas no item 1.3.1 deste documento. Ademais, conforme indicado no item 1.3.2, vários órgãos ou entidades da administração pública, para atender a sua demanda de análise de segurança de perímetro de rede, contrataram uma das alternativas de solução apresentadas neste documento.

1.3.4. PORTAL DO SOFTWARE PÚBLICO BRASILEIRO

- 1.3.4.1. Não existem soluções no Portal do Software Público Brasileiro capazes de satisfazer plenamente os requisitos definidos no item 1.2.

1.3.5. ALTERNATIVA DE SOFTWARE LIVRE NO MERCADO DE TIC

- 1.3.5.1. Dada a natureza da demanda, não existem soluções de software livre ou software público capazes de satisfazer plenamente os requisitos definidos no item 1.2.

1.3.6. MODELO NACIONAL DE INTEROPERABILIDADE - MNI

- 1.3.6.1. Não se aplica por tratar de uma solução que não possui o requisito para intercâmbio de informações de processos judiciais e assemelhados entre os diversos órgãos de administração de justiça, nem tampouco

servir de base para implementação das funcionalidades pertinentes no âmbito do sistema processual, nos termos tratados pela Resolução Conjunta CNJ/CNMP nº 3 de 16/04/2013.

1.3.7. INFRAESTRUTURA DE CHAVES PÚBLICAS BRASILEIRA – ICP-BRASIL

- 1.3.7.1. As alternativas de solução levantadas são capazes de fazer uso dos recursos tecnológicos disponíveis em certificados digitais, estando alinhadas à Infraestrutura de Chaves Públicas – ICP Brasil e em conformidade com a MP nº 2.200-2 – de 24 de agosto de 20013 - e demais arcabouços normativos aplicáveis a solução, instituídos pelo Instituto Nacional de Tecnologia da Informação (ITI).

1.3.8. MODELO DE REQUISITOS MOREQ-JUS

- 1.3.8.1. Não se aplica por tratar de uma solução que não possui o requisito de gestão de processos e documentos, nos termos tratados pela Resolução CNJ nº 91 de 29/09/2009.

1.4. ANÁLISE DOS CUSTOS TOTAIS DA DEMANDA

- 1.4.1.1. Dentre as soluções que atendem ao Tribunal que foram analisadas, a solução 1A foi aprofundada sob a perspectiva financeira. Por lógica, a implementação do cenário 1B será notadamente mais cara, haja vista que os custos de aquisição dos equipamentos serão os mesmos da solução 1A, com o diferencial de que a CONTRATADA embutirá seus próprios custos para adquirir os equipamentos, considerando o risco da intermediação da compra e os riscos inerentes à manutenção do serviço;
- 1.4.1.2. O ANEXO TR1 – PROPOSTAS DE PREÇOS detalha os custos que foram levantados para solução 1A;

1.5. ESCOLHA E JUSTIFICATIVA DA SOLUÇÃO DE TIC A SER CONTRATADA

1.5.1. MOTIVAÇÃO DA ESCOLHA

- 1.5.1.1. Dentre os cenários disponíveis no mercado de TIC apresentadas nestes Estudos, o cenário 1A, que consiste na aquisição de Firewall de última geração (Next Generation Firewall - NGFW), se mostra mais vantajosa para o TJAL, dado aos diferenciais extraídos da Tabela 1:
- 1.5.1.1.1. Valor econômico mais vantajoso;
- 1.5.1.1.2. Minimização do risco de interrupção do fornecimento da solução por questões ligadas à CONTRATANTE (orçamentário, administrativo) ou à CONTRATADA (inadimplência do serviço, falência, etc);
- 1.5.1.1.3. Massiva adoção na esfera pública: é um cenário de implementação de projeto que se mostra maduro, pela sua massiva adoção, o que implica em uma exposição menor a riscos ligados à contratação.
- 1.5.1.1.4. Maior autonomia e retenção do conhecimento: os funcionários da CONTRATANTE serão treinados pela fabricante da solução. Isto implicará em maior autonomia para administrar a ferramenta adotada, retenção do conhecimento e facilitação da sustentação e da continuidade do negócio.

1.5.2. DESCRIÇÃO DA SOLUÇÃO

- 1.5.2.1. Aquisição de solução de segurança para o perímetro de rede do TJAL, abrangendo proteção do tipo *Next Generation Firewall* (NGFW) de alta disponibilidade, o que inclui suporte e garantia do fabricante, assinaturas de proteção, suporte técnico em repositório mundial do fabricante, suporte técnico do fabricante local e/ou remoto e serviços de instalação e treinamento.

1.5.3. ALINHAMENTO DA SOLUÇÃO

1.5.3.1. A presente pretensão encontra consonância com os instrumentos estratégicos da Corte, tanto o PETIC quanto o PDTIC, além do plano de contratações 2022;

ALINHAMENTO AO PLANO ESTRATÉGICO INSTITUCIONAL VIGENTE		
ID	Objetivos Estratégicos	
11	Melhoria da Infraestrutura e Governança de TIC	<p>Iniciativa 11.2.2 – aprimoramento da segurança da informação.</p> <p>Iniciativa 11.2.3 – melhoria da disponibilidade dos sistemas judiciais.</p>

ALINHAMENTO AO PETIC		
ID	Indicador	Ação associada
2A	Possuir ambiente de processamento central (Datacenter) com requisitos mínimos de segurança e de disponibilidade	Garantir ambiente de processamento central (Data Center) com requisitos mínimos de segurança e de disponibilidade estabelecidos em normas nacionais e internacionais, que abrigue os equipamentos principais de processamento e de armazenamento de dados; de segurança e ativos de rede centrais, para maximizar a segurança e a disponibilidade dos serviços essenciais e de sistemas estratégicos do órgão.

1.5.4. BENEFÍCIOS ESPERADOS

- 1.5.4.1. Maior visibilidade do tráfego de rede, possibilitando a detecção e proteção em tempo real contra ameaças;
- 1.5.4.2. Controle efetivo do tráfego de dados através de regras de segurança;
- 1.5.4.3. Detecção e prevenção contra ameaças e tentativas de invasão;
- 1.5.4.4. Monitoramento e rastreabilidade das atividades de rede;
- 1.5.4.5. Manter o monitoramento abrangente e eficiente sobre acessos à internet e tráfego de dados na rede corporativa de computadores;
- 1.5.4.6. Garantir que o TJAL esteja aderente às melhores práticas nacionais e internacionais da área de Segurança da Informação e em consonância com as normas vigentes, tais como a LGPD – Lei Geral de Proteção de Dados (Lei nº 13.709/2018) e o Marco Civil da Internet Lei nº 12.965/2014);
- 1.5.4.7. Garantir que o TJAL preste serviços de qualidade à sociedade, bem como atenda as próprias necessidades institucionais, com base nos pilares de confiabilidade, integridade e disponibilidade.
- 1.5.4.8. Promover proteção superior aos serviços disponibilizados de forma online;
- 1.5.4.9. Promover a melhoria da imagem do Poder Judiciário de Alagoas como provedor de serviços;

1.5.5. RELAÇÃO ENTRE A DEMANDA PREVISTA E A QUANTIDADE DE BENS/SERVIÇOS A SEREM CONTRATADOS

- 1.5.5.1. Item 1: “Solução de segurança da informação do tipo Next Generation Firewall (NGFW), com garantia, suporte técnico e licença de uso por 60 meses”:

Demanda prevista

- Throughput de tráfego, Quantidade de sessões/conexões simultâneas (média/pico) e quantidade de novas sessões por segundo (CPS) (média/pico), em um intervalo de 30 dias:

Informações extraídas pela ferramenta FortiAnalyzer, que analisa os logs dos Fortigates 500E, pertencentes ao conjunto da solução fornecida por terceiros:

All FortiGate - Last 4 Weeks - Dec 23 2021 - Jan 20 2022

Resource Usage Average

#	Device Name	Role	CPU Usage	Memory Usage	Disk Usage	Logs Per Second	Concurrent Sessions	Bandwidth	New Sessions/Sec
1	FG-TJAL-FGSHOE3917901303		0.33%	30.03%	0%	139.21	9479.12	123.126 kbps	175.79
2	FG-TJAL-FGSHOE3917901593		0.05%	24.66%	0%	0.02	61.47	318 kbps	0.34

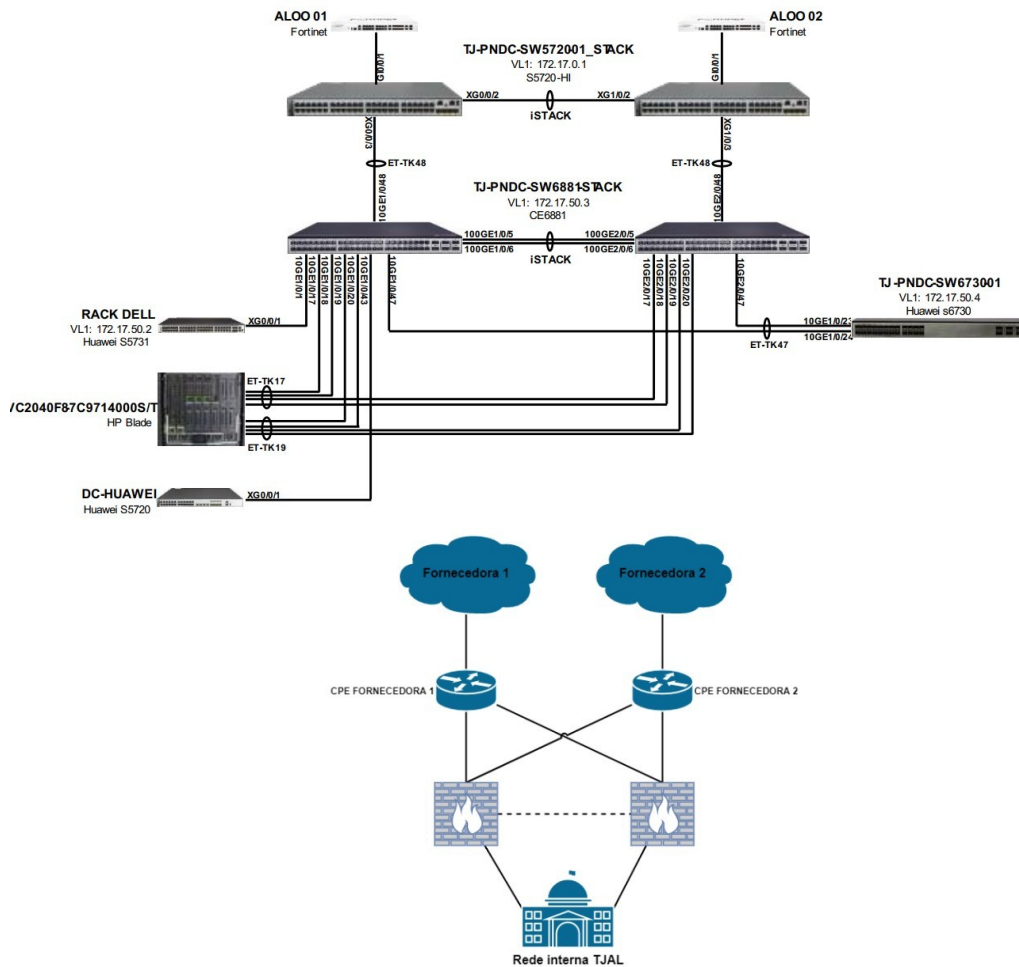
Resource Usage Peak

#	Device Name	Role	CPU Usage	Memory Usage	Disk Usage	Logs Per Second	Concurrent Sessions	Bandwidth	New Sessions/Sec
1	FG-TJAL-FGSHOE3917901303		14%	37%	0%	2.057	44695	1.637.809 kbps	730
2	FG-TJAL-FGSHOE3917901593		20%	26%	0%	1	409	5.163 kbps	104

- Tamanho da banda de Internet disponível:

2 links internet, com 2 trânsitos distintos, sendo 500Mbps em cada link, simétrico (down/up), com possibilidade de expansão para 700Mbps em cada canal no prazo de 5 anos.

- topologia LAN/WAN atual:

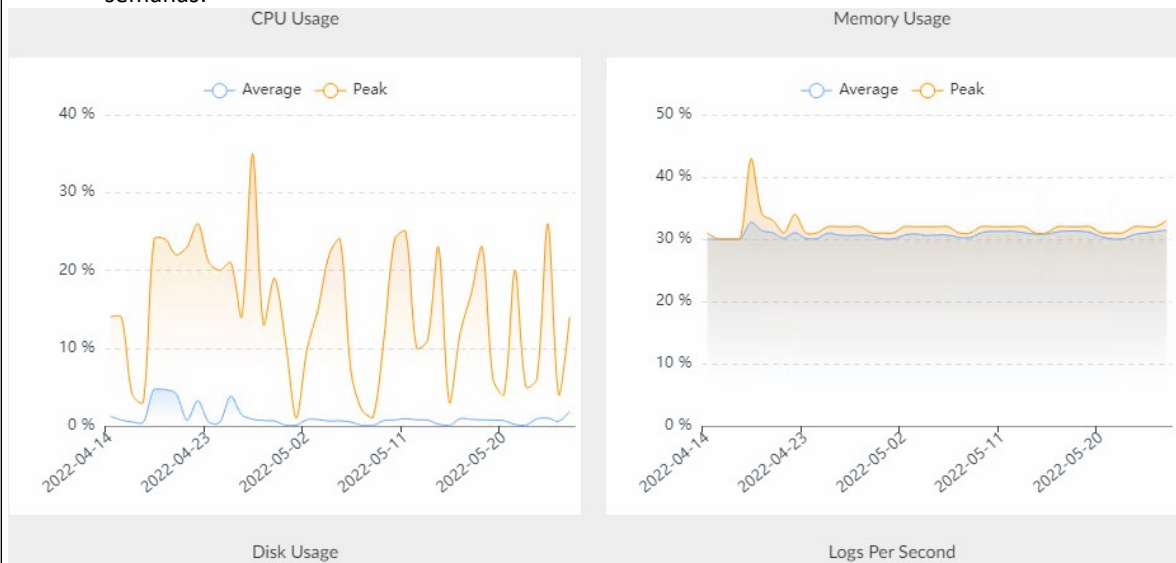


- VPNs:

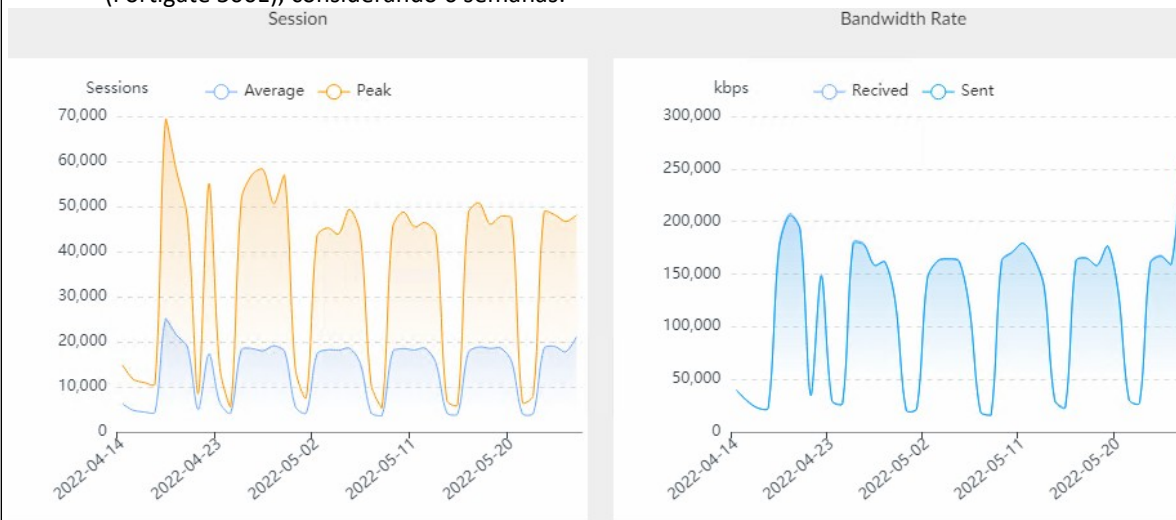
4 VPN's Site-To-Site
Mínimo de 700 usuários de VPN (Client-To-Site)

- Quantidade de regras de firewall atual: 40
- Quantidade de regras de NAT: 3
- Quantidade de perfis para o filtro de conteúdo: aproximadamente 15
- Quantidade de regras de inspeção de IPS e AntiMalware: aproximadamente 15
- Configuração de cluster atual: ativo/passivo

- Uso de disco e memória do firewall atualmente implementado (Fortigate 500E), considerando 6 semanas:



- Pico do número de sessão ativas e largura de banda passante do firewall atualmente implementado (Fortigate 500E), considerando 6 semanas:



Quantidade a ser contratado

- 2 appliances, em configuração ativo/passivo:
 - para garantir a alta disponibilidade nas atividades de inspeção e análise de ameaças;
 - para garantir a alta disponibilidade da solução na função de gateway principal entre a rede do TJAL e a internet;
 - cada appliance dimensionado conforme os requisitos de volume de tráfego, de VPN, conexões simultâneas e os demais requisitos técnicos levantados.
- Licenciamento de 48 meses
 - O número de meses de garantia a ser contratado está alinhado com o manual de "boas práticas, orientações e vedações para contratação de ativos de TIC – versão 4", vinculado à Portaria MP/STI nº 20, de 14 de junho de 2016, na forma de anexo. Neste manual, em contratações que envolvem aquisição de servidores de rede, aplicação, equipamentos de backup, armazenamento, segurança, entre outros, deve-se considerar o tempo de vida útil mínimo de 4 (**quatro**) anos para fins de posicionamento da tecnologia e de garantia de funcionamento.

2. SUSTENTAÇÃO DO CONTRATO

- 2.1. Este plano de sustentação tem como objetivo garantir as condições necessárias à execução do serviço contratada e definir formas e regras de transição após o fim do contrato de modo a não permitir a interrupção do serviço.

2.2. ADEQUAÇÃO DO AMBIENTE

- 2.3. A partir da escolha de alternativa de solução definida no item “Descrição da Solução” do artefato de “Análise de Viabilidade da Contratação”, não será realizada nenhuma adequação do ambiente do TJAL, uma vez que os já há uma solução similar implementada na infraestrutura tecnológica deste Tribunal, sendo necessário apenas sua substituição. O rack que acomodará a solução tem espaços suficientes para uma transição de soluções.

2.4. RECURSOS MATERIAIS E HUMANOS NECESSÁRIOS À CONTINUIDADE DE NEGÓCIO

- 2.5. O contrato envolve entrega de produto com garantia do fabricante. Não haverá necessidade de recursos materiais a serem disponibilizados pelo Tribunal para a execução e continuidade do serviço contratado, tendo em vista que o objeto engloba aquisição de bens e serviços pontuais.
- 2.6. Com relação aos Recursos Humanos, 8 (oito) membros do departamento de redes do TJAL serão treinados para administrar a solução durante todo o seu ciclo de vida.
- 2.7. A Administração deverá formalizar os nomes que farão parte da equipe que se encarregará de acompanhar e viabilizar a implantação da solução adquirida, além dos fiscais que acompanharão a entrega da solução e a prestação dos serviços contratados durante o período de vigência do contrato.

Id	Função	Formação	Atribuições		Carga horária semanal necessária
1	Acompanhamento e fiscalização	Servidor concursado	1	Verificar o cumprimento integral da execução dos serviços	10 horas
			2	Manter registro de ocorrências relacionadas com a execução do contrato, determinando todas as ações necessárias para a regularização das faltas ou defeitos.	10 horas
			3	Comunicar, formalmente, irregularidades cometidas passíveis de penalidades, em como efetuar as glosas na Nota fiscal/Fatura	10 horas

2.8. DESCONTINUIDADE DO FORNECIMENTO

- 2.9. Com o intuito de prevenir danos decorrentes de uma interrupção contratual, a CONTRATADA deverá repassar todo o conhecimento relacionado à administração da solução. Isto minimizará a dependência técnica para configurações necessárias para administrar a solução nos mais variados cenários de utilização.
- 2.10. O risco de descontinuidade está em grande parte vinculado ao risco da fabricante, uma vez que esta deverá oferecer a garantia do produto durante 5 anos.
- 2.11. Os principais fabricantes da solução de segurança de perímetro que será adquirida, como Palo Alto, possuem parceiras localizadas no Brasil, com capacidade similar à empresa que vai fornecer a solução ao Tribunal. Caso

haja alguma interrupção contratual considerada grave, o fabricante da solução pode assumir as pendências deixadas pela empresa parceira, ou indicar outra parceira para dar continuidade, precisando ser realizada uma análise jurídica prévia para este caso.

- 2.12. Nas hipóteses de eventual interrupção da extensão de garantia técnica motivada por fatores puramente técnicos, quando as atualizações e acessos a base de conhecimento da solução de Segurança do Perímetro de Redes fossem violadas, o gestor da solução e sua equipe deverão tomar as seguintes ações:

2.12.1. Hipótese 1: Os equipamentos foram descontinuados pela fabricante da solução durante o período de vigência da extensão da garantia

2.12.1.1. Ação 1: Solicitar ao fornecedor a imediata substituição do equipamento por um outro com características iguais ou superiores.

2.12.1.2. Ação 2: Solicitar a área demandante da solução de TIC que sejam realizados novos Estudos Preliminares para a adoção de uma nova solução de tecnologia da informação.

2.12.1.3. Ação 3: Solicitar que Administração aplique as sanções, dentro dos mecanismos legais possíveis a serem definidos no Termo de Referência e demais instrumentos da contratação

2.12.2. Hipótese 2: Fornecedor deixou de substituir peças, atualizar os firmwares ou interrompeu o acesso a base de conhecimento da solução;

2.12.2.1. Ação 1: Solicitar ao fornecedor a imediata atualização dos firmwares e/ou o reestabelecimento do acesso à base de conhecimento, por meio do canal técnico a ser definido no Termo de Referência.

2.12.2.2. Ação 2: Solicitar que Administração aplique as sanções, dentro dos mecanismos legais possíveis a serem definidos no Termo de Referência e demais instrumentos da contratação.

2.13. TRANSIÇÃO CONTRATUAL E ENCERRAMENTO DO CONTRATO

- 2.14. Havendo transição contratual para outro fornecedor da mesma solução de tecnologia da informação, por motivos de ordem puramente administrativa nos termos do art. 78 da Lei nº 8.666/93, o gestor da solução e sua equipe deverão garantir que todas as ocorrências que estejam eventualmente abertas sejam repassadas para o novo fornecedor. Ademais, deverão verificar se a titularidade da informação dos equipamentos e das licenças de *firmware* permanece a mesma perante o fabricante;
- 2.15. No caso do encerramento da vigência da garantia técnica, o gestor da solução e sua equipe deverão, com antecedência mínima de 15 (quinze) dias, solicitar a imediata atualização dos equipamentos e da base de conhecimento ao fornecedor para a última versão estável disponível pelo fabricante;

2.16. ESTRATÉGIA DE INDEPENDÊNCIA TECNOLÓGICA

- 2.17. É senso comum que o fabricante de equipamentos que operam estruturas baseadas em *firmware* é a única entidade capaz de prover atualizações de versões da plataforma, uma vez que é detentor exclusivo dos meios de produção do programa, tendo os direitos de propriedade intelectual protegido por 50 (cinquenta) anos, nos termos do art. 2º, § 2º da Lei nº 9.609/98;
- 2.18. Para garantir o adequado funcionamento do equipamento, as peças que vierem a ser substituídas e os profissionais que realizarem a substituição devem ser homologados e credenciados pelo fabricante, sendo essa condição determinante para habilitação dos fornecedores/revendas;
- 2.19. A melhor estratégia para independência tecnológica é solicitar que a área demandante realize, a cada 2 (dois) anos, um novo Estudo Preliminar para verificar no mercado de TIC novas soluções tecnológicas para Segurança de Perímetro de Rede, nos termos dos requisitos definidos no artefato de “Análise de Viabilidade da Contratação”. Ao término desse período, os equipamentos estarão com 60 (sessenta) meses de uso, validando a necessidade de novos estudos, com possível troca de tecnologia considerada superada;

3. ESTRATÉGIA PARA CONTRATAÇÃO

Natureza do objeto	Trata-se de contratação de bens, de acordo com o parágrafo único do art. 1º da Lei do Pregão Eletrônico, n. 10.250/2002, “aqueles cujos padrões de desempenho e qualidade possam ser objetivamente definidos pelo edital, por meio de especificações usuais no mercado”
Parcelamento do objeto	Os ativos de segurança e os serviços associados, todos componentes do objeto ofertado, possuem alta correlação técnica entre si, de forma que é bastante recomendável que sejam adjudicados a um único fornecedor para que seja mantida a máxima compatibilidade técnica entre as soluções.
Adjudicação do objeto	Lote único, agrupando itens distintos, adjudicados a uma única empresa. O lote a ser ofertado possui componentes que serão configurados e mantidos em conjunto, o que torna viável a garantia de funcionamento de ambos pelo mesmo período e a cargo do mesmo fornecedor.
Modalidade e Tipo de licitação	Os bens e serviços da contratação pretendida podem ser classificados como comuns, uma vez que padrões de desempenho e qualidade podem ser objetivamente definidos pelo edital, por meio de especificações usuais no mercado. Desta forma, a aquisição pretendida deverá ser realizada pela modalidade Pregão Eletrônico, do tipo menor preço global .
Classificação e indicação da fonte de recursos	A fonte dos recursos financeiros será indicada pelo Funjuris. A classificação da despesa, segundo o tipo de item a ser adquirido é categorizada como contratação de equipamentos de Tecnologia da Informação.
Vigência e prazo de garantia	Os efeitos da contratação, serviços de garantia e suporte técnico, deverão perdurar pelo período de 48 meses (4 anos)
Equipe de gestão da contratação	Gestor do Contrato: Indicação a cargo da Subdireção-Geral Fiscal Técnico: Indicação a cargo da Diretoria Adjunta de TI

4. ANÁLISE DE RISCOS

4.1. RISCOS DO PROCESSO DE CONTRATAÇÃO

Risco 1.1				
Descrição		Demora na conclusão do processo licitatório em face de impugnações, recursos ou outros motivos		
Grau do risco		Impacto: Média Probabilidade: Alta	Id	Dano
			1	Atraso no processo de contratação
			2	Serviço de segurança de perímetro atual perder a vigência
Id	Ação preventiva		Responsável	
1	Verificação do teor de impugnações e recursos em contratações similares		Integrante administrativo e técnico	
Id	Ação de contingência		Responsável	
1	Acompanhamento com o auxílio da área jurídica para resposta às impugnações e recursos.		DIATI	
2	Tomar medidas para manter o atual serviço de segurança de perímetro vigente até a nova solução tomar a frente no propósito de garantir a segurança na borda da rede do TJAL		Gestor/fiscal do contrato	

Risco 1.2				
Descrição		Produto entregue fora das especificações exigidas		
Grau do risco		Impacto: Alto	Id	Dano
		Probabilidade: Baixa	1	Atraso na conclusão do processo de aquisição
Id	Ação preventiva			Responsável
1	Dar prazo para que a empresa regularize a entrega, conforme os Termos do Edital.			Fiscal do Contrato
Id	Ação de contingência			Responsável
1	Não efetuar o recebimento definitivo, fazer a devolução e exigir a conformidade do objeto. Inobservada essa exigência, convocar o próximo classificado no certame			Fiscal do contrato

4.2. RISCOS DE NEGÓCIO

Risco 2.1					
Descrição		Indisponibilidade de serviços essenciais			
Grau do risco		Impacto: Alto Probabilidade: Baixa	Id		Dano
			1	Grandes prejuízos para a imagem institucional do TJAL e para a prestação de serviços de Tecnologia da Informação e Comunicação (TIC) aos jurisdicionados	
Id	Ação preventiva			Responsável	
1	Manter diligência sobre o estado da contratação, incluindo a eficiência e eficácia do suporte técnico			Fiscal do Contrato	
Id	Ação de contingência			Responsável	
1	Configurar um servidor de propósito geral para exercer parcialmente a funções desejadas nessa contratação			DIATI	

4.3. RISCOS DA EXECUÇÃO DO OBJETO

Risco 3.1			
Descrição	A natureza técnica do objeto suscita a ocorrência de eventuais problemas associados ao funcionamento dos equipamentos.		
Grau do risco	Impacto: Médio Probabilidade: Baixa	Id	Dano
		1	Degradação do desempenho das aplicações
Id	Ação preventiva		Responsável
1	Verificar a conformidade do objeto adquirido; garantir que as condições do ambiente físico em que está instalado o equipamento são adequadas para a implantação e o bom funcionamento do ativo		Fiscal Técnico do contrato / Departamento de Redes e Infraestrutura
Id	Ação de contingência		Responsável
1	Acionamento da garantia do fabricante, a fim de que seja efetuada a troca do bem		Fiscal Técnico do contrato / Departamento de Redes e Infraestrutura

Risco 3.2			
Descrição	Ausência de substituição de peças, atualização dos firmwares ou interrupção ao acesso à base de conhecimento da solução		
Grau do risco	Impacto: Médio Probabilidade: Baixa	Id	Dano
		1	Limitação da capacidade de prover segurança ao ambiente tecnológico do TJAL, além de possíveis falhas na disponibilidade dos serviços essenciais disponibilizados.
Id	Ação preventiva		Responsável
1	Monitorar a execução do contrato, com fito de verificar as periodicidade de atualizações e o cumprimento das SLAs		Fiscal técnico
Id	Ação de contingência		Responsável
1	Solicitar ao fornecedor a imediata atualização dos firmwares e/ou o reestabelecimento do acesso à base de conhecimento		Fiscal Técnico
2	Solicitar que Administração aplique sanções, dentro dos mecanismos legais possíveis		Gestor do Contrato

Risco 3.3			
Descrição	Descontinuidade da solução pelo fabricante durante o período de vigência do suporte técnico		
Grau do risco	Impacto: Alto Probabilidade: Baixa	Id	Dano
		1	Limitação da capacidade de prover segurança ao ambiente tecnológico do TJAL, além de possíveis falhas na disponibilidade dos serviços essenciais disponibilizados.
Id	Ação preventiva		Responsável
1	Monitorar a execução do contrato, com fito de verificar se as atualizações estão sendo realizadas regularmente.		Fiscal técnico / Equipe de redes e infraestrutura
Id	Ação de contingência		Responsável
1	Solicitar ao fornecedor a imediata substituição dos equipamentos descontinuados, caso as atualizações e substituição de peças estejam prejudicados.		Fiscal Técnico
2	Solicitar a área demandante da solução de TIC que sejam realizados novos Estudos Preliminares para a adoção de uma nova solução de segurança de perímetro de rede;		DIATI
3	Solicitar que a Administração aplique sanções, dentro dos mecanismos legais possíveis;		Gestor do Contrato

4.4. RISCOS ADMINISTRATIVOS

Risco 4.1				
Descrição		Falta de pessoal técnico para fiscalização do contrato		
Grau do risco	Impacto: Médio Probabilidade: Médio	Id	Dano	
		1	Comprometimento na aferição dos níveis de serviço	
		2	Atrasos na emissão do termo de recebimento dos serviços	
		3	Não prestação do serviço ou prestação do serviço com baixa qualidade	
Id	Ação preventiva			Responsável
1	Recrutar e treinar novos fiscais de contrato de TI			Diretoria da DIATI
Id	Ação de contingência			Responsável
1	Acumular papel de fiscal técnico juntamente com gestor do contrato, até a definição do novo fiscal			Gestor do contrato

4.5. MATRIZ DE AVALIAÇÃO QUALITATIVA DOS RISCOS IDENTIFICADOS

Probabilidade/Impacto	Sem impacto	Baixo	Médio	Alto
Baixa			3.1, 3.2	1.2, 2.1, 3.3
Média			4.1	
Alta			1.1	

5. APROVAÇÃO E ASSINATURA

Integrante Demandante	Integrante Técnico	Integrante Administrativo
<hr/> Jose Baptista dos Santos Neto Diretor da DIATI	<hr/> Christiano Rossini Martins Costa DIATI	<hr/> Aline Gama Pinheiro de Melo DGC

6. ANEXO TR1 – PROPOSTAS DE PREÇOS

Id	Descrição do bem ou serviço	Unidade	Qtde	Propostas					
				P1		P2		P3	
				VU	VT	VU	VT	VU	VT
1	Solução de segurança da informação do tipo Next Generation Firewall (NGFW), com garantia, suporte técnico e licença de uso por 60 meses	equipamento	2	R\$ 1.272.000,00	R\$ 2.544.000,00	R\$ 1.041.418,52	R\$ 2.082.837,04	R\$ 3.017.645,01	R\$ 6.035.290,02
2	Serviço de instalação e configuração profissional dos equipamentos	serviço	1	R\$ 89.000,00	R\$ 89.000,00	R\$ 118.424,65	R\$ 118.424,65	R\$ 38.525,92	R\$ 38.525,92
3	Treinamento oficial do fabricante	aluno	8	R\$ 9.200,00	R\$ 73.600,00	R\$ 22.465,68	R\$ 179.725,44	R\$ 19.062,64	R\$ 152.501,13
4	Consultoria técnica especializada da solução	UST	500	R\$ 520,00	R\$ 260.000,00	R\$ 555,46	R\$ 277.730,00	R\$ 259,03	R\$ 129.515,00
				R\$ 2.966.600,00		R\$ 2.658.717,13		R\$ 6.355.832,07	

Menor proposta R\$ 2.658.717,13

Proposta	Empresa	CNPJ	Contato
P1	INFOREADY TECNOLOGIA LTDA (Go Ahead)	13.727.635/0001-37	cpaixao@goaheadit.com.br
P2	SUPRISERVI COMÉRCIO, REPRESENTAÇÕES E SERVIÇOS LTDA (NewSupri)	12.707.105/0003-26	sergio@newsupri.com.br
P3	TrustControl	11.061.153/0001-65	diane.pimentel@trustcontrol.com.br